

CA Service Desk Manager

Administrationshandbuch

Version 12.9.00



Diese Dokumentation, die eingebettete Hilfesysteme und elektronisch verteilte Materialien beinhaltet (im Folgenden als "Dokumentation" bezeichnet), dient ausschließlich zu Informationszwecken des Nutzers und kann von CA jederzeit geändert oder zurückgenommen werden.

Diese Dokumentation darf ohne vorherige schriftliche Genehmigung von CA weder vollständig noch auszugsweise kopiert, übertragen, vervielfältigt, veröffentlicht, geändert oder dupliziert werden. Diese Dokumentation enthält vertrauliche und firmeneigene Informationen von CA und darf vom Nutzer nicht weitergegeben oder zu anderen Zwecken verwendet werden als zu denen, die (i) in einer separaten Vereinbarung zwischen dem Nutzer und CA über die Verwendung der CA-Software, auf die sich die Dokumentation bezieht, zugelassen sind, oder die (ii) in einer separaten Vertraulichkeitsvereinbarung zwischen dem Nutzer und CA festgehalten wurden.

Ungeachtet der oben genannten Bestimmungen ist der Benutzer, der über eine Lizenz für das bzw. die in dieser Dokumentation berücksichtigten Software-Produkt(e) verfügt, berechtigt, eine angemessene Anzahl an Kopien dieser Dokumentation zum eigenen innerbetrieblichen Gebrauch im Zusammenhang mit der betreffenden Software auszudrucken, vorausgesetzt, dass jedes Exemplar diesen Urheberrechtsvermerk und sonstige Hinweise von CA enthält.

Dieses Recht zum Drucken oder anderweitigen Anfertigen einer Kopie der Dokumentation beschränkt sich auf den Zeitraum der vollen Wirksamkeit der Produktlizenz. Sollte die Lizenz aus irgendeinem Grund enden, bestätigt der Lizenznehmer gegenüber CA schriftlich, dass alle Kopien oder Teilkopien der Dokumentation an CA zurückgegeben oder vernichtet worden sind.

SOWEIT NACH ANWENDBAREM RECHT ERLAUBT, STELLT CA DIESE DOKUMENTATION IM VORLIEGENDEN ZUSTAND OHNE JEGICHE GEWÄHRLEISTUNG ZUR VERFÜGUNG; DAZU GEHÖREN INSBESONDERE STILLSCHWEIGENDE GEWÄHRLEISTUNGEN DER MARKTTAUGLICHKEIT, DER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK UND DER NICHTVERLETZUNG VON RECHTEN. IN KEINEM FALL HAFTET CA GEGENÜBER IHNEN ODER DRITTEN GEGENÜBER FÜR VERLUSTE ODER UNMITTELBARE ODER MITTELBARE SCHÄDEN, DIE AUS DER NUTZUNG DIESER DOKUMENTATION ENTSTEHEN; DAZU GEHÖREN INSBESONDERE ENTGANGENE GEWINNE, VERLORENGEGANGENE INVESTITIONEN, BETRIEBSUNTERBRECHUNG, VERLUST VON GOODWILL ODER DATENVERLUST, SELBST WENN CA ÜBER DIE MÖGLICHKEIT DIESES VERLUSTES ODER SCHADENS INFORMIERT WURDE.

Die Verwendung aller in der Dokumentation aufgeführten Software-Produkte unterliegt den entsprechenden Lizenzvereinbarungen, und diese werden durch die Bedingungen dieser rechtlichen Hinweise in keiner Weise verändert.

Diese Dokumentation wurde von CA hergestellt.

Zur Verfügung gestellt mit „Restricted Rights“ (eingeschränkten Rechten) geliefert. Die Verwendung, Duplizierung oder Veröffentlichung durch die US-Regierung unterliegt den in FAR, Absätze 12.212, 52.227-14 und 52.227-19(c)(1) bis (2) und DFARS, Absatz 252.227-7014(b)(3) festgelegten Einschränkungen, soweit anwendbar, oder deren Nachfolgebestimmungen.

Copyright © 2013 CA. Alle Rechte vorbehalten. Alle Marken, Produktnamen, Dienstleistungsmarken oder Logos, auf die hier verwiesen wird, sind Eigentum der entsprechenden Rechtsinhaber.

CA Technologies-Produktreferenzen

Dieses Dokument bezieht sich auf die folgenden CA Technologies-Produkte:

- CA Asset Portfolio Management (CA APM)
- CA CMDB
- CA Business Intelligence
- CA Business Service Insight (CA BSI)
- CA Configuration Automation (früher CA Cohesion ACM)
- CA Embedded Entitlements Manager (CA EEM)
- CA Enterprise Workload Automation (CA EWA)
- CA Process Automation (früher CA IT PAM)
- CA-Management-Datenbank (CA MDB)
- CA Management Portal
- CA Network and Systems Management (CA NSM)
- CA Portal
- CA Remote Control Manager (CA RCM)
- CA Service Desk Manager (CA SDM)
- CA Service Management
- CA Siteminder
- CA Software Delivery
- CA Spectrum® Infrastructure Manager (CA Spectrum)
- CA Wily
- CA Workflow

Technischer Support – Kontaktinformationen

Wenn Sie technische Unterstützung für dieses Produkt benötigen, wenden Sie sich an den Technischen Support unter <http://www.ca.com/worldwide>. Dort finden Sie eine Liste mit Standorten und Telefonnummern sowie Informationen zu den Bürozeiten.

Inhalt

Kapitel 1: Einführung 25

Zielgruppe	25
Was Sie wissen müssen	25
Dienstverwaltungsprozesse und bewährte Praktiken	26

Kapitel 2: Verwalten von Servern 27

Anzahl der Server	27
So ändern Sie eine Serverkonfiguration	28
So starten Sie die CA SDM-Server	28
Starten der CA SDM-Server in konventioneller Konfiguration	30
Starten der CA SDM-Server in der Konfiguration für erweiterte Verfügbarkeit	31
So führen Sie parallele Serverwartung auf CA SDM-Servern aus	32
Überprüfen der Hinweise	34
Unterdrücken der Versionskontrolle zwischen dem Standby-Server und dem Hintergrundserver	35
Hochstufen des Standby-Servers als neuen Hintergrundserver	35
Ausführen der parallelen Wartung auf Anwendungsservern	36
So konfigurieren Sie SSL-Authentifizierung	39
Überprüfen der Voraussetzungen	40
Festlegen der Web-Engine-Funktion durch Web-Director-Parameter	40
Auswählen der SSL-Anmeldeumgebung	41
Einrichten der SSL-Anmeldeumgebung	44
So konfigurieren Sie TCP/IP	51
Bereitstellen von CMDBf-Webservices	52
So starten Sie die CA SDM-Server neu	52
Neustarten der CA SDM-Server in konventioneller Konfiguration	52
Neustarten der CA SDM-Server in der Konfiguration für erweiterte Verfügbarkeit neu	52
So halten Sie die CA SDM-Server an	56
Anhalten der CA SDM-Server in konventioneller Konfiguration	56
Anhalten der CA SDM-Server in der Konfiguration für erweiterte Verfügbarkeit	57
Unterstützte Tablets	59
Tomcat-Protokollierung	61
Servlet-Standards	62
PDA-Schnittstelle	62
REST-Protokollierung	63
Aktivieren der CXF-Protokollierung	64
So konfigurieren Sie Prozesse für CA SDM-Server	70

Hinzufügen eines Servers	71
Erstellen einer Prozesskonfiguration	72
Hinzufügen von CA SDM-Serverprozessen	74
Überprüfen der Konfiguration	89

Kapitel 3: REST-Beispieloberfläche für Mobilgeräte 91

So stellen Sie REST-Beispieloberfläche für Mobilgeräte bereit	93
Konfigurieren von REST-Webservices	94
Aktivieren der mobilen REST-Beispieloberfläche für Mobilgeräte	95
Verwalten von Incidents über die REST-Beispieloberfläche für Mobilgeräte	95
Beispiel: Startseite der Analystenschnittstelle	96
Beispiel: Startseite der Mitarbeiterschnittstelle	97
Beispiel: Der Mitarbeiter erstellt einen Incident	98

Kapitel 4: CA SDM Mobile Enabler-Konfiguration 99

CA SDM Mobile Enabler	99
Analyst-Warteschlange	100
Genehmigungen	101
Open Space	104
Überprüfen der Voraussetzungen	105
Zertifizierte Mobilgerät-Betriebssysteme	106
Anwenden der Patches auf Open Space	106
Aktivieren von CORS-Einstellungen	107
(Optional) Festlegen von Formularfeldern als nicht erforderlich	109
(Optional) Erzwingen der Genehmigungsvereinbarkeit nach Aktualisierung	110
Zugreifen auf CA SDM-Mobile Enabler	110

Kapitel 5: Definieren der Geschäftsstruktur 111

Erstellen der Geschäftsstruktur	112
So erstellen Sie die Geschäftsstruktur	115
Definieren der Unternehmensinfrastruktur	125
Objektdefinitionsreihenfolge	126
Configuration Item-Familien und -Klassen	126
Hersteller und Modelle	127
Dienststatus	127
Anbietertypen und Anbieter	127
Configuration Items	128
Externe Anlagenverwaltungstools	128
Mehrere Mandanten	129
Service Provider	130

Wie Multi-Tenancy funktioniert.....	131
Auswirkung auf die Benutzerschnittstelle	138
Support-Automatisierung-Auswirkung	141
Auswirkung auf Knowledge Management	142
Verwenden von Multi-Tenancy.....	144

Kapitel 6: Integrieren mehrerer Suchmaschinen mithilfe von föderierter Suche 155

Föderierte Suche konfigurieren	156
Erfüllen der Voraussetzungen	157
Aktivieren Sie die föderierte Suche.....	158
Generieren der XML-Dateien der Konfiguration für föderierte Suche	159
Erstellen der Quellen der föderierten Suche in CA SDM.....	166
Deinstallieren der Suchadapter.....	167
Konfigurieren der Crawlers-Oberfläche	169
Erfüllen der Voraussetzungen	170
Erstellen der Crawler-Oberfläche für den CA SDM-Anwender	170
Konfigurieren des Tomcat Remote IP Address Filter	171
Konfigurieren der Anwender-ID für die Crawler-Oberfläche	173
Konfigurieren des SharePoint-Crawlers	180
Erstellen Sie die Inhaltsquelle in SharePoint.....	181
Erstellen von Crawlregeln	182
Starten eines Crawl in SharePoint.....	183
Konfigurieren Sie die Metadaten in SharePoint.....	184
Verifizieren Sie die Crawl-Daten in SharePoint	185
Fehlerbehebung	186
Erstellen Sie einen neuen anwenderspezifischen Adapter mithilfe der SDK-Schnittstelle	188
Kompilieren der JAR-Dateien des neuen anwenderspezifischen Adapters	190
Konfigurieren Sie den neuen anwenderspezifischen Suchadapter mit der Komponente "CAFedSearch"	193
Verifizieren des neuen anwenderspezifischen Suchadapters.....	195
Hinzufügen des Cross-Origin Resource Sharing-Filters (CORS)	196
Abrufen des Servlets "CAFedSearch" mithilfe von REST	197

Kapitel 7: Richtlinie zur Implementierung: 199

Implementieren von Richtlinien.....	199
Benachrichtigungen	199
CA SDM-Integration	315

Kapitel 8: Konfiguration von Anwenderkonten 337

Kontakte	337

Kontaktdefinitionen	337
Gruppen	339
Kontakttypen.....	340
Bestimmen des Verhaltens auf der Basis des Kontakttyps	340
Einrichten von Benachrichtigungen auf der Basis von Kontakttypen	340
Auswählen von Kontakten auf der Basis des Kontakttyps	340
Spezielle Verarbeitungs-Typen.....	341
Konfigurieren von Kontakten zur speziellen Verarbeitung	342
Zuordnen von Kontakten zu bestimmten Verarbeitungstypen	343
LDAP-Verzeichnis-Daten	344

Kapitel 9: Verwalten von Rollen 369

Rollen	369
Vordefinierte Rollen	369
Role-Based Sicherheit	371
Funktionsweise von Zugriffstypen	372
Rollendatensätze.....	375
Funktionale Zugriffsbereiche	376
Datenaufteilungen	381
Rollenbasierte Navigation	381
Registerkarten	381
Vordefinierte Registerkarten	383
Webformulare	385
Formulargruppen	385
Menüstrukturen	386
Menüstrukturressourcen	387
Menüleisten	387
Symbolleisten.....	389
'Los'-Ressourcen.....	389
Hilfesätze.....	390
Implementieren einer benutzerdefinierten Menüstruktur.....	390
Implementieren einer anwenderspezifischen Menüstruktur	392
Erstellen von Rollendatensätzen	393
Erstellen von Registerkartendatensätzen	394
Erstellen von Menüleistendatensätzen.....	395
Erstellen von Webformular-Datensätzen.....	396
Kopieren von Menüstrukturen.....	397
Erstellen und Anpassen von Menüstrukturen.....	398
Erstellen und Veröffentlichen von Helpsets.....	400
Wechseln von Rollen	401

Kapitel 10: Einrichten einer Support-Struktur

403

Modelle	403
Internes Modell	404
Externes Modell	405
Kombiniertes Modell	406
CA Workflow	407
Workflow zur Laufzeit	408
Auswählen einer Workflow-Prozessdefinition	408
Workflow-Aufgaben	410
CA Process Automation-Workflow-Integration	410
CA Process Automation-Komponenten	411
CA Process Automation Integration mit CA SDM zur Laufzeit	412
Erstellen einer Prozessdefinition	413
Erstellen von Startauftragsformularen	414
Anhängen von CA Process Automation-Prozessdefinitionen	416
Freigegebene Codes	417
Prioritätscodes	418
Schweregrad-Codes	418
Auswirkungscodes	419
Dringlichkeitscodes	419
Statuscodes	419
Anfragestatuscodes	420
Statuscodes von Changes	421
Statuscodes von Issues	422
Aufgabenstatuscodes	423
Aufgabentypen	424
Installieren der Incident-Nachverfolgung	426
Request-/Incident-/Problembereiche	427
Anfrage-/Incident-/Problembereich - Eigenschaften	428
Definieren von Anfrage/Zwischenfall-/Problembereichen für Self-Service	430
Change- und Issue-Kategorien	430
Vordefinierte Change-Kategorien	432
Vordefinierte Issue-Kategorien	432
Regeln zum Ändern von Kategorien in einem Ticket	432
Kategorieeigenschaften	433
Definieren von Change-Kategorien und Issue-Kategorien für Self-Service	435
Automatisches Schließen von Tickets	436
Definieren von Einstellungen zur automatischen Schließung von Tickets	437
Definieren einer Aktivitätsbenachrichtigung für die automatische Schließung	438
Aktivitäten zugehöriger Tickets	438
Definieren von Aktivitätsbenachrichtigungen für zugehörige Tickets	439

Definieren von Benachrichtigungen über die Aktivität zugehöriger Tickets.....	440
Prioritätsberechnung	440
Verwaltung von Ticketwerten durch Prioritätsberechnung.....	442
Prioritätsberechnung generiert nach dem Speichern von Self-Service-Tickets einen Dringlichkeitswert.....	445
Einstellen der Prioritätsberechnung	446
Statusübergänge und abhängige Attributsteuerungen.....	458
Arbeiten mit Statusübergängen und abhängigen Attributsteuerungen	459
Konfigurieren der Statusübergänge	460
Konfigurieren abhängiger Attributsteuerelemente	461
Web-Service-Methoden	463
Vordefinierte Übergangsabläufe.....	463
Best Practices: Vordefinierte Statusübergänge	468
Statusübergänge für Self-Service	469
Funktionsweise der Übergänge für Self-Service	470
Erstellen oder Aktualisieren von Übergangstypen für Übergänge	471
Verknüpfen von Übergangstypen mit Übergängen	472
Aktivieren von vordefinierten Übergangstypen.....	472
Timer	474
Zeitzone.....	475
Auslöser für Servicetypereignisse	475
Zeitzone-Event-Auslöser	476
Zeitzoneregeln	477
So richten Sie die Anhangsbibliothek ein	478
Öffnen der CA SDM-Web-Benutzeroberfläche	479
Erstellen von Dateitypen.....	479
Auswählen des Repository	480
Erstellen eines Ordners	487
Ankündigungen	488
Sichtbarkeit interner Ankündigungen	489
Angaben der Ankündigungsdringlichkeit	490
Einrichten von gespeicherten Abfragen	490
Sequenznummern	491
Verwenden des Audit-Protokolls	492
Integration in das CA-Netzwerk und Systemverwaltung	493
Drucken von CA SDM-Webseiten.....	493
Verhalten für die Anzeige von Datensätzen in der Web-Schnittstelle	494
Support-Struktur	495
Aktivieren der CAPA-Hilfe	495
 Kapitel 11: Steuerung des Systemverhaltens	 497
Verwendung des Optionsmanagers	497

Ändern der System-Umgebung	498
Kapitel 12: Konfiguration der Option "Automatische Zuweisung"	505
Automatische Zuweisung	505
Beziehungen bei der automatischen Zuweisung	506
Methoden der automatischen Zuweisung	506
Implementieren von automatischen Zuweisungen	507
Bereiche und Kategorien	507
Analystengruppen	508
Analyst	509
Automatisches Zuweisen von Tickets zu einer Gruppe und nicht zu Kontakten innerhalb der Gruppe	509
Automatische Zuweisung nach Lokation	510
Automatische Zuweisung nach Schicht	512
Standardgruppe und -zuständiger	513
Aktivieren der automatischen Zuweisung	514
Überschreiben der automatischen Zuweisung	515
Zuweisungssteuerungen	516
Manuelle Zuweisung	516
Option „Assignee_set“	516
Iss assignee_set	516
Area_Defaults	517
Optionen, die einen Zuständigen/eine Gruppe erfordern	517
Vorlagen	518
CA Network and Systems Management-Schnittstelle	518
Aktivitätsprotokoll	519
Aktivieren der Aktivitätsprotokollierung für zusätzliche Attribute	520
Ablaufverfolgung der automatischen Zuweisung	520
Gespeicherte Abfragen	521
Automatisches Zuweisen von Tickets	521
Automatisches Zuweisen von Workflow-Aufgaben	529
Configuration Item-basierte automatische Zuweisungen	533
Funktionsweise der auf einem Configuration Item basierenden automatischen Zuweisungen	533
Aktivieren von Configuration Item-basierten automatischen Zuweisungen	537
Kapitel 13: Verwalten Sie Ihre Datenbank	539
Datenbankverwaltungsprogramme	539
Auswählen und Konfigurieren der Datenbank	539
Datenbanklader	540
Erstellen und Nutzen einer Eingabedatei	541
Entfernen und Wiederherstellen von Bedingungen	542
Sichern von Datenbanken	543

Datenbankwiederherstellung.....	543
Datenbanktabellen-Ersatz	544
Extrahieren von Daten	544
Daten-Dereferenzierung	546
Beispiel für das Ausführen von "pdm_deref"	546
Verwenden des dbadmin-Modus.....	549
Verbessern der Leistung mit Browser-Caching	561
Konfigurieren von Microsoft Internet Information Server.....	561
Konfigurieren von Apache.....	562
Löschen des Cache-Speichers	563
Änderung der Konfigurationsdatei.....	563
SchedExpMaximum	573
SelListCacheExclude	573
SelListCacheMax	573

Kapitel 14: Verwenden der Text-API 579

Text-API	579
Befehlszeilenschnittstelle.....	580
CA Network and Systems Management-Schnittstelle	580
Eingabeformat.....	581
Schlüsselwörter	582
Eingabekonventionen für Schlüsselwörter	584
Formatieren von E-Mail-Nachrichten zum Aktualisieren eines Tickets	585
Start- und Endtrennzeichen in E-Mail-Nachrichten	586
Text-API und Artefakte.....	586
Einrichten von Benachrichtigungsantworten zum Aktualisieren von Tickets	587
Konvertierungsmethoden	591
Die Konfigurationsdatei	593

Kapitel 15: So führen Sie eine Versionskontrolle der Systemanpassungen auf CA SDM-Servern durch 597

Überprüfen der Voraussetzungen.....	599
Ändern der Versionskontrolldatei des Servers	599
Versionskontrollkomponenten	600
Versionskontrollparameter	601
Neustarten von CA SDM auf dem Client.	606
Auswählen des Anwendungsservers, der wenig aktiv ist.....	606
Anhalten der anderen Anwendungsserver	606
Überprüfen der Anpassungen auf dem Client	607

Kapitel 16: Verwalten von Konfigurationselementen

609

Verwenden der Web-Schnittstelle	609
Anzeigen von Configuration Items	610
Erstellen von Configuration Items.....	610
Aktualisieren von Configuration Items.....	611
Zuordnen eines Wartungsfensters zu einem CI	612
Anzeigen von zugeordneten Change-Fenstern	612
Anzeigen des Configuration Item-Verlaufs	613
Deaktivieren von Konfigurationselementen	613
Neu aktivieren von Konfigurationselementen	614
Configuration Items: Kontakt, Standort und Organisation	614
Erstellen eines CI auf der Grundlage eines Basisobjekts	614
Wählen eines Basisobjekts für ein CI	615
Bearbeiten von Configuration Item-Details für ein Basisobjekt.....	616
Bearbeiten von CI-Attributen für ein Basisobjekt	616
Erstellen eines Basisobjekt-CI mit Hilfe von GRLoader	617
CI Relationships	617
CI-Beziehungstypen.....	618
Erstellen eines Beziehungstyps	619
Verwalten von CI-Beziehungen	620
Erstellen von CI-Beziehungen.....	620
Anzeigen von Beziehungen für ein CI.....	621
Deaktivieren von CI-Beziehungen	621
Neuaktivieren einer CI-Beziehung.....	622
Deaktivieren von CI-Beziehungen (Listenbearbeitung).....	622
Deaktivieren von CI-Beziehungen mit Hilfe von GRLoader	623
Erneutes Aktivieren von CI-Beziehungen mit Hilfe von GRLoader	624
Löschen von CI-Beziehungen aus der Datenbank	625
CI-Beziehungs-Verlauf und -Vergleich.....	626
Versionskontrolle	626
Verwenden von Versionskontrolle.....	628
Datensätze für gemeinsame Assets und CI-Audit-Kontrolle	629
Terminologie der Versionskontrolle	629
Datenquellen für Versionskontrollen.....	633
CA SDM Change Management-Integration.....	634
CA APM-Integration	635
CI-Versionsmanagement.....	636
CA SDM Change Management	653
Anzeigen von CI-Attributen in anderen CA-Produkten	654
Verwenden des CMDBf-Viewers	655
CMDB Visualizer	655

Durchführen der Ursachenanalyse	658
Visualizer-Administration	659
Hinzufügen von ermittelten Assets	659
Asset- und CI-Markierungen	660
Abstimmung von CIs	661
MDR-basierte Abstimmung	662
Identifizieren und Auflösen von mehrdeutigen CIs	664
Überprüfen und Ändern von eingehenden Daten mit dem Transaktionsarbeitsbereich (TWA)	676
Verwalten bereitgestellter Transaktionen	682
Transaktionsarbeitsbereich	683
Auffüllen des Transaktionsarbeitsbereichs	684
Aktualisieren von Daten im TWA über die Web-Schnittstelle	696
Verwalten von Beziehungstransaktionen	700
Laden von Transaktionen in die CMDB	701
TWA-Administration	703
CA CMDB-Datenwartung	707
CA CMDB-Strukturen für Familie und Klasse	708
Ändern der Familie/Klasse eines einzigen CI	709
Ändern der Familie/Klasse einer Liste von CIs	709
Ändern von CI-Familien oder CI-Klassen mit GRLoader	710
Erweitern von CA CMDB	710
Configuration Audit and Control Facility (CACF)	722
CACF-Verwaltung und Richtliniendefinition	724
Verwaltete Attribute	740
Verwaltete Change-Zustände	740
Change-Spezifikationen	743
Ablauf der Change-Verifizierung	748
Archivieren und Bereinigen von Audit-Daten	754
Implementieren einer Change-Verifizierungsstrategie	755
Planen und Implementieren von Change-Verifizierung	759
Best Practices für Change-Verifizierung	766
Manuelles Verifizieren von aktualisierten Attributwerten	770
Beispiel: Rogue-Aktualisierungen nur von einer bestimmten Lokation erlauben	775
Beispiel: Durchführen eines Upgrade für Laptops in Ihrer Organisation	777
Beispiel: Sperren nicht verifizierter Changes	778
Beispiel: Erlauben einer CI-Aktualisierung, wenn kein übereinstimmender Change vorhanden ist	779
Beispiel: Verschieben aller Aktualisierungen aus CA Configuration Automation in den TWA	779
Beispiel: Richtlinienergebnisse zu Testzwecken nur ins Protokoll schreiben	780
Beispiel: Ablehnen einer CI-Aktualisierung	780
Beispiel: Erlauben von Changes ohne Spezifikationen	781
Beispiel: Verboten von Changes ohne Spezifikationen	781
Beispiel: Erlauben von Rogue-Einfügungen aus ausgewählten Quellen	782

Beispiel: Erlauben einer Rogue-Aktualisierung für ein CI, dass nicht zur Produktion gehört	782

Kapitel 17: Verwalten von MDRs 875

Was ist ein MDR?	785
MDR-Klassen und MDR-Namen	786
Wie ergänzt ein MDR CA SDM?.....	786
Definition eines MDR für CA SDM.....	787
MDR Launcher	787
Definieren einer URL zum Starten eines MDR	788
Einrichten eines CA APM-MDR-Providers	790
Starten im Kontext von CA CMDB an CA APM	790
Eigenschaften von Configuration Items, die MDR-Zusammenschluss unterstützen	791
Föderierte Anlagen-ID	791
MDR-Name.....	792
MDR Class.....	792
MDR-Definition bei der Installation von CA Cohesion ACM	792
CA Cohesion ACM MDRs	793
Manuelles Verknüpfen eines MDR mit einem CI	795
Automatischer Import aus CA Cohesion	795
Zuordnung von CI zu MDR	795
Verwalten der MDR-Definition	797
CA Cohesion ACM-Bericht.....	797
Mit GRLoader	798
Namenskonventionen und Einschränkungen für Configuration Items	798
Namenskonventionen für system_name	799
Verwenden des CMDBf-Viewers	801
Aktualisieren von Metadatendateien für die CMDBf-Zuordnung	801
Anzeigen von MDR-Attributwerten mit CA CMDB-Attributnamen.....	803
Ausblenden von Attributen des MDR-Providers	804
Definieren von MDR-Attributen ohne CA CMDB-Entsprechungen	805
Definieren von Metadaten des CMDBf-Datenanbieters	805

Kapitel 18: Change Management 807

Change Management in CA SDM	807
Change-Management-Komponenten	808
Anzeigen des Change-Kalenders	809
CAB-Zuständigkeiten	810
Funktionsweise der CAB-Prozessdefinitionen.....	810
Zuweisen von Mitgliedern zur CAB-Gruppe.....	811
Zuständigkeiten des Change Managers	811
Funktionsweise der Rolle des Changes Managers	812

Definieren der Aufgaben für die Rolle des Change Managers	813
Change-Kategorien, Status und Risikoebenen	814
Anzeigen des Change-Scoreboards	815
Definieren von gespeicherten Abfragen für Changes	815
Konfigurieren von Change Manager-Optionen	817
Change-Kalender	817
Hinzufügen von Ablaufplaninformationen zu einem Change	818
iCalendar-Event-Vorlagen	818
Exportieren von Ablaufplänen in iCalendar	819
Ablaufplan-Ansichten	820
Konfigurieren von Planungsansichten	822
So planen Sie Changes:.....	830
Beispiel: Verwenden des Change-Schedulers	831
So planen Sie Change-Fenster:.....	835
Anzeigen von Change-Fenstern	836
Zuordnen eines CIs zu einem Wartungsfenster	837
Anzeigen von zugeordneten CIs	837
Erstellen eines Beispiel-Sperrfensters.....	838
Erstellen eines globalen Wartungsfensters.....	839
Konfliktanalyse und Konflikterkennung	839
CA Workflow-Visualisierung	840
So visualisieren Sie den Workflow:	840
Change-Management-Prozessdefinition für CA Workflow	842
Komponenten der Change-Management-Prozessdefinition	843
Einrichten der Change Management-Vorgangsdefinition	843
Funktionsweise der Change Management-Prozessdefinitionen.....	849
ActivityNode Actor not found: Update Object -Service Desk r12 ("ActivityNode"-Akteur nicht gefunden: Objekt -Service Desk r12 aktualisieren")	864
Change wird nicht geschlossen	865
CAB-Konsole und Berichterstattung.....	865
Verwalten von CAB-Gruppen	866
Zuweisen von CAB-Gruppen	868
CAB-Genehmigungen	868
Ändern der CAB-Konsoleneigenschaften	869
Change Management-Berichterstellung	870
Risikobewertung.....	871
So implementieren Sie die Risikoumfrage:	872
Zugreifen auf eine Risikoumfrage direkt über eine URL	874
Auswirkungs-Explorer	875
Starten von Auswirkungs-Explorer.....	876
Untersuchen von angehängten CIs	876
Anzeigen von CIs in Auswirkungs-Explorer	877

Hinzufügen von verwandten CIs zu Changes	877
Anzeigen der Liste der nachfolgenden Elemente des CI	878
Starten von CMDB Visualizer im Auswirkungs-Explorer	878
Konfigurieren von Auswirkungs-Explorer	879

Kapitel 19: Verwalten von Berichten 881

Kapitel 20: CA Business Intelligence-Berichte 883

Berichterstellungsszenarios	883
Berichtskomponenten	884
Berichtsdatenflussdiagramm	887
Anzeigen von webbasierten Berichte in InfoView	888
Sicherheit und Autorisierung	889
Gruppen und Anwender	889
CA SDM-Datenpartitionen in Infoview	890
Universum und Verbindungen mit einem Universum	891
Berichtsordner	891
Zugriffsebenen	893
Verweisen eines vorhandenen CA Business Intelligence-Servers auf einen CA SDM-Server	895
Erstellen einer ODBC-Datenquelle	895
Konfigurieren des Universums	896
Exportieren des Universums	897
Einrichten der Datenaufteilungssicherheit für die Berichterstellung	897
Hinzufügen des privilegierten CA SDM-Anwenders zu CMC	898
Definieren der Universe-Datenbank-Anmeldeinformationen	898
Einrichten von Datenaufteilungen	899
Replizierte Datenbank für Offline-Berichterstellung	899
Rollenbasierte Berichte	900
Definieren rollenbasierter Berichte für die Rolle	900
Anzeigen neuer Berichte auf der Registerkarte 'Berichte'	902
Webbasierte Berichte	909
Business Objects InfoView-Schnittstelle	909
Navigieren zu Berichten	910
InfoView-Voreinstellungen	910
Planen von Berichten	910
Einrichten der Datenanalyse	911
Veröffentlichen und Verteilen von Berichten	912
KPIs (Kritische Prozess-Indikatoren)	912
KPI-Typen	912
Vordefinierte KPIs	913
KPI-Daemon	913

System-KPIs	914
Gespeicherte Abfrage-KPI	916
SQL KPIs	916
KPI - Felder	918
Abrufen von Ticket-Daten	919
Fehlerbehebung	922
Ad-hoc-Berichte	924
Web Intelligence-Schnittstelle	925
Funktionsweise der Ad-hoc-Berichterstellung	925
Ad-hoc-Beispielberichte	926
Beispiel: Anzeigen aller offenen Requests mit Priorität 1 und 2 für alle Anwender	926
Beispiel: Anzeigen aller offenen Requests, deren Status nicht "In Bearbeitung" ist.	928
Beispiel: Anzeigen aller in den letzten 30 Tagen geschlossenen Requests für Anwender, deren Nachname mit "C" beginnt.	930
Dashboard-Berichte	932
Anzeigen von Dashboards und Berichten in InfoView	933
Schreiben von CA Business Intelligence-Berichten	933
CA SDM-ODBC-Treiber	933
Schreiben von SQL für BusinessObjects-Berichte	934
PDM-Funktionen	935
Attributaliasnamen	938
pdm_isql - interaktives SQL	938

Kapitel 21: Generieren von Berichten in USDK 941

Berichte erzeugen	941
Datenbankansichten	941
Grundlegende Ansichten	942
Erweiterte Ansichten	944
Einrichten von Berichtsmethoden	945
Berichtsformatierung	945
Ändern der Sortierreihenfolge der Spalten	946
Zusammengefasste Berichte und Detailberichte	946
Analyseberichte	947
Generieren von Berichten zu Requests und Issues	947
Generieren von Berichten zu Request-Bereichen und Issue-Kategorien	948
Erstellen von Berichten zur Priorität von Anforderungsbereichen und zur Priorität von Issue-Kategorien	948

Kapitel 22: Verwalten von Knowledge 949

Knowledge Management	949
Suchen von Prozeduren für das Knowledge Management	950

Knowledge und Mandantenfähigkeit	950
So richten Sie eine Knowledge Base ein:	951
Importieren von Knowledge-Beispieldaten	951
Überwachen der Knowledge Base	952
Neuindizierung der Knowledge Base	952
Indizieren der Warteschlangeneinstellungen für Batch-Verarbeitung und sofortige Verarbeitung bzw. Entfernen der Indizierung	953
So verwenden Sie Dokumente in der Knowledge Base:	954
Knowledge-Einreichung in CA SDM	955
Knowledge-Einreichung über Self-Service	956
Dokument-Attribute	956
Dokumentberechtigungen	956
Bearbeiten der Lösung	957
Vorbereiten der Dokumentveröffentlichung	957
Dokumentveröffentlichung	958
Versionsdokumente	958
Dokumentablauf	959
Archivieren und Bereinigen von Dokumenten	960
Knowledge-Suche	960
So rufen Sie das CAFedSearch-Servlet über einen REST-Webservice auf	961
Foren	962
Knowledge-Baumstrukturdokumente	962
Knowledge-Dokument-Ablaufplan	963
Knowledge - Ablaufplanfilter	963
Ansichten von Knowledge-Ablaufplänen	965
Konfigurieren von Planungsansichten	966
Zugreifen auf Export/Import	973
So exportieren/importieren Sie Knowledge:	974
Exportieren/Importieren von Dokumenten	978
Exportieren/Importieren von Paketen	978
Anzeigen von Export-/Importvorlagen	980
Hilfsprogramm "pdm_ket": Knowledge-Export-Tool	987
Hilfsprogramm "pdm_kit": Knowledge- Import-Tool	988
Exportieren oder Importieren von Knowledge durch Benutzer	989
Webservices	990

Kapitel 23: Verwalten von Knowledge Management 991

Knowledge-Verwaltung	991
Suchen von Prozeduren für die Knowledge-Administration	992
Rollen und Funktionen von Knowledge Management	992
Knowledge Management-Benutzeroberflächen	993

Konfiguration und Verwaltungsfunktionen von Knowledge Management	994
Optionen für Self-Service-Knowledge	995
Dokumente und Anwender	1000
So verwalten Sie Rollenberechtigungen und die Dokumentsichtbarkeit:	1004
Aktionsinhalte	1004
Anzeigen von Aktionsinhalten	1006
Erstellen von Aktionsinhalten (Aktions-URL)	1007
Erstellen von Aktionsinhalt (interner HTML)	1008
Bearbeiten von Aktionsinhalten	1008
Suchen nach Aktionsinhalten	1009
Genehmigungsvorgang für Dokumente	1010
Manager für den Genehmigungsvorgang	1011
Festlegen eines Genehmigungsvorgangs für die Dokumentbearbeitung	1012
Erstellen einer Genehmigungsprozessvorlage	1013
Definitionen für den Dokumentstatus	1016
Automatisierungsrichtlinien	1018
Anzeigen von Automatisierungsrichtlinien	1018
Einrichten von Automatisierungsrichtlinien	1020
Erstellen von Automatisierungsrichtlinien	1020
Bearbeiten von Automatisierungsrichtlinien	1021
Planen von Automatisierungsrichtlinien	1021
Anzeigen von Berichten zu Lebenszyklusrichtlinien für Dokumente	1022
Knowledge-Dokumentsteuerung	1023
Kommentartypen	1024
Dokumentvorlagen	1030
Erstellen von Verknüpfungen für Knowledge-Dokumente	1038
Knowledge-Kategorien	1041
Berichte und Indikatoren	1051
Suchen	1053
Lösungsumfrage	1080
Knowledge Management-Systemeinstellungen	1083
Konfigurieren von allgemeinen Einstellungen	1083

Kapitel 24: Verwalten von Support-Automatisierung 1087

Automatisieren des Supports in Ihrer Umgebung	1087
Live-Unterstützung	1088
Verwalten von Support-Automatisierung-Analysten	1090
Einführung	1091
So konfigurieren Sie die Live-Unterstützung für Analysten	1092
Starten der Live-Unterstützung durch Analysten	1101
Konfigurieren von Live-Unterstützung für Analysten	1102

Verbinden von Endbenutzern mit Unterstützungssitzungen	1103
Wie Analysten die Unterstützung für Endbenutzer automatisieren	1104
Bereitstellen der Live-Unterstützung durch Analysten	1105
Support-Automatisierung-Anwenderverwaltung	1105
Konfigurieren von Rollenberechtigungen	1106
Support-Automatisierung anonyme und registrierte Benutzer	1107
So legen Sie die Support-Automatisierung für einen Gastanwender fest	1108
Verwalten der Support-Automatisierung-Zugriffsebenen	1111
Support-Automatisierung-Aktivitätsbenachrichtigungsverwaltung	1112
Support-Automatisierung-Seitenanpassungen	1113
Branding-Verwaltung	1114
Verwalten der Lokalisierung	1114
Seitenlayoutkonfiguration	1115
Support-Automatisierung-Systemeigenschaften	1115
Support-Automatisierung-Warteschlangenverwaltung	1116
Warteschlangenverwaltung	1116
Verwalten von Warteschlangen-Zusammenfassungen	1117
Verwalten der Warteschlangen-Stunden	1118
Verwaltung von Ticket-Vorlagen	1118
Administrationseinstellungen	1118
So konfigurieren Sie die Support-Automatisierung-Einstellungen:	1119
Anpassen von Support-Automatisierung-Tools	1121
Automatisierte Aufgaben	1121
Verwalten von Chat-Voreinstellungen	1127
Standardanmeldeinformationen	1128
Disclaimer	1128
Sitzungsprotokoll-Verwaltung	1129
Anzeigen des Sitzungsprotokolls	1129
Support-Automatisierung-Berichte	1130
Empfangen eines Ticket-Request	1132
Einladen des Endanwenders zu einer Unterstützungssitzung	1132
Lösen eines Tickets in einer Chat-Sitzung	1133
Live-Unterstützung	1134
Beenden der Unterstützungssitzung und Schließen des Tickets	1135

Kapitel 25: So identifizieren Sie Leistungsprobleme in CA SDM **1135**

Definieren des Leistungsproblems	1138
Überprüfen der Voraussetzungen	1139
Installieren der Ps-Tools für Windows	1139
Erfassen der Informationen über das CA-Tool für Diagnoseberichte	1140
Ausführen des CA-Tools für Diagnoseberichte	1140

Überprüfen der Windows-Berichte.....	1142
Überprüfen der UNIX-Berichte	1143
Überprüfen der gesammelten Diagnoseberichte	1144
Erfassen von Details zur Umgebung des Datenbankservers	1145
Erfassen Sie Leistungsdaten von CA SDM-Servern.....	1146
Erfassen von Nutzungsdaten mithilfe der Intervallprotokollierung.....	1147
Lesen der allgemeinen Optimierungsempfehlungen	1150

Anhang A: Referenzbefehle 1151

bop_sinfo – Systeminformationen anzeigen.....	1152
dbmonitor_nxd – Daemon zur Überwachung von Datenbanken	1153
pdm_backup – Exportieren der Datenbank in eine ASCII-Datei	1155
pdm_cache_refresh – Aktualisieren der Datenbank.....	1156
pdm_configure – Öffnen des Konfigurationsfensters	1158
pdm_d_refresh – Starten fehlgeschlagener Daemons.....	1158
pdm_deref – Dereferenzieren von ASCII-Daten.....	1159
pdm_discimp – Importieren ermittelter Assets	1163
pdm_discupd – Asset-Aktualisierung ermittelt.....	1165
pdm_extract – Extrahieren von Daten aus der Datenbank.....	1165
pdm_halt – Beenden von Daemons oder Anhalten von Diensten	1169
pdm_init – Starten von Daemons	1169
pdm_key_refresh – Aktualisieren von im Cache gespeicherten Schlüsselinformationen	1170
"pdm_lexutil" – CA SDM-Lexika ändern.....	1170
"pdm_k_reindex" – Dienstprogramm zur Knowledge-Neuindizierung	1172
Verwenden von pdm_k_reindex.....	1173
Verfolgen der Neuindizierung	1174
Importieren und Neuindizieren	1174
Indizieren der Warteschlangeneinstellungen für Batch-Verarbeitung und sofortige Verarbeitung bzw. Entfernen der Indizierung	1175
pdm_listconn – Auflisten der aktiven Verbindungen.....	1176
pdm_load – Hinzufügen, Aktualisieren und Löschen von Datenbank-Datensätzen	1178
pdm_logfile – Ändern der Cutover-Größe von STDLog	1180
pdm_log4j_config-Hilfsprogramm: Ändern der log4j-Eigenschaftsdatei.....	1181
Beispiele für die Verwendung des Hilfsprogramms	1183
Manuelles Ändern Sie des Aktualisierungsintervalls der Protokolldatei	1184
Ändern des Appenders jsrvr.log.....	1185
Ändern des Appenders jstd.log.....	1185
pdm_proctor_init – Starten von Proctor auf sekundären Servern	1186
pdm_replace – Ersetzen einer Datenbanktabelle	1186
pdm_rest_util: Verwalten der CA SDM-Webservices-Anwendung RESTful	1188
Aufheben der Bereitstellung der REST-Webservices-Anwendung.....	1189

pdm_restore – Wiederherstellen einer Datenbank	1189
pdm_status – Anzeigen des Status von Daemons oder Prozessen	1191
pdm_task – Einstellen der Umgebungsvariablen	1192
pdm_text_cmd – Befehlszeilenschnittstelle für Text-API	1192
Beispiele für Eingaben.....	1195
pdm_uconv – Konvertiert den lokalen Zeichensatz in UTF-8.....	1196
pdm_userload – Hinzufügen, Aktualisieren und Löschen von Datenbank-Datensätzen	1199
pdm_webstat – Zurückgeben von Webnutzungsstatistiken	1201
report – Generieren von Berichten	1205
rpt_srv – Generieren von Berichten.....	1206
uniconv – Starten des UNIX CA NSM-Event Converter-Daemons	1208
Dienstprogramm "pdm_mail" - Senden von E-Mail-Informationen	1209
pdm_server_control Utility--Identify Servers	1211

Anhang B: Beschreibungen der Felder in Ansichten 1213

Beschreibungen der Felder in Ansichten	1214
View_Act_Log.....	1214
View_Audit_Assignee.....	1216
View_Audit_Group.....	1216
View_Audit_Priority	1217
View_Audit_Status	1218
View_Change_Act_Log.....	1218
View_Change.....	1220
View_Change_to_Assets	1225
View_Change_to_Change_Act_Log	1225
View_Change_to_Change_WF.....	1227
View_Change_to_Properties	1229
View_Contact_Full	1230
View_Contact_to_Environment.....	1233
View_Group	1234
View_Group_to_Contact.....	1235
View_Issue	1235
View_Issue_Act_Log.....	1240
View_Issue_to_Assets.....	1241
View_Issue_to_Issue_Act_Log	1242
View_Change_to_Request	1243
View_Issue_to_Issue_WF.....	1247
View_Issue_to_Properties	1249
View_Request	1250
View_Request_to_Act_Log	1255
View_Request_to_Properties	1255

Anhang C: Formulargruppen **1257**

Formulargruppe "Kunden"	1257
Formulargruppe "Mitarbeiter"	1258
Formulargruppe "Analysten"	1260

Anhang D: LDAP-Ergebniscodes von RFC 2251 **1283**

LDAP-Rückgabecodes	1283
Rückgabecodes des LDAP-Servers	1283
Rückgabecodes des LDAP-Clients	1289
LDAP-spezifische RFC-Standards	1291

Kapitel 1: Einführung

Dieses Kapitel enthält folgende Themen:

[Zielgruppe](#) (siehe Seite 25)

[Was Sie wissen müssen](#) (siehe Seite 25)

[Dienstverwaltungsprozesse und bewährte Praktiken](#) (siehe Seite 26)

Zielgruppe

Dieses Handbuch richtet sich an den CA Service Desk Manager-Administrator (CA SDM), d. h. die Person, die die gesamte Verantwortung für die Verwaltung des Produkts hat. Einige Aufgaben, die der Administrator ausführt, sind Folgende:

- Starten und Anhalten der für den CA SDM-Server erforderlichen Dienste
- Einrichten verschiedener Systemkomponenten
- Festlegen der Optionen, die Anwendern zur Verfügung stehen.
- Generieren von Berichten auf der Basis der Service Desk-Daten

Zweck dieses Handbuchs ist es, den Administrator bei seiner Arbeit mit CA SDM zu unterstützen, um die Dienstübermittlung zu implementieren, zu verwalten und durchzusetzen. Dieses Handbuch ist für jeden nützlich, der verstehen möchte, wie das Produkt die Herausforderung einer kompletten Automatisierung und Verwaltung der Dienstübermittlung löst, von der Entstehung bis zur Behebung von Problemen.

Was Sie wissen müssen

Für eine erfolgreiche Verwaltung von CA SDM sollten Sie mit Folgendem vertraut sein:

- Betriebsumgebung, auf der CA SDM installiert ist.
- Betrieb Ihres Webservers
- Grundlegende Administrationsaufgaben

Im Handbuch wird davon ausgegangen, dass das Produkt entsprechend den Informationen im *Implementierungshandbuch* korrekt installiert worden ist.

Dienstverwaltungsprozesse und bewährte Praktiken

Die Implementierung bewährter Praktiken und standardisierter Verfahren hat direkte Auswirkungen auf Effizienz, Produktivität und Kosten der Service Support-Umgebung. CA bietet eine Bibliothek empfohlener Prozesse und bewährter Praktiken für das Service Management, die im Einklang mit Industriestandards und anerkannten Best Practices-Rahmen einschließlich ITIL, CobIT, BS15000 und weitere steht. Die für CA SDM beschriebenen Prozesse umfassen:

- Vorfallverwaltung
- Problemverwaltung
- Change Management
- Anforderungsverwaltung
- Configuration Management
- Versionsverwaltung
- Knowledge Management
- Support-Automatisierung

Hinweis: Informationen zur Best Practices-Bibliothek sind online verfügbar. Informationen zu den Best Practices von CA für Service Management sowie White Paper und andere Materialien finden Sie unter <http://www.ca.com/sm/bp> <http://www.ca.com/sm/bp>. Fachkundige Partner von CA für strategische Prozesse können Ihnen dabei helfen, die Best Practices-Bibliothek für Ihre Organisation zu personalisieren.

Kapitel 2: Verwalten von Servern

Dieses Kapitel enthält folgende Themen:

- [Anzahl der Server](#) (siehe Seite 27)
- [So ändern Sie eine Serverkonfiguration](#) (siehe Seite 28)
- [So starten Sie die CA SDM-Server](#) (siehe Seite 28)
- [So führen Sie parallele Serverwartung auf CA SDM-Servern aus](#) (siehe Seite 32)
- [So konfigurieren Sie SSL-Authentifizierung](#) (siehe Seite 39)
- [So konfigurieren Sie TCP/IP](#) (siehe Seite 51)
- [Bereitstellen von CMDBf-Webservices](#) (siehe Seite 52)
- [So starten Sie die CA SDM-Server neu](#) (siehe Seite 52)
- [So halten Sie die CA SDM-Server an](#) (siehe Seite 56)
- [Unterstützte Tablets](#) (siehe Seite 59)
- [Tomcat-Protokollierung](#) (siehe Seite 61)
- [PDA-Schnittstelle](#) (siehe Seite 62)
- [REST-Protokollierung](#) (siehe Seite 63)
- [So konfigurieren Sie Prozesse für CA SDM-Server](#) (siehe Seite 70)

Anzahl der Server

Ihre CA SDM-Installation hat eine oder mehrere Serverkomponenten, die ein Administrator verwalten kann. Die Anzahl der Server hängt von der CA SDM-Konfiguration ab:

- Konventionell: Ein Primärserver und ein oder mehrere Sekundärserver.
- Erweiterte Verfügbarkeit: Ein Hintergrundserver, ein oder mehrere Standby-Server und ein oder mehrere Anwendungsserver.

Nach der Installation von CA SDM müssen Sie jeden Computer, auf dem Produktkomponenten ausgeführt werden, konfigurieren. Sie können die Server-Konfiguration als Teil des Installationsprozesses ausführen oder später ausführen. Die CA SDM-Dienste müssen neu gestartet werden, nachdem Sie die Serverkonfiguration geändert haben.

Weitere Informationen über das Planen und Konfigurieren von Servern finden Sie im *Implementierungshandbuch*.

So ändern Sie eine Serverkonfiguration

Als Administrator konfigurieren Sie alle Server der CA SDM-Installation. Die Anzahl und die Typen der Server hängen von der CA SDM-Konfiguration ab. Die anfängliche Konfiguration ist Teil des CA SDM-Installationsprozesses.

Hinweis: Eine Änderung in der Systemumgebung kann eine Änderung der Serverkonfiguration erforderlich machen. Zum Beispiel: Änderungen im Datenbankmanagementsystem oder die Integration mit einem Webserver, wie z. B. Tomcat, oder die Integration mit CA EEM.

Mit dem Konfigurationsdienstprogramm können Sie Änderungen an einer Serverkonfiguration vornehmen. Weitere Informationen zur Serverkonfiguration finden Sie im *Implementierungshandbuch*.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei dem Server an, den Sie erneut konfigurieren möchten.
2. Wählen Sie im Windows-Startmenü "Programme", "CA", "CA SDM" und anschließend "Konfiguration".

Das Dienstprogramm für die CA SDM-Konfiguration wird geöffnet.

3. Füllen Sie die erforderlichen Felder aus, und klicken Sie auf "Weiter".

Im Bereich auf der rechten Seite werden die entsprechenden Felder für die Verknüpfung angezeigt, die im Navigationsbereich links markiert wurde.

4. Folgen Sie den Anweisungen auf dem Bildschirm, um die Installation abzuschließen, und klicken Sie auf "Fertig stellen".

Die Serverkonfiguration wurde geändert.

So starten Sie die CA SDM-Server

Führen Sie abhängig von Ihrer CA SDM-Konfiguration folgende Aktionen durch:

- [Starten Sie die CA SDM-Server in konventioneller Konfiguration](#) (siehe Seite 30)
- [Starten Sie die CA SDM-Server in der Konfiguration für erweiterte Verfügbarkeit](#) (siehe Seite 31).

Folgende Tabelle beschreibt die Prozesse, die automatisch starten, nachdem Sie die CA SDM-Server starten:

Prozess	Beschreibung
Daemon Agent (pdm_proctor_nxd)	Der Daemon Agent ist für das Starten der verwalteten Daemons verantwortlich.
Daemon Monitor (pdm_d_mgr)	Überwacht Daemon-Prozesse.

Prozess	Beschreibung
BOP Virtual DB (bpvirtodb_srvr)	BOP Virtual-Datenbankserver
Datenlexikon (ddictbuild)	Erstellt das Datenlexikon bei jedem Systemstart. Dieses wird ausgeführt und dann beendet
KPI Daemon (kpi_daemon)	Verwaltet die Erfassung, Organisation und Speicherung von KPI-Daten.
Oracle-Agent (orcl_agent)	Agent für Oracle-Datenbank - viele Instanzen, je nach Last
Oracle-DB (orcl_prov_nxd)	Oracle-Datenbankanbieter
SQL Agent (sql_agent) (Ausführung nur bei Verwendung von MS SQL)	Agent für SQL Server-Datenbank - viele Instanzen, je nach Last
SQL DB (sql_prov_nxd) (Ausführung nur bei Verwendung von MS SQL)	Microsoft SQL Server-Datenbankanbieter
Event Manager (ehm_nxd)	Event-Manager
Message Dispatcher (sslump_nxd)	Stellt Meldungen zu.
Notification Manager (bpnotify_nxd)	Verwaltet Benachrichtigungen
Object Engine (domsrvr)	CA SDM-Objektmanager
Report Manager (pcrpt_nxd)	PC-Berichterstellung
Software Version Control (pdm_ver_nxd)	Verwaltet Versionen angegebener Systemkomponenten.
Method Engine (spel_srvr)	Rechtschreibcode-Interpretationsserver
Text API (pdm_text_nxd)	Text-API-Daemon für E-Mail- und CA NSM-Schnittstellen
Timed Events/Notifications (animator_nxd)	Zeit-Events und Benachrichtigungen
User Validation (boplogin)	Validierung für Anwenderkonto
Anwenderauthentifizierung (bopauth)	Authentifizierung für Anwenderkonto
Web Engine (webengine)	Führt die Engine für den Webclient aus
Archive Purge Daemon (arcpur_srvr)	Verwaltet die Hintergrundverarbeitung von Archivierungs- und Löschvorgängen
BU Daemon (bu_daemon)	Wickelt die Ermittlung der FAQ-Bewertung für Knowledge-Dokumente ab
DB Monitor (dbmonitor_nxd)	Überwacht allgemeine Tabellen von CA in Bezug auf Änderungen
EBR Daemon (bpebr_nxd)	Wickelt Knowledge-Suchanfragen ab

Prozess	Beschreibung
EBR Idx Daemon (bpeid_nxd)	Wickelt die Indizierung/Neuindizierung für das EBR-Schlüsselwort ab
KRC Daemon (krc_daemon)	Verwaltet statistische Berechnungen und Benachrichtigungen für die Knowledge-Berichtskarte
KT Daemon (kt_daemon)	Verwaltet Knowledge-Dokumente (KD-Genehmigungsvorgang, Berechtigungen, Benachrichtigungen usw.)
LDAP vrtddb (ldap_vrtddb)	Agent für die Kommunikation mit LDAP-Servern
Mail Daemon (pdm_mail_nxd)	Wickelt ausgehende E-Mail-Benachrichtigungen ab
Mail Eater (pdm_maileater_nxd)	Wickelt eingehende E-Mail-Benachrichtigungen ab
MDB Registration Server (mdb_registration_nxd)	Agent zur Abwicklung von MDB-Registrierungsanfragen
PDM RPC (PDM_RPC)	Verwaltet die Webservices-Requests
Repository Daemon (rep_daemon)	Verarbeitet Repositorys für Anhänge
Spell checker (lexagent_nxd)	Verarbeitet Anfragen zur Rechtschreibprüfung
Time-to-Violation (ttv_nxd)	Vorhersage von SLA-Verletzungen
tomcat controller (pdm_tomcat_nxd)	Verwaltet Tomcat-Services

Hinweis: In dieser Tabelle bezieht sich der Benachrichtigungs-Manager-Prozess nur auf Windows-Umgebungen und der Standard-DB-Prozess nur auf UNIX-Umgebungen.

Starten der CA SDM-Server in konventioneller Konfiguration

Starten Sie die Server in folgender Reihenfolge:

1. [Starten des Sekundärservers](#) (siehe Seite 30).
2. [Starten des Primärservers](#) (siehe Seite 31).

Starten des Sekundärservers

Wenn Ihre Installation einen oder mehrere Sekundärserver umfasst, müssen Sie diese vor dem Primärserver starten.

Gehen Sie wie folgt vor:

- (Windows) Wählen Sie Dienste über die Systemsteuerung aus, wählen Sie den Dienst CA SDM-Remote-Überwachung aus, und klicken Sie auf Starten.
- (UNIX) Verwenden Sie "pdm_init" in der Befehlszeile.

Weitere Informationen:

[pdm_proctor_init – Starten von Proctor auf sekundären Servern](#) (siehe Seite 1186)

Starten des primären Servers

Jede CA SDM-Installation hat einen Primärserver, der die grundlegende Produktfunktionalität abwickelt.

Wichtig! Wenn Ihre Installation einen oder mehr sekundäre Server einschließt, müssen Sie die [Sekundärserver](#) (siehe Seite 30) vor dem Primärserver starten.

Gehen Sie wie folgt vor:

- (Windows) Wählen Sie Systemsteuerung aus, wählen Sie den Dienst CA SDM-Server aus, und klicken Sie auf Starten. Sie können den Dienst jederzeit starten, oder Sie können ihn so konfigurieren, dass er wie jeder andere Windows-Dienst automatisch gestartet wird.
- (UNIX) Verwenden Sie "pdm_init" in der Befehlszeile.

Starten der CA SDM-Server in der Konfiguration für erweiterte Verfügbarkeit

Starten Sie die Server in folgender Reihenfolge:

Hinweis: (Windows) Wählen Sie Systemsteuerung aus, wählen Sie den Dienst CA SDM-Server aus, und klicken Sie auf Starten. Sie können den Dienst jederzeit starten, oder Sie können ihn so konfigurieren, dass er wie jeder andere Windows-Dienst automatisch gestartet wird. (UNIX) Verwenden Sie "pdm_init" in der Befehlszeile.

1. Starten des Hintergrundservers.
2. Starten der Standby- und Anwendungsserver (in beliebiger Reihenfolge).

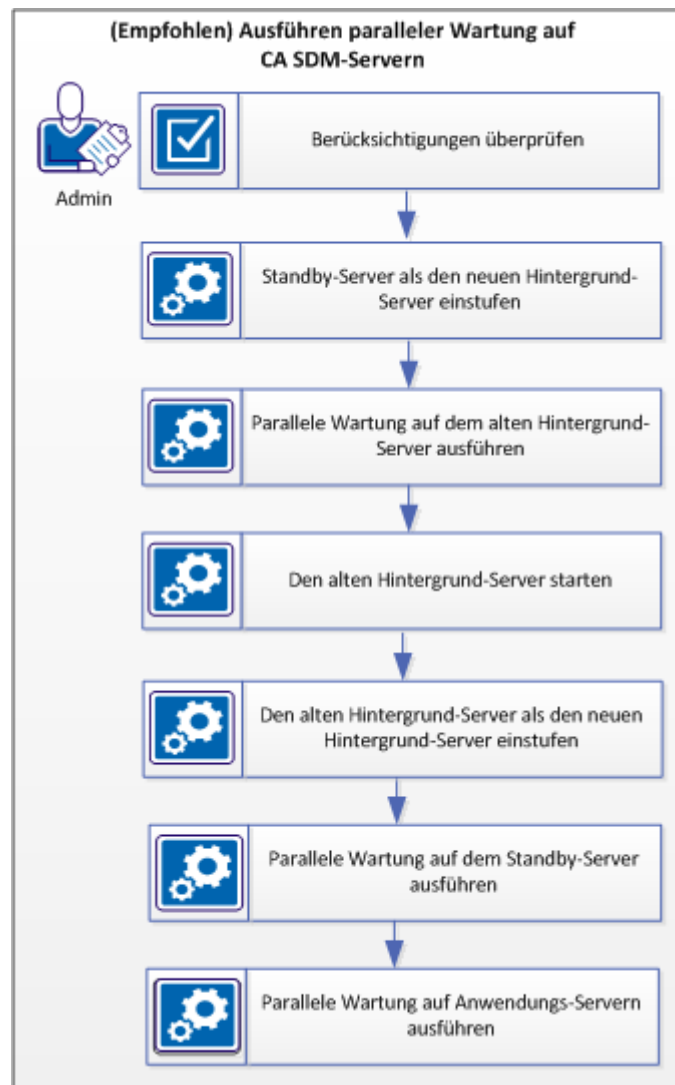
So führen Sie parallele Serverwartung auf CA SDM-Servern aus

Als Systemadministrator führen Sie die parallele Serverwartung auf CA SDM-Servern aus. Diese Wartung kann ausgeführt werden, um Patches anzuwenden oder um eine allgemeine Wartung der Server auszuführen. Wir empfehlen Ihnen, die Wartung aller Server in einer spezifischen Reihenfolge auszuführen. Dieser Vorgang stellt sicher, dass alle Server mit ähnlichen Änderungen aktualisiert werden, wobei minimale oder keine Unterbrechungen für den Endanwender auftreten. Für serverspezifische Änderungen, müssen nicht alle anderen Server aktualisiert werden.

Wichtig! Bevor Sie einen allgemeinen MDB-Patch oder einen BS- oder Sicherheits-Patch anwenden, müssen Sie alle CA SDM-Server herunterfahren. In diesem Fall wird der Anwendervorgang unterbrochen, und der Anwender hat keinen Zugriff auf CA SDM, bis alle Server wieder hochgefahren sind und ausgeführt werden. Wir empfehlen dem Systemadministrator, die Anwendung des Patch entsprechend zu planen.

Folgendes Diagramm zeigt den empfohlenen Vorgang, um eine parallele Wartung der CA SDM-Server auszuführen:

Hinweis: Abhängig von Ihren Organisationsstandards kann der parallele Wartungsvorgang in Ihrer Organisation vom empfohlenen Vorgang abweichen.



Gehen Sie wie folgt vor:

1. [Überprüfen Sie die Hinweise](#) (siehe Seite 34).
2. Halten Sie den Standby-Server an (den Sie als neuen Hintergrundserver hochstufen möchten).
3. Führen Sie die parallele Wartung auf dem Standby-Server aus.
4. [Unterdrücken Sie Versionskontrolle zwischen dem Standby-Server und dem Hintergrundserver](#) (siehe Seite 35).
5. Starten Sie den Sekundärserver.
6. [Stufen Sie den Standby-Server als neuen Hintergrundserver hoch](#) (siehe Seite 35).
7. Führen Sie die parallele Wartung auf dem alten Hintergrundserver aus.
8. Starten Sie den alten Hintergrundserver.
Wenn Sie den Hintergrundserver starten, dann wird der Server ein Standby-Server.
9. Führen Sie die parallele Wartung auf allen anderen Standby-Servern aus.
Hinweis: Halten Sie den Standby-Server an, führen Sie eine parallele Wartung aus, und starten Sie den Server.
10. [Führen Sie die parallele Wartung auf Anwendungsservern aus](#) (siehe Seite 36).

Überprüfen der Hinweise

Beachten Sie Folgendes, während ein Failover des Hintergrundservers zum Standby-Server durchgeführt wird:

- Die neuen Anwender können sich nicht anmelden.
- Während des Failovers werden folgende Aktionen bei bereits verbundenen Anwendern nicht funktionieren. Nach dem Failover muss der Anwender versuchen, diese Aktionen erneut durchzuführen:
 - Beim Erstellen von Tickets mit Anhängen.
 - Beim Herunterladen von Anhängen.
 - Suchen nach Knowledge-Dokumenten.
 - Beim Indizieren von neuen Knowledge-Dokumenten.
 - Bei eingehenden E-Mails.
 - Bei SLA-Events, die nicht ausgelöst werden, bis das Failover abgeschlossen ist.

Wichtig! Wenn Sie das Tool eines Drittanbieters so konfiguriert haben, dass Auto-Failover für die CA SDM-Server aktiviert ist, müssen Sie dies deaktivieren, bevor Sie mit der Rolling-Wartung.

Unterdrücken der Versionskontrolle zwischen dem Standby-Server und dem Hintergrundserver

Mit der CA SDM-Versionskontrolle können Sie die Systemanpassungen auf allen CA SDM-Servern verwalten. Stellen Sie sicher, dass Sie die Versionskontrolle auf dem Standby-Server unterdrücken, bevor Sie ihn starten. Dieser Vorgang stellt sicher, dass kein Upgrade der Standby-Server auf die Systemanpassungen des Hintergrundservers durchgeführt wird. Um die Versionskontrolle zu unterdrücken, führen Sie folgenden Befehl auf dem Standby-Server aus, auf dem Sie gerade ein Upgrade durchgeführt haben:

```
pdm_server_control -v
```

Hochstufen des Standby-Servers als neuen Hintergrundserver

Bevor Sie den Hintergrundserver anhalten, stufen Sie den Standby-Server (auf dem Sie ein Upgrade durchgeführt haben) als neuen Hintergrundserver hoch. Wenn Support-Automatisierung mit CA SDM installiert ist, dann informieren Sie die aktiven Support-Automatisierung-Anwender darüber, dass der Hintergrundserver heruntergefahren wird.

Gehen Sie wie folgt vor:

1. Führen Sie folgenden Befehl auf dem Hintergrundserver aus, sodass mithilfe von Support-Automatisierung alle aktiven Anwender benachrichtigt werden, ihre Arbeit zu speichern:

```
sa_server_notifier [-h] | [-q seconds] | [-c]
```

-h

Zeigt die Hilfeseite an.

-q seconds

Diese Option benachrichtigt einen lokalen Server (Hintergrundserver), eine Stilllegung in einem angegebenen Zeitintervall durchzuführen. Dieses Intervall ist die Anzahl von Sekunden, bevor der Server offline geschaltet wird. Diese Option kann nicht für einen Standby-Server oder einen Anwendungsserver verwendet werden.

-c

Diese Option bricht einen zuvor gesendeten Request zur Stilllegung ab.

Eine Pop-up-Meldung wird allen aktiven Anwendern angezeigt, die Support-Automatisierung verwenden. Diese Meldung weist die Anwender auf das Herunterfahren des Servers hin, und die verbleibende Zeit bis zum Herunterfahren des Servers wird angezeigt. Die Anwender müssen ihre Arbeit speichern und sich innerhalb der angegebenen Zeit abmelden.

2. Führen Sie folgenden Befehl auf dem Standby-Server aus, den Sie als neuen Hintergrundserver hochstufen möchten:

```
pdm_server_control -b
```

-b

Benachrichtigt einen lokalen Standby-Server, der in den Hintergrundserver gewechselt wird. Der Standby-Server muss bereits ausgeführt werden. Wenn der Server nicht ausgeführt wird, dann wird er gestartet, aber es wird kein Failover durchgeführt. Um ein Failover zu starten, führen Sie den Befehl erneut aus.

Der Hintergrundserver fährt automatisch herunter, und der Standby-Server wird als neuer Hintergrundserver hochgestuft. Diese Änderung wirkt sich nicht auf die Endanwendersitzungen aus. Die Aktualisierungen (sofern vorhanden), die sich in Bearbeitung befinden, werden gespeichert und aufgeschoben, bis der neue Hintergrundserver online geschaltet wird.

Ausführen der parallelen Wartung auf Anwendungsservern

Als Best Practice können Sie die parallele Wartung zuerst auf einem Anwendungsserver ausführen, auf dem die minimalen oder keine Anwender verbunden sind. Benachrichtigen Sie dann alle aktiven Anwender auf anderen Anwendungsservern, sich beim aktualisierten Server anzumelden. Danach können Sie die Wartung auf anderen Anwendungsservern ausführen. Durch diesen Vorgang wird sichergestellt, dass die Anwender nicht mehrmals zwischen Anwendungsservern verschoben werden.

Gehen Sie wie folgt vor:

1. [Wählen Sie einen Anwendungsserver aus, der wenig aktiv ist](#) (siehe Seite 36).
2. Halten Sie den wenig aktiven Anwendungsserver an, führen Sie die parallele Wartung aus, und starten Sie ihn.
Der Anwendungsserver wird mit allen Änderungen aktualisiert.
3. [Halten Sie den anderen Anwendungsserver an](#) (siehe Seite 37).
4. Führen Sie die parallele Wartung auf dem Anwendungsserver aus, und starten Sie ihn.
Der Anwendungsserver wird mit allen Änderungen aktualisiert.
5. Führen Sie die Schritte 3 und 4 für die anderen Anwendungsserver aus.
Alle Anwendungsserver werden mit allen Änderungen aktualisiert.

Auswählen des Anwendungsservers, der wenig aktiv ist

Sie wählen einen Anwendungsserver mit der geringsten Anwenderaktivität aus. Führen Sie folgenden Befehl auf jedem Anwendungsserver aus, um den Server auszuwählen, der keine oder nur wenige aktive Sitzungen hat.

`pdm_webstat`

Hinweis: Dieser Befehl erfasst nicht die SOAP- oder REST-Webservice-Sitzungen.

Anhalten der anderen Anwendungsserver

Sie benachrichtigen alle aktiven Anwender auf einem Anwendungsserver darüber, auf den am wenigsten aktiven Anwendungsserver zu wechseln, bevor Sie ihn anhalten. Stellen Sie sicher, dass Sie den Anwendungsserver, der am wenigsten aktiv ist, neu gestartet haben, bevor Sie alle Anwender dorthin verschieben.

Gehen Sie wie folgt vor:

1. (Empfohlen) Fordern Sie alle aktiven Support-Automatisierung-Analysten auf dem Anwendungsserver, den Sie anhalten möchten, dazu auf, ein Ticket in CA SDM mit ihren Sitzungsinformationen zu erstellen. Dieser Vorgang stellt sicher, dass die Sitzungsinformationen nicht verloren gehen. Zum Beispiel ist der Support-Automatisierung-Analyst in einer Sitzung mit einem Kunden, um einen Hardware-Issue zu lösen. In diesem Fall kann der Support-Automatisierung-Analyst einen Issue in CA SDM mit den Sitzungsinformationen erstellen, bevor der Anwendungsserver heruntergefahren wird.
2. Senden Sie eine Benachrichtigung (zum Beispiel eine E-Mail-Benachrichtigung) an alle aktiven Anwender auf dem Anwendungsserver, in der die Anwender aufgefordert werden, zum Anwendungsserver, der am wenigsten aktiv ist und den Sie gerade neu gestartet haben, zu wechseln. Diese Benachrichtigung kann die Details des aktualisierten Anwendungsservers enthalten.
3. Führen Sie folgenden Befehl auf dem Anwendungsserver aus:

```
pdm_server_control [-h] -q interval -s server_name
```

-h

Zeigt die Hilfeseite an.

-q *interval* -s *server_name*

Benachrichtigt einen lokalen Anwendungsserver oder einen Remote-Anwendungsserver, eine Stilllegung in einem angegebenen Zeitintervall durchzuführen. Dieses Intervall ist die Anzahl der Sekunden, bevor der Server offline geschaltet wird. Wenn man diese Option ohne `server_name` verwendet wird, dann wird der lokale Server zur Stilllegung benachrichtigt. Diese Option kann für einen Hintergrundserver oder einen Standby-Server nicht verwendet werden.

Eine Pop-up-Meldung wird allen aktiven Anwendern auf dem Anwendungsserver angezeigt. Die Meldung weist auf das Herunterfahren des Servers und auf die verbleibende Zeit bis zum Herunterfahren hin. Die Anwender müssen ihre Arbeit speichern und sich innerhalb dieser Zeit abmelden. Der Anwendungsserver wird nach der angegebenen Zeit angehalten. Die Anwender melden sich auf dem anderen Anwendungsserver an, um ihre Arbeit fortzusetzen. Der Support-Automatisierung-Analyst kann sich auf das Ticket beziehen und seine Arbeit fortsetzen.

Der Anwendungsserver wird erfolgreich angehalten.

So konfigurieren Sie SSL-Authentifizierung

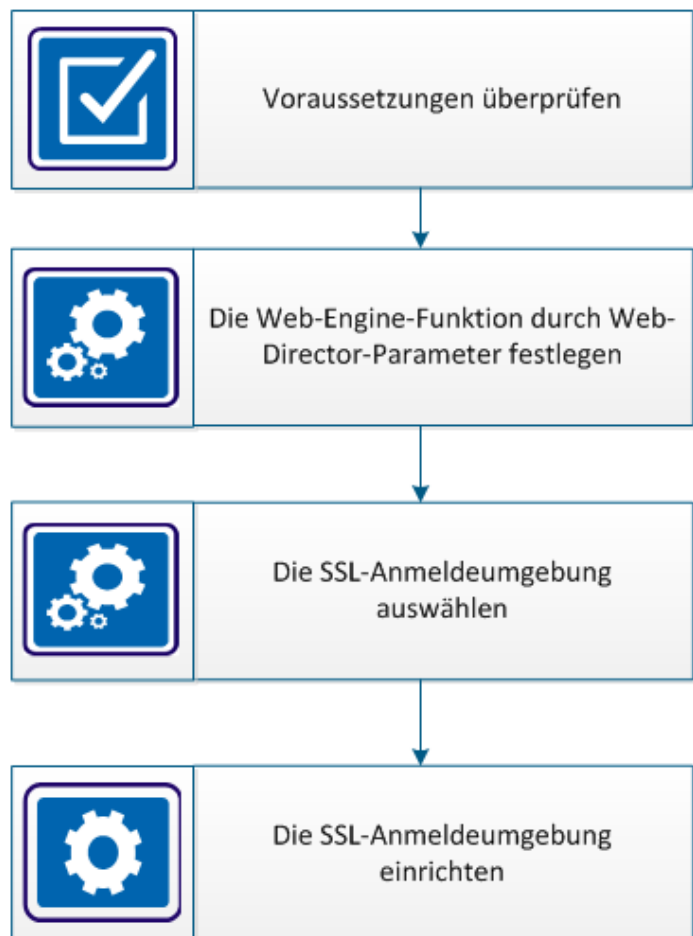
Als Systemadministrator können Sie den Web-Director konfigurieren, um Anmelde-Requests mithilfe des Protokolls "Secure Socket Layer" (SSL) in eine spezifische Web-Engine zu leiten. Durch das Konfigurieren der SSL-Authentifizierung wird eine erweiterte Anmeldesicherheit bereitgestellt. Gleichzeitig wird es den Anwendern ermöglicht, auf eine höhere Leistungsverbinding zuzugreifen.

Equation 1: So konfigurieren Sie SSL-Authentifizierung für CA SDM

Konfigurieren der SSL-Authentifizierung



System-admin



Weitere Informationen:

[Festlegen der Web-Engine-Funktion durch Web-Director-Parameter](#) (siehe Seite 40)

[Einrichten der SSL-Anmeldeumgebung](#) (siehe Seite 44)

[Auswählen der SSL-Anmeldeumgebung](#) (siehe Seite 41)

[Überprüfen der Voraussetzungen](#) (siehe Seite 40)

Überprüfen der Voraussetzungen

Überprüfen Sie die folgenden Voraussetzungen, bevor Sie die SSL-Konfiguration durchführen:

- CA SDM ist auf dem Server, auf dem Sie SSL implementieren möchten, installiert und konfiguriert.
- Mindestens zwei Web-Engines, die konfiguriert und an einen Web-Director zugewiesen sind. Weitere Informationen über das Konfigurieren von Web-Engines und Web-Directors finden Sie unter *So konfigurieren Sie Serverprozesse für CA SDM, um Leistungsszenarien zu verbessern*.

Festlegen der Web-Engine-Funktion durch Web-Director-Parameter

Nachdem Sie die Web-Engine zur Verwendung eines Web-Directors konfiguriert haben, kann die Web-Engine die Webclient-Requests verarbeiten. Die Web-Engine kann Anmelde-Requests (Nicht-Anmeldungen umleiten) oder Nicht-Anmelde-Requests (Anmeldungen umleiten) oder beides ("allgemeiner Zweck" der Web-Engine) bedienen. Der Parameter "WebDirector", der sich in der Datei "<Host_Name>-web[#].cfg" befindet, legt fest, wie die Web-Engine Anmelde-Requests bedienen kann.

Folgende Tabelle zeigt die Beziehung zwischen der Web-Engine-Rolle und der Web-Director-Parametereinstellung an:

Web-Engine-Funktion	WebDirector-Parametereinstellungen in <Host_Name>-web[#].cfg
Anmeldeanforderungen bedienen	UseDirector AfterLogin; Willingness 0
Nicht-Anmeldeaktivität bedienen	UseDirector BeforeLogin; Willingness [1 thru 10]
Universell	UseDirector Yes; Willingness [1-10]

Auswählen der SSL-Anmeldeumgebung

Sie können den Web-Director für eine gezielte SSL-Anmeldung in einer gemischten SSL-/Nicht-SSL-Webumgebung verwenden, um jeden Web-Anmelde-Request an die spezifischen SSL-Web-Engines umzuleiten. Alle anderen Requests können umgeleitet und von den Nicht-SSL-Web-Engines bedient werden.

Wählen Sie aus folgender SSL-Anmeldeumgebung aus:

- Nicht-SSL-Umgebung mit grundlegendem Lastausgleich
- Globale SSL-Umgebung mit grundlegendem Lastausgleich
- Gezielte Anmeldung in einer Nicht-SSL-Umgebung mit optionalem Lastausgleich
- Gezielte SSL-Anmeldung in einer gemischten Umgebung mit optionalem Lastausgleich

Nicht-SSL-Umgebung mit grundlegendem Lastausgleich

Sie können WebDirector in einer Nicht-SSL-Umgebung mit einfachem Lastenausgleich verwenden. Der WebDirector gleicht die Last über alle Web-Engines entsprechend dem "Willingness"-Wert jeder Web-Engine aus. Jede Web-Engine kann Anmeldungsanfragen und Nicht-Anmeldungsanfragen bedienen. Für die Kommunikation zwischen dem Webclient und dem Webserver wird das HTTP-Protokoll verwendet.

Legen Sie für jede Web-Engine unter der Kontrolle des WebDirectors die WebDirector-Parameter in der Datei "<Host_Name>-web[#].cfg" der Web-Engine wie folgt fest:

- UseDirector: Ja
- WebDirectorSlumpName: (ändern Sie diesen Wert nicht)
- WillingnessValue: [1 bis 10]
- RedirectingURL: (der vorangestellte Protokollwert kann entweder fehlen oder "http" lauten)

Globale SSL-Umgebung mit grundlegendem Lastausgleich

Sie können WebDirector in einer globalen SSL-Umgebung mit einfachem Lastenausgleich verwenden. Der WebDirector gleicht die Last über alle Web-Engines entsprechend dem "Willingness"-Wert jeder Web-Engine aus. Jede Web-Engine kann Anmeldungsanfragen und Nicht-Anmeldungsanfragen bedienen. Für jede Kommunikation zwischen den Webclients und dem Webserver muss das HTTPS-Protokoll verwendet werden.

Legen Sie für jede Web-Engine unter der Kontrolle des WebDirectors die WebDirector-Parameter in der Datei "<Host_Name>-web[#].cfg" der Web-Engine wie folgt fest:

- UseDirector: Ja
- WebDirectorSlumpName: (ändern Sie diesen Wert nicht)
- WillingnessValue: [1 bis 10]
- RedirectingURL: (der vorangestellte Protokollwert muss "https" sein)

Gezielte Anmeldung in einer Nicht-SSL-Umgebung mit optionalem Lastausgleich

Sie können WebDirector für eine gezielte Anmeldung bei einer Nicht-SSL-Umgebung mit optionalem Lastenausgleich verwenden. Die nur für Anmeldungen zuständige Web-Engine bedient nur die Anmeldungsanfragen. Die restlichen Web-Engines unter der Kontrolle des WebDirectors bedienen alle anderen Anfragen. Bei dieser Konfiguration liegt die gesamte Last der Bedienung von Anmeldungsanfragen auf den angegebenen, nur für die Anmeldung zuständigen Web-Engines. Für die Kommunikation zwischen dem Webclient und dem Webserver wird das HTTP-Protokoll verwendet.

Stellen Sie für die nur für die Anmeldung zuständigen Web-Engines die WebDirector-Parameter in der Datei "<Host_Name>-web[#].cfg" der Web-Engine folgendermaßen ein:

- UseDirector: AfterLogin
- WebDirectorSlumpName: (ändern Sie diesen Wert nicht)
- WillingnessValue: 0
- RedirectingURL: (der vorangestellte Protokollwert kann entweder fehlen oder "http" lauten)

Stellen Sie für die "Nicht-Anmeldungs"-Web-Engines die WebDirector-Parameter in der Datei "<Host_Name>-web[#].cfg" der Web-Engine folgendermaßen ein:

- UseDirector: Before Login
- WebDirectorSlumpName: (ändern Sie diesen Wert nicht)
- WillingnessValue: [1 bis 10]
- RedirectingURL: (der vorangestellte Protokollwert kann entweder fehlen oder "http" lauten)

Gezielte SSL-Anmeldung in einer gemischten Umgebung mit optionalem Lastausgleich

Sie können WebDirector für eine gezielte SSL-Anmeldung in einer gemischten SSL-/Nicht-SSL-Webumgebung mit optionalem Lastenausgleich verwenden. Jeder Web-Anmelde-Request wird an die SSL-Web-Engines umgeleitet und von diesen bedient. Alle anderen Requests werden an die Nicht-SSL-Web-Engines umgeleitet und von diesen bedient. Für jede Kommunikation zwischen dem Webclient und den SSL-Web-Engines muss das HTTPS-Protokoll verwendet werden.

Einrichten der SSL-Anmeldeumgebung

Das Einrichten von SSL ermöglicht Ihnen die Verschlüsselung von Webtransaktionen, wodurch maximale Sicherheit für sensible Daten, insbesondere Kennwörter geboten wird. Abhängig von Ihrem Konfigurationstyp können Sie eine SSL-Anmeldeumgebung auf den konfigurierten CA SDM-Servern implementieren.

Gehen Sie wie folgt vor::

1. Melden Sie sich abhängig von Ihrer CA SDM-Konfiguration bei folgendem Server an:
 - Erweiterte Verfügbarkeit: Anwendungsserver
 - Konventionell: Primärserver oder Sekundärserver

2. Stellen Sie sicher, dass der Server erfolgreich ein SSL-Zertifikat importiert hat.

3. Erstellen Sie eine Kopie (einschließlich Unterverzeichnissen) des Verzeichnisses "\$NX_ROOT/bopcfg/www/wwwroot", und weisen Sie der Kopie den folgenden Namen zu:

\$NX_ROOT/bopcfg/www/wwwrootsec

4. Fügen Sie ein neues virtuelles Verzeichnis für den Webserver mit der Bezeichnung CAisdsec hinzu.

5. Dieses virtuelle Verzeichnis soll auf das folgende physische Verzeichnis zeigen:

\$NX_ROOT/bopcfg/www/wwwrootsec

6. Stellen Sie sicher, dass die virtuellen Verzeichnisberechtigungen für "CAisdsec" den virtuellen Verzeichnisberechtigungen von "CAisd" zur Skriptausführung entsprechen. Erzwingen Sie SSL für das virtuelle Verzeichnis "CAisdsec".

Hinweis: In diesem Beispiel ist CAisdsec anwenderdefiniert und kann umbenannt werden.

7. Speichern Sie die Änderungen.

Hinweis: Web-Directors verwenden nicht die Datei "<Host_Name>-web[#].cfg". Web-Engines erfordern jedoch die eindeutige Datei <Host_Name>-Web[#].cfg. Die Beispieldateien "web.cfg" werden bei der Ausführung der Konfiguration automatisch generiert. Sie können die Anpassungen in der Originaldatei "web.cfg" durch Angeben der Originaldatei "web.cfg" als Vorlagendatei, die Sie verwenden möchten, in die neuen Webkonfigurationsdateien importieren.

8. Kopieren und Speichern Sie die folgenden Dateien. Eine Sicherung von diesen Dateien ist nützlich, wenn Sie sich für die Wiederherstellung der ursprüngliche Umgebung entscheiden:

- \$NX_ROOT/pdmconf/pdm_startup.tpl
- \$NX_ROOT/pdmconf/pdm_startup
- \$NX_ROOT/bopcfg/www/web.cfg file
- jede vorhandene Datei "primary-web[#].cfg"</cs>

- `$NX_ROOT/bopcfg/www/CATALINA_BASE/webapps/CAisd/WEB-INF/web.xml` und `web.xml.tpl`
 - Erstellen Sie für die Konfiguration eines Sekundärserver Sicherungskopien vorhandener `$NX_ROOT/bopcfg/www/web.cfg`- oder `<Hostname_Sekundärserver>-web[#].cfg`-Dateien und von `$NX_ROOT/bopcfg/www/CATALINA_BASE/webapps/CAisd/WEB-INF/web.xml*`
9. Überprüfen Sie für jede Web-Engine, die einem Web-Director zugewiesen ist, ob die Parameter (`<Hostname>-web[#].cfg 'webdirector'`) der Web-Engine richtig festgelegt wurden. Überprüfen Sie die Datei dazu in einem Texteditor. Ändern Sie bei Bedarf die Parameterwerte des WebDirectors, um die Web-Engine-Rolle zu reflektieren. Kopieren Sie sie dann in das Verzeichnis "`$NX_ROOT/bopcfg/www`".
 10. Verschieben Sie alle Dateien `"$NX_ROOT/samples/pdmconf/primary-web[#].cfg</cs>"` in das Verzeichnis `"$NX_ROOT/bopcfg/www</cs>"`.

Bei der Konfiguration des Sekundärserver verschieben Sie alle Dateien vom Typ `"$NX_ROOT/samples/pdmconf/'secondary_server_name-web[#].cfg"` vom Primärserver in das Verzeichnis "`$NX_ROOT/bopcfg/www`" auf dem Sekundärserver.
 11. Für einen Servlet-Server wie Tomcat erstellt CA SDM die Dateien "web.xml", die die Datei "web.xml" auf jedem Server, der eine Web-Engine hostet, ersetzen können. Diese Dateien haben den Namen "primary-web.xml". Benennen Sie die Dateien um und kopieren Sie sie in das Verzeichnis `"$NX_ROOT/bopcfg/www/CATALINA_BASE/webapps/CAisd/WEB-INF"`.

Wenn Sie einen HTTP-Server wie IIS oder Apache verwenden, erstellen Sie Kopien von "pdmweb.exe" im Verzeichnis "`$NX_ROOT/bopcfg/www/wwwroot`", eine Datei vom Typ "pdmweb[#].exe" für jede Web-Engine sowie eine Datei vom Typ "pdmweb_d[#].exe" für jeden konfigurierten Web-Director. Stellen Sie sicher, dass "pdmweb[#].exe" und "pdmweb_d[#].exe" gemäß den korrekten CGI I/F-Werten benannt wurden (zum Beispiel "pdmweb1.exe", "pdmweb2.exe", "pdmweb_d1.exe" usw.).
 12. Wenn Sie IIS verwenden und für jede CGI-Schnittstelle Servererweiterungen hinzufügen möchten, können Sie die Datei "primary-site.dat" als "site.dat" in das Verzeichnis "`$NX_ROOT/bopcfg/www`" kopieren. Bei der erneuten Konfiguration des Systems werden diese Sites IIS hinzugefügt.
 13. Konfigurieren Sie den Primärserver ohne die Datenbank erneut zu initialisieren, und starten Sie die Dienste.
 14. Überprüfen Sie die aktuellen Einstellungen nach dem Neukonfigurieren auf Gültigkeit. Starten Sie die CA SDM-Daemons. Prüfen Sie, ob keine Fehler in den STDLog-Dateien vorhanden sind. Zeigen Sie mit `"pdm_status</cs>"` die Daemons und ihren Status an. Verwenden Sie `http://localhost:8080/CAisd/pdmweb.exe`, um auf das System zuzugreifen.
 15. Für die Integration von Knowledge Management in CA SDM muss der URL-Protokollwert von CA SDM geändert werden, wenn SSL für CA SDM erzwungen wurde.

- a. Ändern Sie im Knowledge Tool-Einstellungsmanager unter "Allgemein" > "Integration" den CA SDM-URL-Protokollwert von "http" in "https".
 - b. Klicken Sie auf „Speichern“ und anschließend auf „Beenden“.
16. Öffnen Sie die CA SDM-Anmeldeseite in einem Web-Browser, und überprüfen Sie, ob sich ein Anwender anmelden kann und ob das erwartete Umleitungs-/Anmeldeverhalten eingehalten wird.

Implementieren der SSL-Anmeldeumgebung

Um die von Ihnen eingerichtete SSL-Anmeldung zu implementieren, nehmen Sie Änderungen an den Web-Director-Parameterwerten vor.

Gehen Sie wie folgt vor:

1. Bearbeiten Sie "<Host_Name>-web[#].cfg" für Web-Engines für sichere Anmeldung folgendermaßen:
 - a. Ändern Sie den "CAisd"-Parameterwert von "/CAisd" in "/CAisdsec".
 - b. Ändern Sie den "UseDirector"-Parameterwert von "Yes" zu "AfterLogin", wenn der Web-Director die Authentifizierung weitergibt.
 - c. Ändern Sie den „Willingness“-Parameterwert von 5 in 0.
 - d. Stellen Sie sicher, dass als Protokoll für den Parameter "RedirectingURL" der Wert "https" eingestellt ist.
 - e. Ändern Sie für "RedirectingURL" den Wert <cgi directory> von "CAisd" in "CAisdsec".
 - f. Speichern Sie die Änderungen.
2. Bearbeiten Sie für nicht sichere Web-Engines, die alle anderen Aktivitäten verarbeiten, die Dateien "<Host_Name>-web[#].cfg" folgendermaßen:
 - a. Überprüfen Sie, ob der "CAisd"-Parameterwert "/CAisd" ist.
 - b. Ändern Sie den "UseDirector"-Parameterwert von "Yes" in "BeforeLogin".
 - c. Behalten Sie den „Willingness“-Wert 5 bei, oder stellen Sie ihn auf eine Ganzzahl zwischen 1 und 10 ein, abhängig davon, welche Lastverteilung Sie wünschen.
 - d. Stellen Sie sicher, dass als Protokoll für den Parameter "RedirectingURL" der Wert "http" eingestellt ist.
 - e. Stellen Sie sicher, dass der "RedirectingURL <cgi directory>"-Wert "CAisd" lautet.
 - f. Speichern Sie die Änderungen.

Starten Sie Service Desk nach der Konfiguration neu. Nachdem der Dienst neu gestartet wurde, testen Sie die Anmeldung, indem Sie mithilfe von HTTP auf die Nicht-SSL-Web-Engine zugreifen. Überprüfen Sie, ob Sie für die Anmeldung automatisch an die sichere HTTPS-Web-Engine umgeleitet werden. Sobald Sie angemeldet sind, werden Sie für die normale Service Desk-Aktivität automatisch auf die HTTP-Web-Engine (Nicht-SSL) umgeleitet.

Überprüfen der SSL-Anmeldeumgebung

Sie können die SSL-Anmeldeumgebung für Web-Engines überprüfen.

Gehen Sie wie folgt vor:

- Die Web-Engines für sichere Anmeldung müssen sich in dem physischen Verzeichnis befinden, das dem virtuellen Verzeichnis mit SSL-Erzwingung zugeordnet ist (in diesem Beispiel "CAisdsec").

Erstellen Sie für Web-Engines für sichere Anmeldung neue Instanzen der Datei "pdmweb.exe" im Verzeichnis "\$NX_ROOT/bopcfg/www/wwwrootsec" mit dem Namen "pdmweb[#].exe". Der Name der ausführbaren Datei muss dem CGI I/F-Wert für jede Web-Engine für sichere Anmeldung entsprechen.

Beispiel: Wenn Sie den CGI I/F-Wert einer Web-Engine für sichere Anmeldung "pdmweb2" zugewiesen haben, erstellen Sie eine physische Kopie der Datei "pdmweb.exe", und nennen Sie diese in "pdmweb2.exe" um.

- Die nicht sicheren Web-Engines und die Web-Directors müssen sich im physischen Verzeichnis befinden, das dem virtuellen Verzeichnis ohne SSL "CAisd" zugeordnet ist.

Erstellen Sie für nicht sichere Web-Engines und WebDirectors Instanzen der Datei "pdmweb.exe" im Verzeichnis "\$NX_ROOT/bopcfg/www/wwwroot". Eine Kopie von "pdmweb.exe" muss für jede nicht sichere Web-Engine und den konfigurierten Web-Director vorhanden sein. Benennen Sie die Kopien um, damit die neuen Namen der ausführbaren Dateien mit den CGI I/F-Werten übereinstimmen, die für die Web-Engines und die Web-Directors definiert wurden.

Beispiel: Wenn Sie der nicht sicheren Web-Engine den CGI I/F-Wert "pdmweb3" und dem Web-Director den Wert "pdmweb_d1" zugewiesen haben, dann erstellen Sie zwei Kopien von "pdmweb.exe". Nennen Sie die erste Kopie in "pdmweb3.exe" und die zweite Kopie in "pdmweb_d1.exe" um.

Einrichten der SSL-Anmeldung für einen Tomcat-Server

Konfigurieren Sie SSL auf Tomcat-Servern in Ihrer CA SDM-Umgebung.

Gehen Sie wie folgt vor:

1. Um einen Schlüsselspeicher auf jedem CA SDM-Server, der ein SSL-Zertifikat benötigt, zu erstellen, führen Sie folgende Schritte aus:

Hinweis: Ein Schlüsselspeicher ist ein Speicher oder Speichereinheit für Zertifikate. Hier werden die Zertifikate importiert, und dann Tomcat weist darauf hin, diesen Schlüsselspeicher und die Zertifikate für SSL zu verwenden.

- a. Erstellen Sie ein Verzeichnis unter dem Laufwerk "C:" (oder ein von Ihnen gewünschtes lokales Laufwerk) mit dem Namen "certificates".
- b. Navigieren Sie über die Befehlszeile zum JRE-bin-Verzeichnis (für die mit Service Desk installierte JRE - normalerweise /SC/JRE)
- c. Führen Sie den Befehl "keytool -genkey -alias tomcat -keyalg RSA -keystore c:/certificates/keystore.jks" aus.
- d. Füllen Sie die Felder entsprechend aus (stellen Sie sicher, dass Sie den Inhalt, den Sie in jedes Feld eingeben, notieren. Möglicherweise werden Sie diese Informationen zu einem späteren Zeitpunkt benötigen).

Die Datei "keystore.jks" wird im Verzeichnis "C:\certificates\" erstellt.

2. Generieren Sie den Zertifikats-Request für jeden Server. Führen Sie folgende Schritte aus, um den Zertifikats-Request zu generieren:

- a. Navigieren Sie über die Befehlszeile zum JRE-bin-Verzeichnis (für die mit Service Desk installierte JRE - normalerweise /SC/JRE)
- b. Führen Sie den Befehl "keytool -certreq -alias tomcat -keystore c:/certificates/keystore.jks -file servername-certreq.csr" aus

Eine .csr-Datei wird im Verzeichnis "c:/certificates" auf jedem Server erstellt, wo Sie den Zertifikats-Request generiert haben.

- c. Senden Sie die .csr-Dateien an den Anbieter Ihrer Wahl, der dann für jeden Server die entsprechenden Zertifikate, die auf dem Zertifikats-Request basieren müssen, generieren wird.

Hinweis: Das Zertifikat, das Sie jeweils erhalten, ist unterschiedlich. Einige Anbieter werden Ihnen mehrere Zertifikate senden, darunter möglicherweise ein Stammzertifikat, ein Zwischenzertifikat und ein Ausstellerzertifikat. Jeder Anbieter hat unterschiedliche Anweisungen für das Importieren der bereitgestellten Zertifikate in den Schlüsselspeicher. Wichtig ist es, den spezifischen Anbieter, der normalerweise Zertifikate für Sie generiert, nach spezifischen Anweisungen für das Importieren der Zertifikate in einen Tomcat-Schlüsselspeicher zu fragen.

Sobald Sie die spezifischen Anweisungen des Anbieters erhalten, können Sie diese befolgen, um die entsprechenden Zertifikate in den Schlüsselspeicher auf jedem Server zu importieren. Nach Abschluss können Sie Tomcat auf der Service Desk-Seite konfigurieren, um auf diesen Schlüsselspeicher zu verweisen, wo die Zertifikate importiert wurden.

3. Öffnen Sie die Datei "\\bopcfg\www\CATALINA_BASE\conf\server.xml" mithilfe eines Texteditors, und suchen Sie Folgendes:

```
<!-- <Connector port="8443" maxHttpHeaderSize="8192"
maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
enableLookups="false" disableUploadTimeout="true"
acceptCount="100" scheme="https" secure="true"
clientAuth="false" sslProtocol="TLS"
keystoreFile="keystoreFile="C:\Documents and Settings\user\.keystore"
keystorePass="password"/> -->
```

4. Ändern Sie den Code folgendermaßen:

```
<Connector port="8443" maxHttpHeaderSize="8192"
maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
enableLookups="false" disableUploadTimeout="true"
acceptCount="100" scheme="https" secure="true"
clientAuth="false" sslProtocol="TLS"
keystoreFile="keystoreFile="C:\certs\keystore.jks"
keystorePass="password"/>
```

Hinweis: Stellen Sie sicher, dass Sie die Tags "<!--" und "-->" entfernen, die derzeit den HTTPS-/SSL-Connector für Tomcat auskommentieren, und legen Sie den entsprechenden Pfad und das Kennwort für Ihren Schlüsselspeicher fest, den Sie zu Beginn generiert haben.

5. Speichern Sie die Datei "server.xml".
6. Starten Sie Tomcat mit den folgenden Befehlen neu:
pdm_tomcat_nxd -c stop
pdm_tomcat_nxd -c start

Hinweis: Wir empfehlen Ihnen, alle CA SDM-Server neu zu starten, um sicherzustellen, dass Tomcat neu gestartet wird.

7. Testen Sie Ihre Tomcat-SSL-Verbindung, indem Sie einen Browser öffnen und mithilfe des HTTPS-Protokolls und des Tomcat-Ports zur Service Desk-URL navigieren. Verwenden Sie zum Beispiel die folgende URL:

`https://servername:8080/CAisd/pdmweb.exe`

Das Service Desk-Anmeldefenster sollte sich öffnen. Sie haben erfolgreich SSL auf Tomcat konfiguriert.

So konfigurieren Sie TCP/IP

Sie können das Standard-TCP-Internet-Protokoll (TCP/IP) auf einem oder mehreren Servern ändern. Diese Einstellung kann auf dem Client nicht erzwungen werden, wenn sie nicht auf dem Server unterstützt wird.

Die TCP/IP-Einstellung wird mit Hilfe der Datei "NX.env" gesteuert, die im Verzeichnis "\$NX_ROOT " gespeichert ist. Benutzen Sie einen Texteditor wie WordPad, um diese Datei zu bearbeiten. Die folgende Option steuert die TCP/IP-Einstellung:

`NX_PROTOCOL_ONLY=Modus`

Dabei kann *Modus* einen der folgenden Werte annehmen:

IPv4

Im IPv4-Modus öffnet das System Sockets für Slump-Vorgänge, die IPv4-Datenverkehr empfangen.

IPv6

Im IPv6-Modus öffnet das System Sockets für Slump-Vorgänge, die IPv6-Datenverkehr empfangen.

Mixed

Im Mixed-Modus öffnet das System Sockets für Slump-Vorgänge, die sowohl IPv4- als auch IPv6-Datenverkehr empfangen. Abhängig von Ihrer CA SDM-Konfiguration können Sie den gemischten Modus unter folgenden Umständen konfigurieren:

- Konventionell: Sekundärserver, die ein anderes Internetprotokoll vom Primärserver oder einander verwenden.
- Erweiterte Verfügbarkeit: Anwendungsserver, die ein anderes Internetprotokoll vom Hintergrundserver oder einander verwenden.

Hinweis: Wenn IPv4- und IPv6-Hosts auf dem Netz koexistieren, stellen Sie sicher, dass die angemessenen Übergangsstrategien, Tools und Mechanismen zur Unterstützung dieser Technologien implementiert sind, bevor Sie die Server-Konfiguration ändern.

Beispiel

`NX_PROTOCOL_ONLY=ipv4`

Bereitstellen von CMDBf-Webservices

Nach der Installation von CA SDM können Sie CMDBf-Webservices bereitstellen.

Gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass der Server in Betrieb ist.
2. Navigieren Sie zum Verzeichnis "CMDBHOME\sdk\websvc\CMDBf".
3. Führen Sie die Datei "deploy_cmbdws.bat" aus.

Die CMDBf-Webservices werden bereitgestellt und gestartet.

Hinweis: Weitere Informationen zu CMDBf finden Sie im *technischen CA CMDB-Referenzhandbuch*.

So starten Sie die CA SDM-Server neu

Führen Sie abhängig von Ihrer CA SDM-Konfiguration folgende Schritte durch:

- [Starten Sie die CA SDM-Server in konventioneller Konfiguration neu](#) (siehe Seite 52).
- [Starten Sie die CA SDM-Server in der Konfiguration für erweiterte Verfügbarkeit neu](#) (siehe Seite 52).

Neustarten der CA SDM-Server in konventioneller Konfiguration

Für die konventionelle Konfiguration starten Sie die Server in folgender Reihenfolge neu:

Hinweis: Um einen Server neu zu starten, klicken Sie auf Start, Einstellungen, Systemsteuerung, Verwaltung, Dienste. Klicken Sie mit der rechten Maustaste auf den CA SDM-Server, und wählen Sie Starten aus.

1. Starten Sie den Sekundärserver neu.
2. Starten Sie den Primärserver neu.

Neustarten der CA SDM-Server in der Konfiguration für erweiterte Verfügbarkeit neu

Für die Konfiguration für erweiterte Verfügbarkeit empfehlen wir, dass Sie die CA SDM-Server in folgender Reihenfolge neu starten:

Hinweis: Um einen Server neu zu starten, klicken Sie auf Start, Einstellungen, Systemsteuerung, Verwaltung, Dienste. Klicken Sie mit der rechten Maustaste auf den CA SDM-Server, und wählen Sie Starten aus.

1. Starten Sie alle Standby-Server neu.
2. [Stufen Sie den Standby-Server als neuen Hintergrundserver hoch](#) (siehe Seite 35).
3. Starten Sie den alten Hintergrundserver.

Wenn Sie den Hintergrundserver starten, dann wird der Server ein Standby-Server.

4. [Wählen Sie einen Anwendungsserver aus, der wenig aktiv ist](#) (siehe Seite 36).
5. Starten Sie den Anwendungsserver neu, der wenig aktiv ist.
6. [Halten Sie den anderen Anwendungsserver an](#) (siehe Seite 37).
7. Starten Sie den Anwendungsserver.
8. Führen Sie die Schritte 6 und 7 für die anderen Anwendungsserver aus.

Hochstufen des Standby-Servers als neuen Hintergrundserver

Bevor Sie den Hintergrundserver anhalten, stufen Sie den Standby-Server (auf dem Sie ein Upgrade durchgeführt haben) als neuen Hintergrundserver hoch. Wenn Support-Automatisierung mit CA SDM installiert ist, dann informieren Sie die aktiven Support-Automatisierung-Anwender darüber, dass der Hintergrundserver heruntergefahren wird.

Gehen Sie wie folgt vor:

1. Führen Sie folgenden Befehl auf dem Hintergrundserver aus, sodass mithilfe von Support-Automatisierung alle aktiven Anwender benachrichtigt werden, ihre Arbeit zu speichern:

```
sa_server_notifier [-h] | [-q seconds] | [-c]
```

-h

Zeigt die Hilfeseite an.

-q seconds

Diese Option benachrichtigt einen lokalen Server (Hintergrundserver), eine Stilllegung in einem angegebenen Zeitintervall durchzuführen. Dieses Intervall ist die Anzahl von Sekunden, bevor der Server offline geschaltet wird. Diese Option kann nicht für einen Standby-Server oder einen Anwendungsserver verwendet werden.

-c

Diese Option bricht einen zuvor gesendeten Request zur Stilllegung ab.

Eine Pop-up-Meldung wird allen aktiven Anwendern angezeigt, die Support-Automatisierung verwenden. Diese Meldung weist die Anwender auf das Herunterfahren des Servers hin, und die verbleibende Zeit bis zum Herunterfahren des Servers wird angezeigt. Die Anwender müssen ihre Arbeit speichern und sich innerhalb der angegebenen Zeit abmelden.

2. Führen Sie folgenden Befehl auf dem Standby-Server aus, den Sie als neuen Hintergrundserver hochstufen möchten:

```
pdm_server_control -b
```

-b

Benachrichtigt einen lokalen Standby-Server, der in den Hintergrundserver gewechselt wird. Der Standby-Server muss bereits ausgeführt werden. Wenn der Server nicht ausgeführt wird, dann wird er gestartet, aber es wird kein Failover durchgeführt. Um ein Failover zu starten, führen Sie den Befehl erneut aus.

Der Hintergrundserver fährt automatisch herunter, und der Standby-Server wird als neuer Hintergrundserver hochgestuft. Diese Änderung wirkt sich nicht auf die Endanwendersitzungen aus. Die Aktualisierungen (sofern vorhanden), die sich in Bearbeitung befinden, werden gespeichert und aufgeschoben, bis der neue Hintergrundserver online geschaltet wird.

Auswählen des Anwendungsservers, der wenig aktiv ist

Sie wählen einen Anwendungsserver mit der geringsten Anwenderaktivität aus. Führen Sie folgenden Befehl auf jedem Anwendungsserver aus, um den Server auszuwählen, der keine oder nur wenige aktive Sitzungen hat.

```
pdm_webstat
```

Hinweis: Dieser Befehl erfasst nicht die SOAP- oder REST-Webservice-Sitzungen.

Anhalten der anderen Anwendungsserver

Sie benachrichtigen alle aktiven Anwender auf einem Anwendungsserver darüber, auf den am wenigsten aktiven Anwendungsserver zu wechseln, bevor Sie ihn anhalten. Stellen Sie sicher, dass Sie den Anwendungsserver, der am wenigsten aktiv ist, neu gestartet haben, bevor Sie alle Anwender dorthin verschieben.

Gehen Sie wie folgt vor:

1. (Empfohlen) Fordern Sie alle aktiven Support-Automatisierung-Analysten auf dem Anwendungsserver, den Sie anhalten möchten, dazu auf, ein Ticket in CA SDM mit ihren Sitzungsinformationen zu erstellen. Dieser Vorgang stellt sicher, dass die Sitzungsinformationen nicht verloren gehen. Zum Beispiel ist der Support-Automatisierung-Analyst in einer Sitzung mit einem Kunden, um einen Hardware-Issue zu lösen. In diesem Fall kann der Support-Automatisierung-Analyst einen Issue in CA SDM mit den Sitzungsinformationen erstellen, bevor der Anwendungsserver heruntergefahren wird.
2. Senden Sie eine Benachrichtigung (zum Beispiel eine E-Mail-Benachrichtigung) an alle aktiven Anwender auf dem Anwendungsserver, in der die Anwender aufgefordert werden, zum Anwendungsserver, der am wenigsten aktiv ist und den Sie gerade neu gestartet haben, zu wechseln. Diese Benachrichtigung kann die Details des aktualisierten Anwendungsservers enthalten.
3. Führen Sie folgenden Befehl auf dem Anwendungsserver aus:

```
pdm_server_control [-h] -q interval -s server_name
```

-h

Zeigt die Hilfeseite an.

-q *interval* -s *server_name*

Benachrichtigt einen lokalen Anwendungsserver oder einen Remote-Anwendungsserver, eine Stilllegung in einem angegebenen Zeitintervall durchzuführen. Dieses Intervall ist die Anzahl der Sekunden, bevor der Server offline geschaltet wird. Wenn man diese Option ohne *server_name* verwendet wird, dann wird der lokale Server zur Stilllegung benachrichtigt. Diese Option kann für einen Hintergrundserver oder einen Standby-Server nicht verwendet werden.

Eine Pop-up-Meldung wird allen aktiven Anwendern auf dem Anwendungsserver angezeigt. Die Meldung weist auf das Herunterfahren des Servers und auf die verbleibende Zeit bis zum Herunterfahren hin. Die Anwender müssen ihre Arbeit speichern und sich innerhalb dieser Zeit abmelden. Der Anwendungsserver wird nach der angegebenen Zeit angehalten. Die Anwender melden sich auf dem anderen Anwendungsserver an, um ihre Arbeit fortzusetzen. Der Support-Automatisierung-Analyst kann sich auf das Ticket beziehen und seine Arbeit fortsetzen.

Der Anwendungsserver wird erfolgreich angehalten.

So halten Sie die CA SDM-Server an

Führen Sie abhängig von Ihrer CA SDM-Konfiguration eine der folgenden Aktionen aus:

- [Halten Sie die CA SDM-Server in konventioneller Konfiguration an](#) (siehe Seite 56).
- [Halten Sie die CA SDM-Server in der Konfiguration für erweiterte Verfügbarkeit an](#) (siehe Seite 57).

Anhalten der CA SDM-Server in konventioneller Konfiguration

Sie halten folgende Server an:

- [Halten Sie den Primärserver an](#) (siehe Seite 56).
- [Halten Sie den Sekundärserver an](#) (siehe Seite 56).

(Konventionelle Konfiguration) Anhalten des Primärservers

Sie können den Primärserver in der Windows- oder UNIX-Umgebung anhalten.

(Windows) Gehen Sie folgendermaßen vor:

1. Wählen Sie in der Systemsteuerung die Option Dienste aus.
Das Fenster Dienste wird geöffnet.
2. Wählen Sie den Dienst CA Service Desk Manager-Server aus, und klicken Sie auf Anhalten.
Der Primärserver wird angehalten. Die Prozesse oder Daemons auf den Sekundärservern werden auch angehalten.

(UNIX) Gehen Sie folgendermaßen vor:

- Geben Sie in der Eingabeaufforderung folgenden Befehl ein:

`pdm_halt`
Der Primärserver wird angehalten. Die Prozesse oder Daemons auf den Sekundärservern werden auch angehalten.

(Konventionelle Konfiguration) Anhalten des Sekundärservers

Sie können den Sekundärserver in der Windows- oder UNIX-Umgebung anhalten.

(Windows) Gehen Sie folgendermaßen vor:

1. Wählen Sie in der Systemsteuerung die Option Dienste aus.
Das Fenster Dienste wird geöffnet.

2. Wählen Sie den Dienst CA Service Desk Manager-Remote-Überwachung aus, und klicken Sie auf Anhalten.

Der Sekundärserver wird angehalten.

(UNIX) Gehen Sie folgendermaßen vor:

- Geben Sie in der Eingabeaufforderung folgenden Befehl ein:

`pdm_halt`

Der Sekundärserver wird angehalten.

Anhalten der CA SDM-Server in der Konfiguration für erweiterte Verfügbarkeit

Sie halten folgende Server an:

- [Halten Sie den Standby-Server an](#) (siehe Seite 57).
- [Halten Sie den Hintergrundserver an](#) (siehe Seite 57).
- [Halten Sie den Anwendungsserver an](#) (siehe Seite 59).

(Konfiguration für erweiterte Verfügbarkeit) Anhalten des Standby-Servers

Sie können den Standby-Server in der Windows- oder UNIX-Umgebung anhalten.

(Windows) Gehen Sie folgendermaßen vor:

1. Wählen Sie in der Systemsteuerung die Option Dienste aus.
Das Fenster Dienste wird geöffnet.
2. Wählen Sie den Dienst CA Service Desk Manager-Server aus, und klicken Sie auf Anhalten.
Der Standby-Server wird angehalten.

(UNIX) Gehen Sie folgendermaßen vor:

- Geben Sie in der Eingabeaufforderung folgenden Befehl ein:

`pdm_halt`

Der Standby-Server wird angehalten.

(Konfiguration für erweiterte Verfügbarkeit) Anhalten des Hintergrundservers

Bevor Sie den Hintergrundserver anhalten, stufen Sie den Standby-Server (auf dem Sie ein Upgrade durchgeführt haben) als neuen Hintergrundserver hoch. Wenn Support-Automatisierung mit CA SDM installiert ist, dann informieren Sie die aktiven Support-Automatisierung-Anwender darüber, dass der Hintergrundserver heruntergefahren wird.

Gehen Sie wie folgt vor:

1. Führen Sie folgenden Befehl auf dem Hintergrundserver aus, sodass mithilfe von Support-Automatisierung alle aktiven Anwender benachrichtigt werden, ihre Arbeit zu speichern:

```
sa_server_notifier [-h] | [-q seconds] | [-c]
```

-h

Zeigt die Hilfeseite an.

-q seconds

Diese Option benachrichtigt einen lokalen Server (Hintergrundserver), eine Stilllegung in einem angegebenen Zeitintervall durchzuführen. Dieses Intervall ist die Anzahl von Sekunden, bevor der Server offline geschaltet wird. Diese Option kann nicht für einen Standby-Server oder einen Anwendungsserver verwendet werden.

-c

Diese Option bricht einen zuvor gesendeten Request zur Stilllegung ab.

Eine Pop-up-Meldung wird allen aktiven Anwendern angezeigt, die Support-Automatisierung verwenden. Diese Meldung weist die Anwender auf das Herunterfahren des Servers hin, und die verbleibende Zeit bis zum Herunterfahren des Servers wird angezeigt. Die Anwender müssen ihre Arbeit speichern und sich innerhalb der angegebenen Zeit abmelden.

2. Führen Sie folgenden Befehl auf dem Standby-Server aus, den Sie als neuen Hintergrundserver hochstufen möchten:

```
pdm_server_control -b
```

-b

Benachrichtigt einen lokalen Standby-Server, der in den Hintergrundserver gewechselt wird. Der Standby-Server muss bereits ausgeführt werden. Wenn der Server nicht ausgeführt wird, dann wird er gestartet, aber es wird kein Failover durchgeführt. Um ein Failover zu starten, führen Sie den Befehl erneut aus.

Der Hintergrundserver fährt automatisch herunter, und der Standby-Server wird als neuer Hintergrundserver hochgestuft. Diese Änderung wirkt sich nicht auf die Endanwendersitzungen aus. Die Aktualisierungen (sofern vorhanden), die sich in Bearbeitung befinden, werden gespeichert und aufgeschoben, bis der neue Hintergrundserver online geschaltet wird.

(Konfiguration für erweiterte Verfügbarkeit) Anhalten des Anwendungsservers

Bevor Sie einen Anwendungsserver anhalten, müssen Sie alle aktiven Anwender darüber informieren, zu einem anderen Anwendungsserver zu wechseln.

Gehen Sie wie folgt vor:

1. Senden Sie eine Benachrichtigung an alle aktiven Anwender auf dem Anwendungsserver, den Sie anhalten möchten, um den Wechsel auf den anderen Anwendungsserver durchzuführen. Diese Benachrichtigung kann die Details des anderen Anwendungsservers enthalten. Zum Beispiel können Sie eine E-Mail-Benachrichtigung senden.
2. Führen Sie folgenden Befehl auf dem Anwendungsserver aus, den Sie anhalten möchten:

```
pdm_server_control -q interval -s server_name
```

-q interval -s server_name

Benachrichtigt einen lokalen Anwendungsserver oder einen Remote-Anwendungsserver, eine Stilllegung in einem angegebenen Zeitintervall durchzuführen. Dieses Intervall ist die Anzahl von Sekunden, bevor der Server offline geschaltet wird. Wenn man diese Option ohne "server_name" verwendet, dann wird der lokale Server zur Stilllegung benachrichtigt. Diese Option kann für einen Hintergrundserver oder einen Standby-Server nicht verwendet werden.

Eine Pop-up-Meldung wird allen aktiven Anwendern auf dem Anwendungsserver angezeigt. Diese Meldung weist die Anwender auf das Herunterfahren des Servers hin, und die verbleibende Zeit bis zum Herunterfahren des Servers wird angezeigt. Die Anwender müssen ihre Arbeit speichern und sich innerhalb dieser Zeit abmelden. Der Anwendungsserver wird nach der angegebenen Zeit angehalten. Die Anwender melden sich auf dem anderen Anwendungsserver an, um ihre Arbeit fortzusetzen.

(Empfohlen) Die aktiven Support Automation-Analysten können ein Ticket erstellen, das sich auf ihre Sitzung bezieht, um ihre Arbeit zu speichern. Sie können sich bei anderen Anwendungsservern anmelden und sich auf dieses Ticket beziehen, um ihre Arbeit fortzusetzen.

Unterstützte Tablets

Auf dem Apple-iPad werden die Schnittstellen für Analysten, Mitarbeiter-Self-Service, Kunden-Self-Service und Anbieter-Self-Service im Standardbrowser mit beschränkter Funktionalität angezeigt. CA SDM unterstützt auf Tablets keine Anhänge.

Hinweis: Auf allen anderen Tablets wird die PDA-Analystenschnittstelle angezeigt. Auf dem iPad unterstützt der Safari-Browser die volle CA SDM-Benutzeroberfläche. Andere Browser zeigen auf iPads die Benutzeroberfläche möglicherweise vollständig an, sind nicht unterstützt.

Tomcat-Protokollierung

CA SDM verwendet eine separate log4j.properties-Datei für Webkomponenten wie Servlets und PDM_RPC. Support-Automatisierung, CMDB Visualizer und REST haben ebenfalls eine separate log4j.properties-Datei. Für das Starten oder Anhalten der Tomcat-Protokollierung müssen Sie die Tomcat-Daemons nicht zurückführen.

Die folgende Liste beschreibt die Unterschiede der log4j.properties-Dateien der einzelnen CA SDM-Komponenten:

- CA SDM überwacht die Datei log4j.properties in NX_ROOT\site\cfg und NX_ROOT\bopcfg\www\CATALINA_BASE\webapps\CAisd\WEB-INF auf Änderungen.
- Support-Automatisierung überwacht die Datei log4j.properties in NX_ROOT\bopcfg\www\CATALINA_BASE_SA\webapps\SupportAutomation\WEB-INF.
- CMDB Visualizer überwacht die Datei cmdbvisualizerlogging.properties in NX_ROOT\bopcfg\www\CATALINA_BASE_VIZ\webapps\CMDBVisualizer\WEB-INF\classes.
- REST überwacht die Datei rest.log4j.properties in NX_ROOT\site\cfg.

Verwenden Sie das pdm_log4j_config-Hilfsprogramm nur zum Ändern von Variablen in den Dateien log4j.properties, cmdbvisualizerlogging.properties und rest.log4j.properties. Sie können das pdm_log4j_config-Hilfsprogramm nicht verwenden, um das Abfrageintervall zu ändern.

CA SDM durchsucht die log4j.properties-Dateien regelmäßig nach Änderungen. Konfigurieren Sie das Zeitintervall durch das Ändern der Variable NX_LOG4J_REFRESH_INTERVAL in der Datei "NX.env".

Servlet-Standards

Die folgenden Servlets fügen standardmäßig Meldungen auf INFO-Ebene zur jsrvr.log-Datei hinzu:

- PDMContextListener: Generiert Protokolleinträge beim Starten und Herunterfahren von Services.
- PDMweb: Generiert Protokolleinträge bei Vorgängen auf der Benutzeroberfläche.
- UploadServlet: Generiert Protokolleinträge, wenn Sie Dateien an ein Ticket anhängen.
- pdmExport: Generiert Protokolleinträge, wenn Sie in Listenformularen auf "Exportieren" klicken.
- pdm_report: Generiert Protokolleinträge, wenn Sie in Listenformularen auf das Menü "Berichte" klicken.
- page_cache: Generiert Protokolleinträge bei Vorgängen auf der Benutzeroberfläche.
- ProcessServlet: Generiert Protokolleinträge, wenn Sie CA Workflow installieren und auf CA Workflow-Aufgaben zugreifen.
Hinweis: Der pdm_rpc-Daemon generiert bei diesen Aktionen ebenfalls Protokolleinträge.
- BOServlet: Generiert Protokolleinträge, wenn Sie CA Business Intelligence konfigurieren und auf die Registerkarte "Berichte" klicken.

PDA-Schnittstelle

CA SDM unterstützt ITIL-Terminologie für die PDA-Schnittstelle (persönlicher digitaler Assistent). Diese Schnittstelle ermöglicht es Endanwendern, Requests, Incidents und Probleme zu erstellen und nach den folgenden Tickettypen zu suchen:

- Incidents
- Probleme
- Requests
- Changes
- Issues

Analysten können die PDA-Schnittstelle verwenden. Diese Schnittstelle berücksichtigt die Rolle im Feld *PDA-Rolle* des Zugriffstyps des Kontakts.

Zeigt die PDA-Schnittstelle auf allen nicht unterstützten Geräten und Browsern an.

Der Suchdienst zum Suchen nach Kontakten funktioniert nur in PDA-Browsern, die mehrere Registerkarten und mehrere Browserfenster unterstützen. Die Mandantenfähigkeit auf der Browseroberfläche ist ähnlich, doch die Drop-down-Liste zum Aktivieren von Mandantenfähigkeit wird nicht angezeigt. Wenn Sie das Ticket erstellen, basieren die Mandanteneigenschaften auf dem Anforderer, dem betroffenen Endanwender und dem Analysten.

Die automatische Berechnung der Prioritäten (Automatic Priority Calculator, APC) hilft bei der Entscheidung der Priorität bei der Erstellung von Incidents und Problemen. Sie basiert auf Attributen, Dringlichkeit, Auswirkung, Request-Bereich sowie dem betroffenen Endanwender.

Hinweis: Ein Sternchen bedeutet, dass ein Feld erforderlich ist. Beispielsweise müssen Sie bei der Erstellung eines Request den betroffenen Endanwender und die Priorität angeben. Die PDA-Schnittstelle unterstützt keine Anhänge bei der Ticketerstellung.

REST-Protokollierung

REST verwendet die Pakete `pdm_rest_util.jar` und `rest-core.jar`, die `log4j`-Protokollierung unterstützen. Diese Komponenten schreiben *keine* Meldungen in die standardmäßigen Protokolle (`stdlog.*`). Stattdessen verwenden Sie die `log4j` Komponente. Standardmäßig erstellen diese Pakete Protokolleinträge für INFO-, ERROR- und WARN-Meldungen. Da die Java-Pakete die gleiche `log4j`-Konfigurationseigenschaftsdatei verwenden, gelangen die Protokolleinträge zu allen Meldungen in dieselbe Ausgabedatei. Sie können die Datei `rest.log4j.properties` im Verzeichnis `$NX_ROOT\site\cfg\` anzeigen.

Um die Protokollebene für Nachverfolgungs- oder Debugging-Zwecke zu erweitern, aktualisieren Sie den folgenden Abschnitt in der Datei `rest.log4j.properties`:

```
log4j.rootCategory=debug, jrestlog
```

Suchen Sie die Ausgabedatei, die in der Konfigurationseigenschaftsdatei definiert ist, im folgenden Verzeichnis:

```
$NX_ROOT\log\jrest.log
```

Aktivieren der CXF-Protokollierung

CA SDM deaktiviert CXF-Protokollierung standardmäßig, da es sich negativ auf die Leistung von Produktionsumgebungen auswirken kann. Wenn Ihre Umgebung diese Protokollierung für Debugging-Zwecke benötigt, kann der Administrator die Datei beans.xml ändern, um die CXF-Protokollierung zu aktivieren.

Gehen Sie wie folgt vor:

1. Suchen Sie die Datei beans.xml im folgenden Verzeichnis:

NX_ROOT\bopcfg\www\CATALINA_BASE_REST\webapps\caisd-rest\WEB-INF

2. Suchen Sie den folgenden Abschnitt der XML-Datei:

```
<cxf:bus>
  <cxf:features>
  </cxf:features>
</cxf:bus>
```

3. Fügen Sie zum Abschnitt wie im folgenden Beispiel <cxf:logging/> hinzu:

```
<cxf:bus>
  <cxf:features>
    <cxf:logging/>
  </cxf:features>
</cxf:bus>
```

4. Speichern Sie die XML-Datei.

ITIL-Konfiguration

Information Technology Infrastructure Library (ITIL) ist eine Sammlung von Best Practices im Datencenter-Management. Zusätzlich zur Definition empfohlener Prozesse besteht ein großer Nutzen des ITIL-Framework in den genauen Definitionen gebräuchlicher Begriffe aus der Datencenter-Terminologie. Im IT-Kontext wird oft dasselbe Wort verwendet, um unterschiedliche Dinge zu benennen, oder verschiedene Personen verwenden ein bestimmtes Wort mit individuell abweichenden Nuancen. ITIL hilft dabei, dieses Problem zu vermeiden.

Folgende Tickettypen stehen zur Verfügung:

- Request
- Change
- Issue
- Incident (Störung)
- Problem

Wichtig! CA SDM wird nur auf ITIL-Oberflächen unterstützt. Die ITIL-Oberfläche unterstützt Datenobjekte, die in bisherigen Nicht-ITIL-Versionen des Produkts nicht verwendet wurden, wie z. B. Problem- und Incident-Tickets.

ITIL führt folgende Aufgaben aus:

- Erstellt eine ITIL-Schnittstelle für Ihre CA SDM-Installation.
- Macht es möglich, dass Ihre CA SDM-Datenbank, -Formulare und -Felder von einer Standardinstallation abweichen und stattdessen ITIL-Konventionen entsprechen.

Wichtig! Wenn Sie ein Upgrade für Ihr vorhandenes System durchführen, deaktivieren Sie das Kontrollkästchen "Standarddaten laden", um die Datenbanktabellen und -daten beizubehalten. Anderenfalls gehen alle vorhandenen Daten verloren. Weitere Informationen zur Migration von einer Nicht-ITIL-Umgebung finden Sie im *Implementierungshandbuch*.

ITIL-Servicedisziplinen

ITIL beschreibt Best Practices für mehrere Disziplinen. Zusammengenommen stellen die Dienstunterstützungs- und die Dienstübermittlungsregeln die Dienstverwaltungsfunktionen einer Organisation bereit. Zwischen allen zehn Service-Managementdisziplinen bestehen komplizierte Wechselbeziehungen, die sicherstellen, dass die IT-Infrastruktur Unternehmen Services auf höchste Ebene bietet.

Der Service-Support umfasst die folgenden Disziplinen:

- Vorfallverwaltung
- Problemverwaltung
- Change Management
- Versionsverwaltung
- Configuration Management

CA SDM befasst sich speziell mit Incident, Problem und Change Management und Konfigurationsverwaltung.

Die Servicebereitstellung umfasst die folgenden Disziplinen:

- Service Management
- Verfügbarkeitsverwaltung
- Kapazitätsverwaltung
- Finanzverwaltung für IT-Dienstleistungen
- Kontinuitätsverwaltung für IT-Dienstleistungen

CA SDM behandelt im besonderen das Service Management.

Optionen für die Mitarbeiter- und Gastschnittstelle

Sie können CA SDM verwenden, um getrennte Schnittstellen für Angestellte und Gäste zu konfigurieren. über den Optionsmanager auf der Registerkarte "Administration" konfigurieren. Die folgenden Werte steuern diese Schnittstellen:

employee_intf_incident_support

Zeigt die folgenden Werte an:

- Nur Anfrage
- Nur Incident
- Incident und Anfrage

guest_intf_incident_support

Zeigt die folgenden Werte an:

- Nur Anfrage
- Nur Incident
- Incident und Anfrage

Wichtig! Bei einer neuen Installation ist ITIL standardmäßig so konfiguriert, dass für den Wert *Nur Incident* festgelegt wurde. Wenn Sie von einer vorherigen Nicht-ITIL-Konfiguration migrieren, werden die Optionen installiert, die Werte werden jedoch auf *"Nur Anfrage"* gesetzt.

Konfigurieren der Mitarbeiterschnittstelle

Sie können die Mitarbeiterschnittstelle so konfigurieren, dass Incidents, Anfragen oder beide angezeigt werden.

So konfigurieren Sie die Mitarbeiterschnittstelle:

1. Klicken Sie auf die Registerkarte "Administration".
Die Admin-Konsole wird angezeigt.
2. Klicken Sie auf "Optionsmanager" > "Anfrage-Mgr".
Die Optionsliste wird angezeigt.
3. Klicken Sie auf "employee_intf_incident_support".
Die Seite "Optionen – Detail" wird angezeigt.
4. Ändern Sie das Feld "Optionswert" in einen der folgenden Werte:

Nur Incident

(ITIL-Standard) Zeigt nur die Incident-Ticket-Typen auf der Mitarbeiterschnittstelle an.

Nur Anfrage

Zeigt nur die Anfrage-Ticket-Typen auf der Mitarbeiterschnittstelle an.

Incident und Anfrage

Zeigt sowohl Incident- als auch Anfragetickettypen in der Mitarbeiterschnittstelle an.

Klicken Sie auf "Speichern".

5. Klicken Sie auf "Aktualisieren", um Ihre Auswahlen zu bestätigen.

Die Seite "Optionen - Detail" wird aktualisiert.

6. Schließen Sie die Seite "Optionen - Detail".

Die Optionsliste wird angezeigt.

Konfigurieren der Gastschnittstelle

Sie können die Gastschnittstelle so konfigurieren, dass Incidents, Anfragen oder beide angezeigt werden.

So konfigurieren Sie die Gastschnittstelle:

1. Klicken Sie auf die Registerkarte "Administration".

Die Admin-Konsole wird angezeigt.

2. Klicken Sie auf "Optionsmanager" > "Anfrage-Mgr".

Die Optionsliste wird angezeigt.

3. Klicken Sie auf "guest_intf_incident_support".

Die Seite "Optionen – Detail" wird angezeigt.

4. Ändern Sie das Feld "Optionswert" in einen der folgenden Werte:

Nur Incident

(ITIL-Standard) Zeigt nur die Incident-Ticket-Typen auf der Gastschnittstelle an.

Nur Anfrage

Zeigt nur die Anfrage-Ticket-Typen auf der Gastschnittstelle an.

Incident und Anfrage

Zeigt sowohl Incident- als auch Anfragetickettypen in der Gastschnittstelle an.

Klicken Sie auf "Speichern".

5. Klicken Sie auf "Aktualisieren", um Ihre Auswahlen zu bestätigen.

Die Seite "Optionen - Detail" wird aktualisiert.

6. Schließen Sie die Seite "Optionen - Detail".

Die Optionsliste wird angezeigt.

Aktivitätsprotokoll – Sicherheit

Die Sicherheitsoption "Aktivitätsprotokoll" verhindert, dass Endbenutzer Felder in einem Aktivitätsprotokoll aktualisieren. Sie können die Option "Intern" auswählen, um zu verhindern, dass Kunden das Protokoll anzeigen.

"Aktivitätsprotokoll - Sicherheit" betrifft die Aktivitätsprotokolle der folgenden Ticket-Typen:

- Request
- Change
- Issue
- Incident (Störung)
- Problem

Aktivieren des Aktivitätsprotokolls – Sicherheit

Sie können auf der Registerkarte "Administration" unter "Optionsmanager" die Option "Aktivitätsprotokoll – Sicherheit" aktivieren.

So aktivieren sie das Aktivitätsprotokoll – Sicherheit:

1. Klicken Sie auf die Registerkarte "Administration".
Die Admin-Konsole wird angezeigt.
2. Klicken Sie auf "Optionsmanager" > "Anfrage-Change-Issue".
Die Optionsliste wird angezeigt.
3. Klicken Sie auf "activity_log_security".
Die Seite "Optionen – Detail" wird angezeigt.
4. Klicken Sie auf "Bearbeiten", und wählen Sie einen der folgenden Optionswerte aus:

Bearbeitbar

(Standard) Lässt zu, dass alle Felder des Aktivitätsprotokolls über die Web-Schnittstelle oder Webservices bearbeitet werden können.

Schreibgeschützt

Zeigt das Aktivitätsprotokoll als schreibgeschützt an. Wenn Sie die interne Option wählen, können nur interne Benutzer das Protokoll bearbeiten, und es kann nicht von Kunden angesehen werden.

Hinweis: Wenn die Sicherheitsoption aktiviert ist, wird eine Fehlermeldung ausgegeben, wenn Sie versuchen, das Protokoll über die Web-Schnittstelle oder Webservices zu bearbeiten. Die Meldung zeigt an, dass das Aktivitätsprotokoll schreibgeschützt ist.

Klicken Sie auf "Speichern".

5. Klicken Sie auf "Aktualisieren", um Ihre Auswahlen zu bestätigen. Schließen Sie das Fenster.

Die Sicherheitsoption des Aktivitätsprotokolls wird aktiviert.

Wichtig! Sie können die Option "activity_log_security" nicht deinstallieren. Sie können nur in "Optionsmanager" > "Anfrage-Change-Issue" den Wert der Option auf "Bearbeitbar" oder "Schreibgeschützt" einstellen.

Auswirkung auf Web Screen Painter ein

Die Funktion Aktivitätsprotokollsicherheit "\$NX_ACTIVITY_LOG_SICHERHEIT" enthält die folgenden Attribute ("time_spent", "time_stamp" "description") für die Objekte "alg", "chgalg", "issalg" in Majic.

Beispiel: \$NX_ACTIVITY_LOG_SECURITY für Objekt "alg" in cm.maj

In diesem Beispiel erscheint für Objekt "alg" in cm.maj \$NX_ACTIVITY_LOG_SECURITY bei den drei Attributen:

```
time_spent DURATION $NX_ACTIVITY_LOG_SECURITY {ON_POST_VAL update_cr_timespent(
call_req_id ) 50 ;
} ;
time_stamp DATE $NX_ACTIVITY_LOG_SECURITYÂ Â Â { ON_NEW DEFAULT NOW ; } ;
descriptionÂ Â Â Â STRING Â Â Â $NX_ACTIVITY_LOG_SECURITY;
```

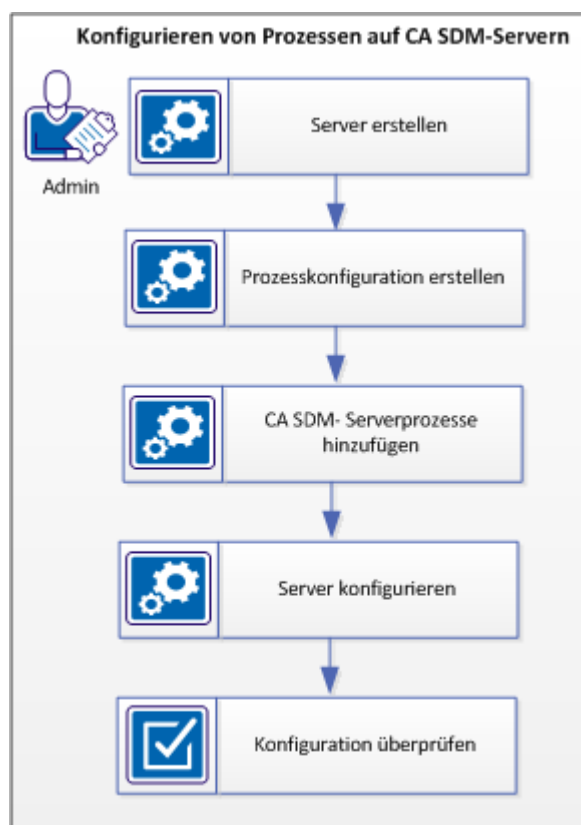
In Web Screen Painter wird das Feld *Nur bei neuem Eintrag aktualisierbar* deaktiviert, wenn der Wert des Schlüsselworts "WRITE_NEW" beträgt.

Hinweis: Informationen zu Web Screen Painter finden Sie im *Implementierungshandbuch*.

So konfigurieren Sie Prozesse für CA SDM-Server

Als Administrator können Sie Prozesse und Daemons hinzufügen oder ändern, um die Leistung der CA SDM-Server zu erhöhen. Sie können Objektmanager, Web-Engines, Web-Directors und andere Prozesse für die CA SDM-Server in Ihrer Umgebung konfigurieren. Sie können die Prozesse über mehrere Server hinzufügen, um Volume, Leistung und Sicherheit zu erhöhen.

Das folgende Diagramm zeigt, wie Sie die Prozesse auf den CA SDM-Servern konfigurieren:



Gehen Sie wie folgt vor:

1. [Erstellen Sie einen Server](#) (siehe Seite 71).
2. [Erstellen Sie eine Prozesskonfiguration](#) (siehe Seite 72).
3. [Fügen Sie CA SDM-Serverprozesse hinzu](#) (siehe Seite 74).
4. Konfigurieren Sie den Server. Weitere Informationen zum Konfigurieren des Servers finden Sie im Szenario *So konfigurieren Sie CA SDM-Server* im *Implementierungshandbuch*.
5. [Überprüfen Sie die Konfiguration](#) (siehe Seite 89).

Hinzufügen eines Servers

Wenn keine Server vorhanden sind, fügen Sie Serverdatensätze für alle Server hinzu, die Sie in Ihrer CA SDM-Bereitstellung installieren möchten.

Gehen Sie wie folgt vor:

1. Melden Sie sich abhängig von Ihrer CA SDM-Konfiguration bei folgendem Server an:
 - Konventionell: Primärserver
 - Erweiterte Verfügbarkeit: Hintergrundserver
2. Wählen Sie in der Registerkarte Administration System, Server aus.
Die Seite "Server - Liste" wird geöffnet.
3. Klicken Sie auf Neu erstellen, um einen Serverdatensatz für den folgenden Server hinzuzufügen, je nach CA SDM-Konfiguration:
 - Konventionell: Sekundärserver
 - Erweiterte Verfügbarkeit: Anwendungsserver oder Standby-Server.Die Seite Neuen Server erstellen wird angezeigt.
4. Vervollständigen Sie die Serverfelder entsprechend dem Server.
5. Klicken Sie auf "Speichern".
Sie haben das Serverdetail hinzugefügt.

Erstellen von Serverfeldern

Die folgenden Felder werden angezeigt, wenn Sie einen Server erstellen:

Hostname

Gibt den lokalen Hostnamen des Servers an. Der lokale Hostname wird in der usp_servers-Tabelle in der local_host-Spalte gespeichert.

Wichtig! Stellen Sie sicher, dass beim Eingeben des Hostnamens in der usp_servers-Tabelle die Groß- und Kleinschreibung beachtet wird.

Zeitzone

Gibt die Zeitzone an, in der sich der Server befindet. Die Zeitzone dient zum Auslösen von Events im System, wenn die Option Use End User Time Zone nicht ausgewählt oder keine Zeitzone für den Servicetyp angegeben wurde.

Datensatzstatus

Zeigt den Zustand des Servers an. Der aktive Status zeigt an, dass der Server ein Teil der CA SDM-Bereitstellung ist.

Wichtig! Wenn Sie einen Server deaktiviert haben, wird empfohlen, keine CA SDM-Services auf diesem Server zu starten. Diese Aktion kann in unerwartetem Verhalten resultieren.

Servertyp

Gibt den Typ des Servers an, den Sie konfigurieren möchten. Folgende Servertypen können je nach Ihrer CA SDM-Konfiguration ausgewählt werden:

- Erweiterte Verfügbarkeit: Anwendungsserver oder Standby-Server.
- Konventionell: Sekundärserver

Konfiguriert

Verfügbar nur bei der erweiterten Verfügbarkeitskonfiguration. Zeigt den Zustand des konfigurierten Servers an. Der Standardwert dieses Felds ist "Nein". Der Wert wird zu "Ja" aktualisiert, nachdem Sie `pdm_configure` erfolgreich auf diesem Server ausgeführt haben. Wenn Sie einen der automatisch eingegebenen Feldwerte eines Serverdatensatzes bearbeiten, ändert sich das Feld Konfiguriert in "Nein".

Erstellen einer Prozesskonfiguration

Sie können eine Prozesskonfiguration für Ihre CA SDM-Installation erstellen, oder Sie können eine vorhandene Konfiguration ändern, um Ihre Anforderungen anzupassen.

Beachten Sie folgende Punkte, während Sie eine Prozesskonfiguration erstellen:

- Bei einer konventionellen Konfiguration erstellen Sie die Konfiguration nur für einen Primärserver, und nicht für Sekundärserver. Alle Konfigurationsdetails für Sekundärserver müssen in der für den Primärserver erstellten Konfiguration enthalten sein. Um zum Beispiel eine Web-Engine mit den Hostnamendetails des Sekundärservers hinzuzufügen, öffnen Sie die Konfiguration für den Primärserver, und fügen Sie die notwendigen Details hinzu.
- Für einen Konfigurationstyp für erweiterte Verfügbarkeit können Sie nur Konfigurationen für den spezifischen Server erstellen. Stellen Sie sicher, dass Sie die gleiche Konfiguration für den Hintergrundserver und für den Standby-Server erstellen.

Gehen Sie wie folgt vor:

1. Wählen Sie auf der Registerkarte Administration die Option Systeme, Konfigurationen.
Die Seite Konfigurationsliste wird geöffnet.
2. Klicken Sie auf "Neu erstellen", um eine Serverkonfiguration hinzuzufügen.
Die Seite "Neue Konfiguration erstellen" wird geöffnet.
3. Füllen Sie die folgenden Felder aus:

Wichtig! Geben Sie nur englische Zeichen in die Eingabefelder lokalisierter Sprachen ein.

Konfigurationsname

Gibt den Namen an, den Sie zu der Konfiguration, die Sie erstellen, zuweisen möchten.

Erweiterte Verfügbarkeit

Gibt an, ob die Konfiguration für konventionelle Konfiguration oder für den Konfigurationstyp für erweiterte Verfügbarkeit erstellt wird. Wählen Sie Ja aus, wenn die Konfiguration für den Konfigurationstyp für erweiterte Verfügbarkeit gültig ist.

Hinweis: Konfigurationen, die für einen Konfigurationstyp (erweiterte Verfügbarkeit oder konventionell) erstellt werden, können nicht für den anderen Konfigurationstyp implementiert werden.

Hostname

Gibt den Hostnamen für die Konfiguration an. Der Hostname wird aus den Serverdatensätzen übernommen, die auf der Seite Server konfiguriert sind. Sie können auf die Schaltfläche Suchen klicken, um nach Servern zu suchen, die zu Ihrer CA SDM-Installation hinzugefügt wurden.

Datensatzstatus

Gibt an, ob der Datensatz der Serverkonfiguration aktiv ist.

Aktuelle Konfiguration

Gibt an, dass die Konfiguration auf dem ausgewählten CA SDM-Server angewendet ist. Dieses Feld ist schreibgeschützt und wird basierend auf der Konfiguration, die Sie bei der Ausführung des Server-Konfigurationsprogramms (pdm_configure) auswählen, aktualisiert.

4. Klicken Sie auf "Speichern".

Die Konfiguration wird gespeichert. Es werden neue Registerkarten auf der Seite aktiviert, um Objektmanager, Web-Engines, Web-Directors und andere Prozesse hinzuzufügen.

Hinweis: Der Hostname und die Felder für erweiterte Verfügbarkeit werden schreibgeschützt, sobald Sie die Konfiguration gespeichert haben.

Klicken Sie auf der Seite Konfiguration - Liste auf In Liste bearbeiten, um den Datensatzstatus einer Prozesskonfiguration zu ändern.

Hinweis: Sie können den Datensatzstatus nicht ändern, wenn die aktuelle Konfiguration eines ausgewählten Servers verwendet wird.

Hinzufügen von CA SDM-Serverprozessen

Sie können Objektmanager, Web-Engines, Web-Directors und andere Prozesse für die CA SDM-Server in Ihrer Umgebung konfigurieren. Es wird empfohlen, dass Sie sich mit folgenden Informationen vertraut machen, bevor Sie die CA SDM-Prozesse konfigurieren:

Wichtig: Konfigurieren Sie den spezifischen Server neu, indem Sie das Hilfsprogramm "pdm_configure" auf dem Server ausführen, nachdem Sie die CA SDM-Prozesse hinzugefügt haben.

Objektmanager

Objektmanager verwalten alle CA SDM-Objekte. Jeder Objektmanager hat einen verknüpften Namen, der verwendet wird, um mit anderen Objekten zu kommunizieren. Unternehmenssysteme mit Multiprozessor-Servern können Objektmanager hinzufügen, um die Verarbeitungslast zu verteilen. Abhängig von Ihrem Konfigurationstyp installiert CA SDM einen standardmäßigen Objektmanager auf den folgenden Servern:

- Konventionell: Primärserver
- Erweiterte Verfügbarkeit: Alle Server.

Hinweis: Sie können den standardmäßigen Objektmanager nicht ändern. Allerdings können Sie einem beliebigen Server zusätzliche Objektmanager hinzufügen.

Web-Engines

Web-Engines unterstützen Sie bei der Vorbereitung von Webseiten für den Webclient. Alle Systeme verfügen über eine oder mehrere Web-Engines. Jede Web-Engine stellt eine Verbindung zu einem Objektmanager her, um alle Requests für CA SDM-Objekte zu verarbeiten. Jede Web-Engine kann direkt ausgeführt werden, und auf jede Web-Engine kann direkt zugegriffen werden. Beim direkten Zugriff gibt jeder Webbrowser die spezifische CGI-Schnittstelle für eine spezifische Web-Engine ein. Mit dieser Vorgehensweise können alle Clients eine Verbindung zu einer Web-Engine aufnehmen und die Web-Engine überlasten, während andere Web-Engines ungenutzt bleiben. Um diesen schweren Datenverkehr zu verarbeiten, können Sie zwei oder mehrere Web-Engines mit einem einzelnen Web-Director verknüpfen. Alle Requests, die zu Web-Engines gehen, werden an den Web-Director geleitet. Der Web-Director leitet dann den Client an die Web-Engine mit der höchsten Verfügbarkeit um.

Abhängig von Ihrem Konfigurationstyp installiert CA SDM eine standardmäßige Web-Engine auf den folgenden Servern:

- Konventionell: Primärserver
- Erweiterte Verfügbarkeit: Alle Server.

Web-Directors

Web-Directors sind optional und werden verwendet, wenn zwei oder mehrere Web-Engines auf einem einzelnen Server installiert sind. WebDirector empfängt Verbindungsanfragen von Anwendern, wählt eine Web-Engine zur Bearbeitung der Anfrage und leitet die Anfrage an diese Web-Engine um. Dieses Verfahren für den Endanwender transparent: Er greift immer mit derselben URL auf CA SDM zu, unabhängig von der Anzahl der konfigurierten Web-Engines. Web-Directors können für folgende Zwecke verwendet werden:

- Konfigurieren von CA SDM für die effiziente Nutzung von Secure Sockets (SSL).

Das HTTPS-Protokoll erlaubt die Verschlüsselung von Webtransaktionen, wodurch maximale Sicherheit für sensible Daten, insbesondere Kennwörter geboten wird. Seiten, die SSL verwenden, können jedoch nicht im Browser-Cache gespeichert werden, was sich negativ auf die Leistung auswirken kann.
- Umleiten von Anmeldungen an eine bestimmte Web-Engine (oder Web-Engines).

Nach der Authentifizierung eines Anwenders kann WebDirector die Sitzung an eine andere Web-Engine auf dem gleichen oder auf einem anderen HTTP-Server verschieben. Mit diesem Setup können Sie SSL für eine Web-Engine konfigurieren und einen Schutz für Ihre Kennwörter bereitstellen, während ein HTTP-Protokoll für Transaktionen verwendet wird.
- Verwenden mehrerer WebDirector-Instanzen, von denen jede für eine andere Gruppe der Web-Engines zuständig ist.

Dies kann in Organisationen nützlich sein, die über verschiedene geografische Standorte verfügen, wenn Web-Engine-Gruppen physisch näher zu den betreffenden Endanwendern liegen sollen.

Aliasnamen

Aliasnamen sind leicht erkennbare Namen, die Sie für Slump-Namen der Objektmanager erstellen können. Sie können Aliasnamen für einen spezifischen Objektmanager oder für eine Gruppe von Objektmanagern erstellen. Diese Aliasnamen können anstelle eines Namens des Objektmanagers verwendet werden, während Sie die CA SDM-Prozesse konfigurieren. Aliasnamen sind in CA SDM optional.

Knowledge-Daemons

Nur auf einen konventionellen Konfigurationstyp anwendbar.

Knowledge-Daemons geben die Knowledge Base für CA SDM an (Knowledge-Dokumente, Genehmigungsvorgang, Berechtigungen, Benachrichtigungen usw.). CA SDM konfiguriert den Knowledge-Daemon standardmäßig auf dem Primärserver. Sie können den Daemon auf einen Sekundärserver verschieben, indem Sie den Hostnamen ändern.

Authentifizierung des angemeldeten Anwenders

Nur auf einen konventionellen Konfigurationstyp anwendbar.

CA SDM konfiguriert den Authentifizierungs-Daemon des angemeldeten Anwenders standardmäßig auf dem Primärserver. Sie können den Daemon auf einen Sekundärserver verschieben, indem Sie den Hostnamen ändern.

Virtuelle LDAP-DB

Nur auf einen konventionellen Konfigurationstyp anwendbar.

CA SDM konfiguriert den Daemon der virtuellen LDAP-Datenbank standardmäßig auf dem Primärserver. Sie können den Daemon auf einen Sekundärserver verschieben, indem Sie den Hostnamen ändern.

Repository-Daemons

Nur auf einen konventionellen Konfigurationstyp anwendbar.

Der Repository-Daemon ermöglicht es Ihnen, die Anhangsdatensätze im Repository-Verzeichnis zu speichern. Mithilfe der CA SDM-Web-Benutzeroberfläche können Sie die Prozesse nur für Sekundärserver hinzufügen. Nachdem Sie den Prozess über die Web-Benutzeroberfläche hinzugefügt haben, aktivieren Sie die spezifische Option während der CA SDM-Konfiguration. Weitere Informationen über das Aktivieren von Prozessen finden Sie in der *Online-Hilfe zur Serverkonfiguration*.

Visualizer

Nur auf einen konventionellen Konfigurationstyp anwendbar.

Sie können Visualizer auf einem CA SDM-Server konfigurieren, um Webservices zu verwenden. Mithilfe der CA SDM-Web-Benutzeroberfläche können Sie die Prozesse nur für Sekundärserver hinzufügen. Nachdem Sie den Prozess über die Web-Benutzeroberfläche hinzugefügt haben, aktivieren Sie die spezifische Option während der CA SDM-Konfiguration. Weitere Informationen über das Aktivieren von Prozessen finden Sie in der *Online-Hilfe zur Serverkonfiguration*.

REST-Webservices für Tomcat-Server

Nur auf einen konventionellen Konfigurationstyp anwendbar.

Mit REST-Webservices können Sie die Web-Benutzeroberfläche konfigurieren, sodass CA SDM mit der Außenwelt kommunizieren kann. Mithilfe der CA SDM-Web-Benutzeroberfläche können Sie die Prozesse nur für Sekundärserver hinzufügen. Nachdem Sie den Prozess über die Web-Benutzeroberfläche hinzugefügt haben, aktivieren Sie die spezifische Option während der CA SDM-Konfiguration. Weitere Informationen über das Aktivieren von Prozessen finden Sie in der *Online-Hilfe zur Serverkonfiguration*.

Support-Automatisierung

Nur auf einen konventionellen Konfigurationstyp anwendbar.

Mithilfe der CA SDM-Web-Benutzeroberfläche können Sie die Prozesse nur für Sekundärserver hinzufügen. Nachdem Sie den Prozess über die Web-Benutzeroberfläche hinzugefügt haben, aktivieren Sie die spezifische Option während der CA SDM-Konfiguration. Weitere Informationen über das Aktivieren von Prozessen finden Sie in der *Online-Hilfe zur Serverkonfiguration*. Sie können nur einen Support-Automatisierungsprozess für jeden Sekundärserver hinzufügen. Sie können folgende Support-Automatisierungsserver konfigurieren:

SA-Hauptserver

Gibt den Server an, auf dem die Support-Automatisierung installiert ist. Sie können den SA-Hauptserver nur auf einem Sekundärserver hinzufügen.

Für SA vorgesehener Objektmanagerserver

Der Server, auf dem sich der Objektmanager für die Support-Automatisierungskonfiguration befindet. Sie können den dedizierten Server des Objektmanagers auf einem Sekundärserver konfigurieren.

Hinweis: Sie können einen dedizierten Server des Objektmanagers nur hinzufügen, wenn der SA-Hauptserver konfiguriert ist.

SA-Nachrichtenroutingserver

Sie können den Nachrichtenroutingserver auf einem Sekundärserver konfigurieren, um mehrere Remote Control-Sitzungen zu verwalten und um die Leistung während der Unterstützungssitzungen zu verbessern.

SA-Socket-Proxy-Server

Sie können den Socket-Proxy-Server auf einem Sekundärserver konfigurieren, um den Hauptserver während CPU-intensiver Vorgänge der Support-Automatisierung, wie z. B. bei Verschlüsselung/Entschlüsselung, zu entlasten.

UNI Converter

Sie können einen UNI-Konverter zu einem beliebigen Server hinzufügen, der auf der Unix-Plattform ausgeführt wird. Sie können den UNI-Konverter zu folgenden Servern hinzufügen:

- Konventionell: Primärserver, Sekundärserver
- Erweiterte Verfügbarkeit: Anwendungsserver

TNG Converter

Sie können einen TNG-Konverter zu einem beliebigen Server hinzufügen, der auf der Windows-Plattform ausgeführt wird. Sie können den TNG-Konverter zu folgenden Servern hinzufügen:

- Konventionell: Primärserver, Sekundärserver
- Erweiterte Verfügbarkeit: Anwendungsserver

Hinweis: Wenn der Daemon-Manager den TNG-Konverter verwaltet, dann wird der Daemon mit den anderen Daemons gestartet und beendet. Wenn der TNG-Konverter Events erfassen soll, nachdem die CA SDM-Daemons heruntergefahren wurden, müssen Sie den Service "TNG-Konverter" starten und beenden.

Hinzufügen von Objektmanagern

Wenn Objektmanager zu CA SDM-Servern hinzugefügt werden, wird die gesamte Systemleistung verbessert. CA SDM installiert einen standardmäßigen Objektmanager auf allen Servern. Sie können den standardmäßigen Objektmanager nicht ändern, aber Sie können weitere Objektmanager auf einen beliebigen CA SDM-Server hinzufügen, um die Serverleistung zu erhöhen. Abhängig von Ihrem Konfigurationstyp installiert CA SDM einen standardmäßigen Objektmanager auf den folgenden Servern:

- Konventionell: Primärserver.
- Erweiterte Verfügbarkeit: Alle Server.

Gehen Sie wie folgt vor:

1. Wählen Sie auf der Registerkarte "Administration" die Option "System", "Konfigurationen" aus.
Die Seite Konfigurationsliste wird geöffnet.
2. Wählen Sie die Konfiguration aus, zu der Sie den Objektmanager hinzufügen möchten.
Die Seite "Konfigurationsdetail" wird geöffnet.
3. Wählen Sie die Registerkarte "Objektmanager" aus.
Die Seite "Objektmanager - Liste" wird geöffnet, die die Objektmanager anzeigt, die für den Server konfiguriert sind. Der standardmäßige Objektmanager (sofern vorhanden) wird ebenfalls in der Liste angezeigt.
4. Klicken Sie auf "Objektmanager hinzufügen".
Die Seite "Neuen Objektmanager erstellen" wird geöffnet.
5. Füllen Sie die folgenden Felder aus:

Wichtig! Geben Sie nur englische Zeichen in die Eingabefelder lokalisierter Sprachen ein.

Hostname

Gibt den Hostnamen an, zu dem Sie den Objektmanager hinzufügen möchten. Sie können auf die Schaltfläche Suchen klicken, um nach Servern zu suchen, die zu Ihrer CA SDM-Installation hinzugefügt wurden.

Für einen Konfigurationstyp für erweiterte Verfügbarkeit ist der Hostname schreibgeschützt und wird basierend auf dem Hostnamen, den Sie während der Konfigurationserstellung angegeben haben, automatisch aufgefüllt.

Anzeigename

Gibt einen Anzeigenamen für den Objektmanager an. Der Anzeigename wird auf den Clients angezeigt, um anzugeben, zu welchem Objektmanager eine Verbindung hergestellt ist.

Objektmanagergruppe

Der Gruppenname, zu dem der Objektmanager hinzugefügt wird.

Wichtig! Geben Sie nur englische Zeichen für den Objektgruppennamen lokalisierter Sprachen ein.

Sie können Objektmanager gruppieren, damit die Gruppen zugewiesen werden können, die bestimmte Gruppen von Web-Engines bedienen. Anwender, die die Gruppenfunktion benötigen, haben häufig Web-Engines, die geografisch vom Primärserver getrennt sind. In diesem Fall soll ein Objektmanager in der Nähe der Web-Engine liegen. Die Anwender gruppieren die Objektmanager, die den lokalen Web-Engines zugewiesen sind, und weisen dann dieser Gruppe von Objektmanagern die Web-Engines zu.

Akzeptierungsmaske

Gibt die Maske für den Objektmanager an. Die Akzeptierungsmaske ist eine Funktion. Sie teilt dem Objektmanager mit, von welchen Clients er Verbindungen annehmen soll.

Zum Beispiel versucht eine Web-Engine, eine Verbindung zu einem Objektmanager mit Namen wie "web:seattle:1", "web:seattle:2" oder "web:texas:1" herzustellen. Sie können eine Akzeptierungsmaske wie z. B. "web:seattle.*" angeben, um alle Seattle-Verbindungen anzunehmen und andere abzulehnen. Sie können auch die Maske "web:.*" angeben, um Verbindungen von Web-Engines anzunehmen und Verbindungen von Clients abzulehnen.

Datensatzstatus

Gibt an, ob der Objektmanager aktiv oder inaktiv ist.

Hinweis: Bevor Sie den Datensatzstatus eines Objektmanagers auf "Inaktiv" festlegen, müssen Sie die Verknüpfung zwischen dem Objektmanager und den verknüpften Web-Engines entfernen.

6. Klicken Sie auf "Speichern".

Der Objektmanager, den Sie hinzugefügt haben, wird in der Liste "Objektmanager" angezeigt.

Hinzufügen von Web-Engines oder Web-Directors

Web-Engines stellen eine Verbindung zu einem Objektmanager her, um alle Requests für CA SDM-Objekte zu verarbeiten. Web-Directors sind optional und werden verwendet, wenn zwei oder mehrere Web-Engines auf einem einzelnen Server installiert sind. Sie können Web-Directors auf einem beliebigen Server konfigurieren. Abhängig von der CA SDM-Konfiguration installiert CA SDM eine standardmäßige Web-Engine auf den folgenden Servern:

- Konventionell: Primärserver.
- Erweiterte Verfügbarkeit: Alle Server.

Gehen Sie wie folgt vor:

1. Wählen Sie auf der Registerkarte Administration die Option Systeme, Konfigurationen.

Die Seite Konfigurationsliste wird geöffnet.

2. Wählen Sie die Konfiguration aus, der Sie die Web-Engine oder den Web-Director hinzufügen möchten.

Die Seite "Konfigurationsdetail" wird geöffnet.

Hinweis: Wenn Sie die Konfiguration zum ersten Mal ändern, dann erstellen Sie zuerst eine Konfiguration. Wenn Sie eine Konfigurationsänderung vornehmen möchten, erstellen Sie immer eine neue Konfiguration, oder kopieren Sie eine vorhandene. Dieser Prozess ermöglicht es Ihnen, bei Bedarf zur früheren Konfiguration zurückzukehren.

3. Wählen Sie die Registerkarte "Web-Engines/Web-Directors" aus.

Die Seite Web-Engines/Web-Directors - Liste wird geöffnet, auf der die für den Server konfigurierten Web-Engines und Web-Directors aufgeführt sind.

- Konventionell: Eine Web-Engine ist standardmäßig auf dem Primärserver vorhanden. Sie können Web-Directors zu einem beliebigen Server hinzufügen.
- Erweiterte Verfügbarkeit: Eine Web-Engine ist standardmäßig auf allen Servern vorhanden. Sie können weitere Web-Directors auf einem beliebigen CA SDM-Server hinzufügen.

4. Klicken Sie auf "Web-Engine/Web-Director hinzufügen".

Die Seite "Neue Web-Engine/Web-Directors erstellen" wird geöffnet.

5. Füllen Sie die folgenden Felder aus:

Wichtig! Geben Sie nur englische Zeichen in die Eingabefelder lokalisierter Sprachen ein.

Hostname

Gibt den Hostnamen für die Web-Engine oder den Web-Director an. Sie können auf Suchen klicken, um die Server zu suchen.

Für einen Konfigurationstyp für erweiterte Verfügbarkeit ist der Hostname schreibgeschützt und wird basierend auf dem Hostnamen, den Sie während der Konfigurationserstellung angegeben haben, automatisch aufgefüllt.

Typ

Gibt an, ob Sie eine Web-Engine oder einen Web-Director konfigurieren. Basierend auf der ausgewählten Option werden die zugehörigen Felder automatisch aufgefüllt.

- Wählen Sie "Web-Engine" aus, wenn Sie eine Web-Engine konfigurieren möchten.
- Wählen Sie "Web-Director" aus, wenn Sie einen Web-Director konfigurieren möchten.

Hinweis: Stellen Sie sicher, dass Sie die entsprechende Option ausgewählt haben. Sie können den Prozesstyp nicht bearbeiten, nachdem Sie die Konfiguration gespeichert haben.

Web Director

Gibt den Web-Director an, der mit der Web-Engine verknüpft ist. Sie können auf Suchen klicken, um die Web-Directors zu suchen, die dem Server hinzugefügt wurden.

Hinweis: Beim Implementieren eines beliebigen Lastenausgleichschemas, einer beliebigen SSL-Anmeldung oder beiden für die Web-Engine, müssen demselben Web-Director mindestens zwei Web-Engines zugewiesen werden.

CGI Name

Gibt den eindeutigen CGI-Namen für die Web-Engine an. Dieser Wert ist der Name einer ausführbaren CGI-Datei, wenn IIS oder Apache als HTTP-Server verwendet wird. Er ist ein Servlet-Parameter bei Verwendung von Tomcat als HTTP-Server.

Beispiele: (Web-Engines) "pdmweb1", "pdmweb2", (Web-Directors) "pdmweb_d1" und "pdmweb_d2".

Standard: pdmweb.exe (Der CGI-Name muss eindeutig sein).

CGI-Portnummer

Gibt den Port an, auf dem CA SDM-Webclients eine Verbindung herstellen können. Die CGI-Portnummer ist der gleiche Port, auf dem der Tomcat-Server ausgeführt wird.

Standard: 8080

Protokoll

Gibt das Protokoll für den Zugriff auf die Web-Engine an.

- Wählen Sie "HTTPS" aus, wenn die Web-Engine für die Verarbeitung aller Requests zur Anwenderauthentifizierung von CA SDM-Webclients konfiguriert ist.
- Wählen Sie "HTTP" aus, wenn die Web-Engine für die Verarbeitung aller Requests zur Nicht-Anwenderauthentifizierung von Webclients konfiguriert ist (nachdem der Anwender über die Web-Engine für sichere Anmeldung authentifiziert wurde).

Datensatzstatus

Gibt an, ob die Web-Engine oder der Web-Director aktiv oder inaktiv ist.

Hinweis: Bevor Sie den Datensatzstatus eines Web-Directors auf "Inaktiv" festlegen, entfernen Sie die Verknüpfung zwischen dem Web-Director und den zugewiesenen Web-Engines.

Objektmanager

Gibt den Objektmanager an, den Sie der Web-Engine zuweisen möchten.

Standard

Gibt an, dass der standardmäßige Objektmanager der Web-Engine zugewiesen ist.

BELIEBIGE

Gibt an, dass die Web-Engine eine Verbindung mit einem verfügbaren Objektmanager mit höherem "Willingness"-Wert herstellen kann. Der "Willingness"-Wert ist die Verfügbarkeit des Servers, neue Clients zu akzeptieren. Ein "Willingness"-Wert von null bedeutet, dass die Web-Engine keine Sitzungen annimmt.

Auswählen

Ermöglicht es Ihnen, einen Objektmanager für die Web-Engine anzugeben. Wenn Sie diese Option auswählen, können Sie der Konfiguration mehrere Objektmanager oder Aliasnamen hinzufügen.

6. Klicken Sie auf "Speichern".

Die Web-Engine oder der Web-Director, die bzw. den Sie hinzugefügt haben, wird in "Web-Engines/Web-Directors - Liste" angezeigt.

Hinzufügen von Aliasnamen

Aliasnamen sind in CA SDM optional. Sie können Aliasnamen für einen spezifischen Objektmanager oder für eine Gruppe von Objektmanagern erstellen. Bevor Sie Aliasnamen erstellen, führen Sie folgende Aufgaben durch:

- Definieren Sie Objektmanager, und fügen Sie einige Gruppen hinzu.
Zum Beispiel: "domsrvr:group1:11", "domsrvr:seattle:12", "domsrvr:seattle:13", "domsrvr:Tacoma:11".
- Geben Sie einen regulären Ausdruck ein, der mit einer Gruppe von Objektmanagern übereinstimmt.
Angenommen, die Java-Clients in Washington sollen eine Verbindung zu Objektmanagern in Seattle herstellen. Sie verbinden sie mit "/domsrvr:seattle.*". Sie können aber auch den Aliasnamen "SEATTLE" definieren und ihm den Wert "/domsrvr:seattle.*" zuweisen.
- Definieren Sie Web-Engines, und weisen Sie Aliasnamen zu den Web-Engines zu.

Wichtig! Wenn Sie Aliasnamen für eine Objektmanagergruppe erstellt haben, stellen Sie sicher, dass Sie die jeweiligen Aliasnamen ändern, nachdem Sie die Objektmanagergruppe geändert haben.

Gehen Sie wie folgt vor:

1. Wählen Sie auf der Registerkarte "Administration" die Option "System", "Konfigurationen" aus.
Die Seite Konfigurationsliste wird geöffnet.
2. Wählen Sie die Konfiguration aus, zu der Sie den Alias hinzufügen möchten.
Die Seite "Konfigurationsdetail" wird geöffnet.
3. Klicken Sie auf die Registerkarte "Aliasnamen".
Die Seite "Alias - Liste" wird geöffnet und zeigt die Aliasnamen an, die für den Server erstellt wurden.
4. Klicken Sie auf "Alias hinzufügen".
Die Seite "Neuen Alias erstellen" wird geöffnet.

5. Füllen Sie die folgenden Felder aus:

Wichtig! Geben Sie nur englische Zeichen in die Eingabefelder lokalisierter Sprachen ein.

Name

Gibt den Namen für den Aliasnamen an, den Sie erstellt haben.

Definition

Gibt den regulären Ausdruck an, der mit dem Aliasnamen verknüpft ist.
Folgendes Format wird für eine Alias-Definition verwendet:

```
domsrvr: [[set the product group or  
family]] [<host_id><id>][.*]
```

Default: /domsrvr.*

Datensatzstatus

Gibt an, ob der Aliasname aktiv oder inaktiv ist.

6. Klicken Sie auf "Speichern".

Der Aliasname, den Sie hinzugefügt haben, wird in der Aliasliste angezeigt.

Hinzufügen von zusätzlichen Prozessen

CA SDM ermöglicht es Ihnen, Support-Automatisierungsserver, Visualizer, LDAP, KT, TNG/UNI, BopLogin-Repository-Daemons und REST-Webservices-Prozesse für einen Server zu konfigurieren.

Gehen Sie wie folgt vor:

1. Wählen Sie auf der Registerkarte Administration die Option Systeme, Konfigurationen.
Die Seite Konfigurationsliste wird geöffnet.
2. Wählen Sie die Konfiguration aus, zu der Sie die zusätzlichen Prozesse hinzufügen möchten.
Die Seite "Konfigurationsdetail" wird geöffnet.
3. Wählen Sie die Registerkarte "Zusätzliche Prozesse" aus.
Unter Zusätzlicher Prozess - Liste wird die Liste von Prozessen angezeigt, die für den Server mit den Standardprozessen konfiguriert wurden, falls zutreffend.

4. Klicken Sie auf "Prozess hinzufügen".

Die Seite "Neuen Prozess erstellen" wird geöffnet.

5. Füllen Sie die folgenden Felder nach Wunsch aus:

Wichtig! Geben Sie nur englische Zeichen in die Eingabefelder lokalisierter Sprachen ein.

Prozess

Zeigt den CA SDM-Serverprozess an, den Sie hinzufügen möchten.

Repository-Daemon

Nur auf einen konventionellen Konfigurationstyp anwendbar.

Gibt den Repository-Daemon an, der für den Server konfiguriert ist. Repository-Daemons unterstützen Anhang-Repositorys. CA SDM konfiguriert einen Repository-Daemon standardmäßig auf dem Primärserver. Sie können den Daemon auf einen Sekundärserver verschieben, indem Sie den Hostnamen ändern.

SA-Hauptserver

Nur auf einen konventionellen Konfigurationstyp anwendbar.

Gibt den SA-Hauptserver an, der für den Server konfiguriert ist. Sie können nur einen SA-Hauptserver konfigurieren.

Für SA vorgesehener Objektmanagerserver

Nur auf einen konventionellen Konfigurationstyp anwendbar.

Gibt den dedizierten Objektmanager für die Support-Automatisierungskonfiguration an. Sie können nur einen dedizierten Objektserver entweder auf dem Primärserver oder auf dem Sekundärserver angeben.

Hinweis: Sie können einen dedizierten Server des Objektmanagers nur hinzufügen, wenn der SA-Hauptserver konfiguriert ist.

SA-Nachrichtenroutingserver

Nur auf einen konventionellen Konfigurationstyp anwendbar.

Gibt den Nachrichtenroutingserver an, der für den Server konfiguriert ist. Sie können den Nachrichtenroutingserver auf einem Sekundärserver konfigurieren, um mehrere Remote Control-Sitzungen zu verwalten und um die Leistung während der Unterstützungssitzungen zu verbessern.

SA-Socket-Proxy-Server

Nur auf einen konventionellen Konfigurationstyp anwendbar.

Gibt den Socket-Proxy-Server an, der für den Server konfiguriert ist. Sie können den Socket-Proxy-Server auf einem Sekundärserver konfigurieren, um den Hauptserver während CPU-intensiver Vorgänge, wie z. B. bei Verschlüsselung/Entschlüsselung, zu entlasten.

REST-Webservices für Tomcat-Server

Nur auf einen konventionellen Konfigurationstyp anwendbar.

Gibt die REST-Webservices an, die für den Server konfiguriert sind. Mit REST-Webservices können Sie die Web-Benutzeroberfläche konfigurieren, sodass CA SDM mit der Außenwelt kommunizieren kann. Mithilfe der CA SDM-Web-Benutzeroberfläche können Sie die Prozesse nur für Sekundärserver hinzufügen. Nachdem Sie den Prozess über die Web-Benutzeroberfläche hinzugefügt haben, aktivieren Sie die spezifische Option während der CA SDM-Konfiguration. Weitere Informationen über das Aktivieren von Prozessen finden Sie in der *Online-Hilfe zur Serverkonfiguration*.

TNG Converter

Sie können einen TNG-Konverter zu einem beliebigen Server hinzufügen, der auf der Windows-Plattform ausgeführt wird. Sie können den TNG-Konverter zu folgenden Servern hinzufügen:

Konventionell: Primärserver, Sekundärserver.

Erweiterte Verfügbarkeit: Anwendungsserver.

Hinweis: Wenn der Daemon-Manager den TNG-Konverter verwaltet, wird dieser Daemon mit den anderen Daemon gestartet und beendet. Wenn der TNG-Konverter Events erfassen soll, nachdem die CA SDM-Daemons heruntergefahren wurden, müssen Sie den Service "TNG-Konverter" starten und beenden.

UNI Converter

Gibt den UNI-Konverter an, der konfiguriert ist, um auf UNIX-Events zu reagieren. Diese Events können gefiltert und konfiguriert werden, um Tickets zu erstellen und um andere Aufgaben in Service Desk auszulösen. Sie können einen UNI-Konverter zu einem beliebigen Server hinzufügen, der auf der Unix-Plattform ausgeführt wird. Sie können den UNI-Konverter zu folgenden Servern hinzufügen:

Konventionell: Primärserver, Sekundärserver.

Erweiterte Verfügbarkeit: Anwendungsserver.

Visualizer-Tomcat-Server

Nur auf einen konventionellen Konfigurationstyp anwendbar.

Gibt den Visualizer an, der für den Server konfiguriert ist.

Sie können Visualizer auf einem CA SDM-Server konfigurieren, um Webservices zu verwenden. Mithilfe der CA SDM-Web-Benutzeroberfläche können Sie die Prozesse nur für Sekundärserver hinzufügen. Nachdem Sie den Prozess über die Web-Benutzeroberfläche hinzugefügt haben, aktivieren Sie die spezifische Option während der CA SDM-Konfiguration. Weitere Informationen über das Aktivieren von Prozessen finden Sie in der *Online-Hilfe zur Serverkonfiguration*.

Hinweis: Sie können nur einen Visualizer-Tomcat-Server auf einem Sekundärserver konfigurieren.

Hostname

Gibt den Server an, der den von Ihnen hinzugefügten Prozess hostet. Sie können auf die Schaltfläche "Suchen" klicken, um nach den Servern zu suchen.

Datensatzstatus

Gibt an, ob der von Ihnen hinzugefügte Prozess aktiv oder inaktiv ist.

6. Klicken Sie auf "Speichern".

Der von Ihnen hinzugefügte Prozess wird auf der Seite "Zusätzlicher Prozess - Liste" angezeigt.

Überprüfen der Konfiguration

- Nach Abschluss der Konfiguration und nachdem die Services ordnungsgemäß gestartet wurden, führen Sie "pdm_status" oder den Task-Manager-Befehl aus, um zu überprüfen, ob die neuen Daemons hinzugefügt wurden.
- Überprüfen Sie, ob die aktuelle Konfiguration mit der Konfiguration aktualisiert wurde, die Sie während "pdm_configure" ausgewählt haben.

Kapitel 3: REST-Beispieloberfläche für Mobilgeräte

Diese REST-Beispieloberfläche für Mobilgeräte enthält zwei Benutzeroberflächen: für Analysten und für Mitarbeiter. Die Rollen "Administrator", "Level 1-Analyst" und "Mitarbeiter" werden in diesem Beispiel ebenfalls unterstützt. Wenn Sie sich bei CA SDM angemeldet haben, wird für Anwender mit den Rollen "Administrator" und "Level 1-Analyst" die Analystenschnittstelle angezeigt. Für Anwender mit der Rolle "Mitarbeiter" wird nur die Mitarbeiterschnittstelle angezeigt. Bei ungültigen Anmeldungen lehnt CA SDM die Anmeldungsanfrage ab und zeigt eine Meldung an. Wenn ein Administrator die automatische Berechnung der Prioritäten deaktiviert hat, wird das Feld "Priorität" auf Erstellungs- und Bearbeitungsseiten angezeigt.

Wichtig! Diese Funktionalität gilt nur für das in CA SDM Version 12.9 enthaltene Beispielprogramm. Es ist kein beschränktes Design in der REST-Webserviceanwendung.

Felder, die automatische Empfehlungen verwenden, benötigen eine Wertauswahl in der Liste der automatischen Vorschläge wie beispielsweise den Bereich für Verantwortlichen und Incidents. Wenn Sie keinen Wert auswählen, wird die Anwendereingabe für dieses Feld gelöscht.

Hinweis: Wir empfehlen, dass Sie für das Navigieren auf REST-Schnittstellen anstelle der Browseroptionen die vorhandenen Schaltflächen verwenden. Verwenden Sie beispielsweise "Startseite" oder "Abbrechen", um zu einer früheren Seite zurückzukehren.

Sie konfigurieren REST im Zuge der CA SDM-Konfiguration, müssen die Beispieloberfläche für Mobilgeräte aber [manuell](#) (siehe Seite 95) aktivieren.

Analysten können die folgenden Aufgaben ausführen:

- Ankündigungen anzeigen.
Standard: Nach Bereitstellungsdatum sortiert
- Incidents anzeigen, die CA SDM dem Analysten zugewiesen hat.
- Zugewiesene Incidents und Incidents mit aufgehobener Zuweisung anzeigen.
- Incidents sortieren.
Standard: Nach Öffnungsdatum sortiert
- Nach Incidents suchen.
- Erstellen von Incidents.

- Status, Dringlichkeit und Auswirkung des Incident ändern.
- Das Aktivitätsprotokoll anzeigen und mit Kommentaren aktualisieren oder "Rückruf" oder "Nachforschung" angeben.

Standard: Nach Aktivitätsdatum sortiert.

Mitarbeiter können die folgenden Aufgaben ausführen:

- Ankündigungen anzeigen.
- Offene und geschlossen Incidents anzeigen, die ein Endanwender erstellt hat.
- Incidents sortieren, beispielsweise nach Öffnungsdatum.
- Erstellen von Incidents.
- Das Aktivitätsprotokoll mit einem Kommentar aktualisieren.
- Nach Incidents suchen.
- Incident-Status von "Offen" in "Geschlossen" oder von "Geschlossen" in "Offen" ändern.

Hinweis: Ein Sternchen bedeutet, dass ein Feld erforderlich ist.

Dieses Kapitel enthält folgende Themen:

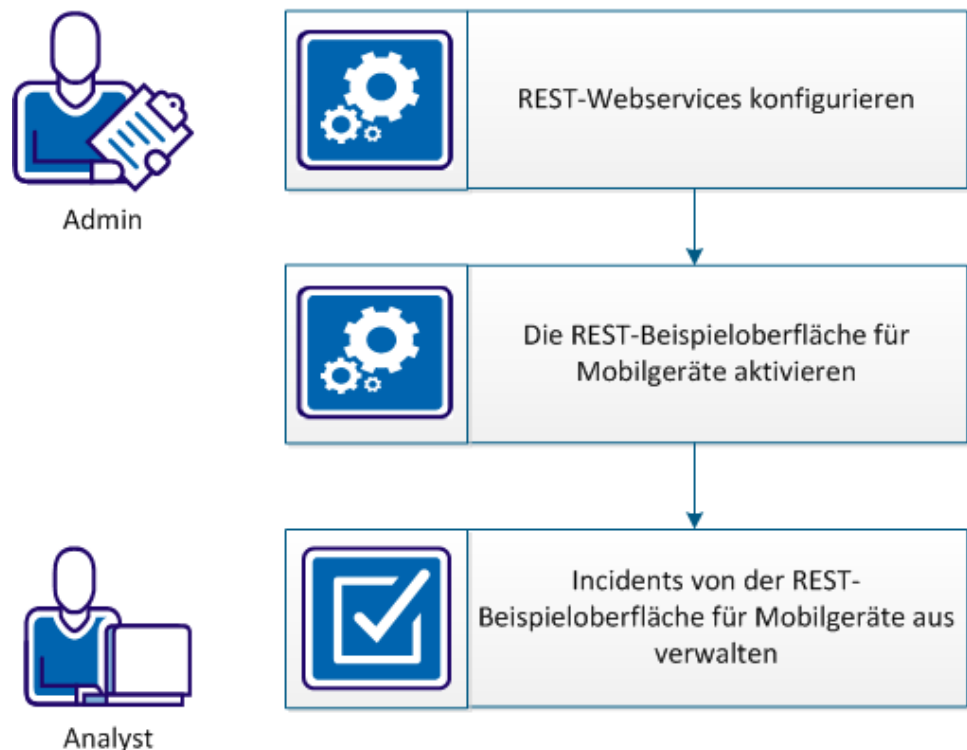
[So stellen Sie REST-Beispieloberfläche für Mobilgeräte bereit](#) (siehe Seite 93)

So stellen Sie REST-Beispieloberfläche für Mobilgeräte bereit

Mit der REST-Beispieloberfläche für Mobilgeräte können Service Desk-Analysten Incidents auf Mobilgeräten verwalten. Der Administrator aktiviert REST-Webservices während der Produktkonfiguration und kopiert Dateien auf den CA SDM-Computer, um die REST-Beispieloberfläche für Mobilgeräte zu aktivieren. Der Analyst verwendet die mobile Schnittstelle, um Incidents zu verwalten, die Endanwender in CA SDM öffnen.

Folgendes Diagramm erklärt, wie ein Administrator REST-Webservices aktiviert, damit der Analyst Incidents in der Warteschlange verwalten kann:

Bereitstellen der REST-Beispieloberfläche für Mobilgeräte



Gehen Sie wie folgt vor:

1. [REST-Webservices konfigurieren](#) (siehe Seite 94).
2. [Mobile REST-Beispieloberfläche für Mobilgeräte aktivieren](#) (siehe Seite 95).
3. [Verwalten Sie Incidents über die REST-Beispieloberfläche für Mobilgeräte](#) (siehe Seite 95).

Konfigurieren von REST-Webservices

Der Administrator aktiviert REST-Webservices während der CA SDM-Konfiguration. Standardmäßig werden durch die CA SDM-Konfiguration keine REST-Webservices aktiviert.

Gehen Sie wie folgt vor:

1. Führen Sie *eine* der folgenden Aktionen aus:
 - Installieren Sie CA SDM und warten Sie, dass das Dialogfeld "Konfiguration" angezeigt wird.
 - Wenn Sie CA SDM bereits installiert haben und bisher keine REST-Webservices konfiguriert hatten, führen Sie in der Befehlszeile `pdm_configure` aus. Klicken Sie unter Windows auf Start, Programme, CA, Service Desk Manager, Konfigurieren.

Das Dialogfeld "Konfiguration" wird geöffnet.

2. Bestätigen Sie die Konfigurationsinformationen für die Dialogfelder Allgemeinen Einstellungen, Systemkonten, Datenbank und Web-Schnittstelle.

Das Dialogfeld REST-Webservices wird geöffnet.

3. Aktivieren Sie die Option REST-Webservices konfigurieren.
4. Geben Sie den REST-Tomcat-Port an.

Standard: 8050

5. Geben Sie den REST-Tomcat-Endpoint an.

Standard: 8055

6. Klicken Sie auf Weiter, und fahren Sie mit der CA SDM-Konfiguration fort.

Die Konfiguration wird abgeschlossen.

Aktivieren der mobilen REST-Beispieloberfläche für Mobilgeräte

CA SDM deaktiviert die REST-Beispieloberfläche für Mobilgeräte standardmäßig, um unerwünschten Zugriff auf die MDB zu verhindern. Der Administrator aktiviert diese Schnittstelle manuell.

Gehen Sie wie folgt vor:

1. Suchen Sie das folgende Verzeichnis auf den CA SDM-Computer, wo REST-Webservices installiert und konfiguriert sind:

`$NX_ROOT/samples/sdk/rest/mobiledemo`

2. Kopieren Sie dieses Verzeichnis zum folgenden Speicherort:

`$NX_ROOT/bopcfg/www/CATALINA_BASE_REST/webapps`

Hinweis: Sie müssen Tomcat nicht neu starten.

Die REST-Beispieloberfläche für Mobilgeräte ist aktiviert.

3. (Optional) Wenn Sie die REST-Beispieloberfläche für Mobilgeräte deaktivieren wollen, entfernen das Verzeichnis "mobiledemo" aus /webapps.

Verwalten von Incidents über die REST-Beispieloberfläche für Mobilgeräte

Der Analyst oder ein Mitarbeiter zeigt die REST-Beispieloberfläche für Mobilgeräte auf seinem mobilen Gerät an, um Incidents in der Warteschlange zu verwalten. Zum Beispiel öffnet der Analyst Incident 30, um einen internen Kommentar hinzuzufügen.

Gehen Sie wie folgt vor:

1. Öffnen Sie die folgenden URLs auf Ihrem mobilen Gerät:

`http://hostname:REST-Tomcat-port/mobiledemo/login.html`

Die Anmeldeseite der REST-Beispieloberfläche für Mobilgeräte wird geöffnet.

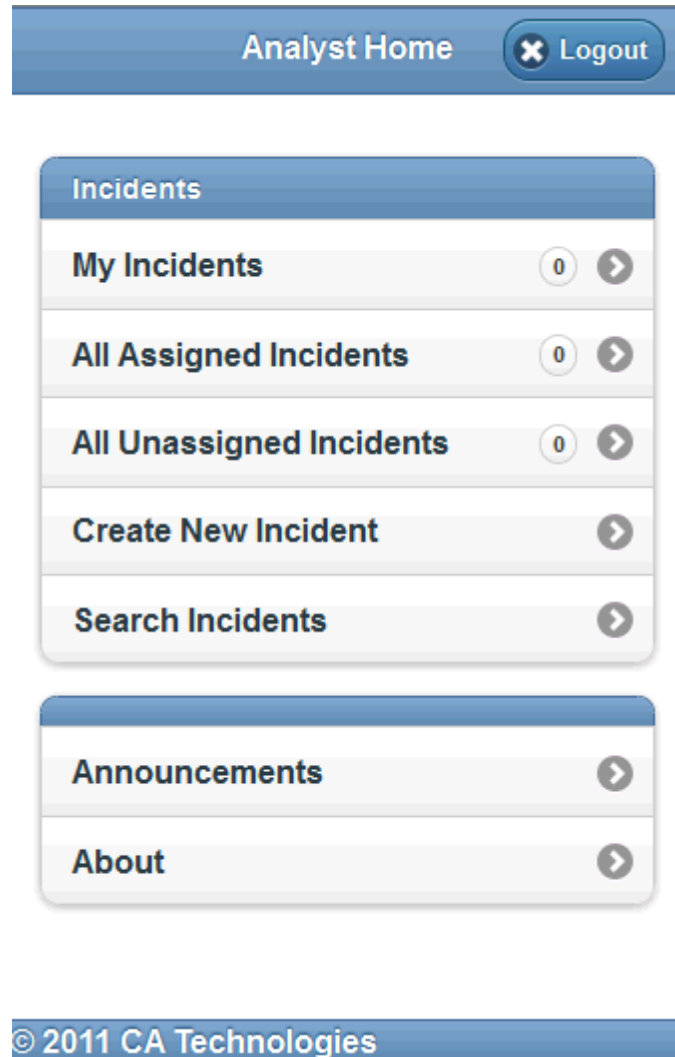
2. Melden Sie sich unter Verwendung Ihrer Anmeldeinformationen bei CA SDM an.

Die REST-Analystenstartseite für Mobilgeräte wird angezeigt.

3. Wählen Sie "Zugewiesene Incidents" aus.
4. Wählen Sie einen Incident, z. B. Incident 30, aus.
5. Wählen Sie auf der Detailseite "Aktivität erstellen" aus.
6. Wählen Sie in der Drop-down-Liste "Kommentar hinzufügen" aus.
7. Wählen Sie für die Option "Intern" den Wert "Ja" aus.
8. Geben Sie einen Kommentar ein, und wählen Sie Speichern aus.

Beispiel: Startseite der Analystenschnittstelle

Die folgende Abbildung zeigt die Analystenstartseite der REST-Beispieloberfläche für Mobilgeräte:



Beispiel: Startseite der Mitarbeiterschnittstelle

Die folgende Abbildung zeigt die Mitarbeiterstartseite der REST-Beispieloberfläche für Mobilgeräte:

The screenshot displays the 'Employee Home' page. At the top, there is a blue header bar with the text 'Employee Home' and a 'Logout' button with a red 'X' icon. Below the header, the page is divided into two main sections. The first section, titled 'Customer Service', contains three items: 'Create a new Incident' with a right-pointing arrow, 'Announcements' with a right-pointing arrow, and 'About' with a right-pointing arrow. The second section, titled 'Look up my existing tickets', contains two items: 'My open incidents' with a circular counter showing '0' and a right-pointing arrow, and 'My closed incidents' with a circular counter showing '0' and a right-pointing arrow. Below these sections is a 'Look up Incident Number' section with a text input field and a blue 'Go' button with a star icon. At the bottom of the page, there is a blue footer bar with the text '© 2011 CA Technologies'.

Beispiel: Der Mitarbeiter erstellt einen Incident

In diesem Beispiel meldet sich ein Mitarbeiter bei der REST-Schnittstelle auf dem Server an, um einen Incident für ein Netzwerkproblem auf seinem Computer zu erstellen.

Gehen Sie wie folgt vor:

1. Der Mitarbeiter meldet sich auf der mobilen der REST-Oberfläche an.
2. Der Mitarbeiter "Neuen Incident Erstellen" aus.
3. Der Mitarbeiter gibt die folgenden Informationen ein:
 - Er gibt seine Telefonnummer ein.
 - Er gibt seine E-Mail-Adresse ein.
 - (Erforderlich) Er wählt in der Drop-down-Liste "Dringlichkeit" "3-Bald" aus.
 - Er gibt **Netzwerk** als Incident-Bereich ein.
 - Er gibt eine Zusammenfassung des Incident ein.

Zum Beispiel sagt die Zusammenfassung aus, dass der Mitarbeiter auf einem Laptop nicht auf das Unternehmensnetzwerk zugreifen kann.
 - (Erforderlich) Er gibt eine Beschreibung des Incident ein.

Zum Beispiel gibt die Beschreibung den Namen des Endanwenderlaptops mit Netzwerk- und Hardwaredetails an.
4. Der Mitarbeiter wählt "Speichern" aus.

Der Incident wird erstellt, und eine Meldung zeigt die Incident-Nummer an.

Kapitel 4: CA SDM Mobile Enabler-Konfiguration

CA SDM Mobile Enabler r2.0 wird jetzt mit CA SDM Version 12.9 bereitgestellt. Als ein Administrator müssen Sie einige Konfigurationsschritte ausführen, damit die Anwender die mobile Anwendung verwenden können.

Dieses Kapitel enthält folgende Themen:

[CA SDM Mobile Enabler](#) (siehe Seite 99)

[Überprüfen der Voraussetzungen](#) (siehe Seite 105)

[Anwenden der Patches auf Open Space](#) (siehe Seite 106)

[\(Optional\) Festlegen von Formularfeldern als nicht erforderlich](#) (siehe Seite 109)

[\(Optional\) Erzwingen der Genehmigungsvereinbarkeit nach Aktualisierung](#) (siehe Seite 110)

[Zugreifen auf CA SDM-Mobile Enabler](#) (siehe Seite 110)

CA SDM Mobile Enabler

CA SDM Mobile Enabler ist eine gemeinsame Oberfläche zum Zugreifen auf einige Kernfunktionen von CA SDM und Open Space über Ihr Mobilgerät. Die folgenden mobilen Funktionen sind in CA SDM Mobile Enabler verfügbar:

- [Analyst Queue](#) (siehe Seite 100): Zeigen Sie in CA SDM erstellte Tickets an, und führen Sie Aktivitäten dafür aus.
- [Genehmigungen](#) (siehe Seite 101): Genehmigen Sie zugewiesene, von einer Workflow-Engine erstellte Arbeitselemente, oder reagieren Sie darauf.
- [Open Space](#) (siehe Seite 104): Veröffentlichen Sie Beiträge in Communitys oder beantworten Sie Fragen; wenn die Community Ihre Fragen nicht beantworten kann, erstellen Sie ein Ticket.

Sie können die Funktionen wählen, die Sie auf der Anmeldeseite verwenden möchten, wenn Sie sich bei CA SDM Mobile Enabler anmelden. Sie können eine Funktion nach der Anmeldung auch aktivieren oder deaktivieren. Gehen Sie zum Fenster "Einstellungen", und tippen Sie auf die Option zum Hinzufügen und Entfernen von Funktionen. Es werden nur solche Funktionen zur Auswahl angezeigt, die in Mobile Enabler hinzugefügt wurden. Wischen Sie, um die Funktion zu aktivieren, geben Sie die Anmeldedaten ein, und tippen Sie auf "Anmelden".

Analyst-Warteschlange

Die Analyst-Warteschlangenfunktion ermöglicht dem angemeldeten Anwender, auf die folgenden CA SDM-Kernfunktionen zuzugreifen:

- Anzeigen der Anzahl der Tickets von CA SDM auf dem Startbildschirm beim Anmelden (nur Incidents, Requests, Probleme, Issues, Changes). Die Abzeichenanzahl auf jeder Kachel zeigt die neue und aktualisierte Anzahl von Tickets seit der letzten Aktualisierung.

Hinweis: Der Startbildschirm zeigt nicht alle Tickets von CA SDM an. Standardmäßig werden hier alle zugewiesenen Tickets aller Anwender angezeigt. Dieser Standardfilter kann geändert werden.

- Tippen Sie auf eine Kachel für einen Tickettyp auf dem Startbildschirm, um die Liste der Tickets anzuzeigen. Filtern Sie die einzelnen Tickettypen, um nur ausgewählte Informationen anzuzeigen. Tippen Sie zum Beispiel in der Incident-Liste auf das Filtersymbol, und wählen Sie "Zugewiesen - Hohe Priorität". Die Liste wird so aktualisiert, dass nur die ausgewählten Incidents angezeigt werden.

Hinweis: Bei dieser Funktion werden ebenfalls solche Filter angezeigt, die auf dem CA SDM-Server angepasst wurden und auf dem CA SDM-Scoreboard angezeigt werden.

- Suchen Sie nach dem Ticket. Tippen Sie auf den Suchbereich, und geben Sie das Suchschlüsselwort ein. Die Suchergebnisse werden angezeigt, während Sie tippen. Sie können anhand der Ticketnummer oder der Zusammenfassung des Tickets nach einem Ticket suchen.
- Tippen Sie auf ein Ticket, um die Details anzuzeigen. Sie können auch die Anhänge und Aktivitätsprotokolle anzeigen (falls vorhanden).
- Tippen Sie auf "Weitere Aktionen" (Pfeilsymbol in der oberen rechten Ecke der Funktion), um Aktionen für ein Ticket auszuführen:
 - Eskalieren oder aktualisieren Sie den Status, oder übertragen Sie das Ticket an einen anderen Anwender.
 - Fügen Sie dem Ticket einen Kommentar hinzu.
 - Fügen Sie dem Ticket einen Anhang hinzu. Ein Anhang darf höchstens 3 MB groß sein.
 - Verwenden Sie die Kamera, um einen Snapshot aufzunehmen.
 - Verwenden Sie die Galerie, um ein Bild auszuwählen (es werden nur die Bildformate .jpeg, .jpg und .png für diese Funktion unterstützt).

Wichtig! Um Anhänge über die Webanwendung von CA SDM-Mobile Enabler anzeigen zu können, deaktivieren Sie im Webbrowser die Option zum Blockieren von Popups.

- Ändern Sie das Aktualisierungsintervall (standardmäßig sind 4 Minuten festgelegt). Tippen Sie im Systemmenü unter "Einstellungen" auf die funktionsbezogenen Einstellungen. Erhöhen (Pluszeichen (+)) oder verringern (Minuszeichen (-)) Sie das Abfrageintervall.
- Wählen Sie die für diese Funktion anzuzeigenden Funktionen. Zum Beispiel kann der angemeldete Anwender auswählen, dass nur Incidents angezeigt werden sollen. Gehen Sie zum Fenster "Einstellungen", und tippen Sie auf die Option zum Hinzufügen und Entfernen von Funktionen. Wischen Sie, um eine Funktion zu aktivieren oder zu deaktivieren.

Genehmigungen

Die Genehmigungs-Funktion wird verwendet, um schnell und nahtlos auf ausstehende Workflow-Aufgaben zu antworten. Die Genehmigungs-Funktion bietet dem mobilen Anwender alle Informationen, die er zum Abschließen der Aufgabe benötigt.

Der angemeldete Anwender kann auf die folgenden Kernfunktionen dieser Funktion zugreifen:

- Anzeigen einer kurzen Tour durch die Funktion. Sie können auch angeben, dass Sie bei der nächsten Verwendung der Funktion die Tour *nicht* mehr anzeigen möchten. Wenn Sie die Tour erneut anzeigen möchten, gehen Sie im Abschnitt Genehmigungen unter den Einstellungen zu den funktionsbezogenen Einstellungen, und aktivieren Sie das Kontrollkästchen zum Anzeigen der Produkttour.
- Zeigen Sie die folgenden Aufgaben an:
 - Ausstehende Aufgaben der folgenden Workflow-Engines, die in CA SDM integriert sind:
 - CA SDM Klassischer Workflow
 - IT Process Automation Manager (ITPAM)
 - CA Workflow (CAWF)

- Workflow-Aufgaben, die dem Anwender zugewiesen sind. Wenn der angemeldete Anwender Teil der PAMAdmins-Gruppe ist, kann er ITPAM-Aufgaben der Genehmigungs-Funktion anzeigen und darauf reagieren.
- Workflow-Aufgaben, die einer Gruppe zugewiesen sind, zu der der Anwender gehört.
 - Beim klassischen Workflow von CA SDM werden Aufgaben, die der CA SDM-Gruppe zugewiesen sind, nicht angezeigt. Es werden nur Aufgaben angezeigt, die einzelnen Anwendern zugewiesen sind.
 - Wenn der angemeldete Anwender Teil der PAMAdmins-Gruppe ist, kann er ITPAM-Aufgaben der Genehmigungs-Funktion anzeigen und darauf reagieren.
- Workflow-Aufgaben, für die der Anwender darum gebeten wird, zu antworten, ungeachtet des CA SDM-Ticketzuständigen oder des Anforderers. So ist es zum Beispiel wahrscheinlich, dass eine Finanzgenehmigungsaufgabe von dem Anwender ausgeführt wird, der nicht direkt an CA SDM beteiligt ist.

Hinweis: Wenn eine Workflow-Engine ausgefallen ist und der Anwender nicht das entsprechende Arbeitselement verwendet, zeigt "Genehmigungen" nicht die Arbeitselemente oder eine Fehlermeldung an. Wenn die Workflow-Engine dann zu einem bestimmten Zeitpunkt wieder funktioniert, werden die entsprechenden Arbeitselemente dem Anwender wieder angezeigt. Wenn Sie jedoch bereits ein Arbeitselement verwenden und der Server dann ausfällt, wird unter "Genehmigungen" eine Fehlermeldung angezeigt.

- Sie können ein Balkendiagramm anzeigen, das die Anzahl der ausstehenden Aufgaben anzeigt, die auf eine Eingabe warten, geordnet nach der Zeit, die sie bereits ausstehend sind. Dieses Balkendiagramm ermöglicht dem Anwender, neue Aufgaben zu identifizieren und direkt zu sehen, wie lange sie bereits ausstehen.
- Zeigen Sie die Liste der Aufgaben gefiltert nach der Wartezeit an. Tippen Sie auf den Balken im Diagramm, oder verwenden Sie das Pulldown-Menü oben im Fenster. Wenn Sie zum Beispiel auf den Balken für die letzte Stunde klicken, werden alle Aufgaben angezeigt, die in der letzten Stunde erstellt oder geändert wurden und auf Genehmigung warten.
- Suchen Sie nach einer ausstehenden Aufgabe; geben Sie den Suchtext in den Suchbereich ein. Das Suchergebnis wird aktualisiert, während Sie tippen. Sie können anhand der Ticketnummer, Priorität oder von Stichwörtern aus der Aufgabenbeschreibungen suchen.

- Zeigen Sie die Arbeitselementdetails an, indem Sie auf eine Aufgabe in der Liste tippen. Wenn die Details angezeigt werden, können Sie die folgenden Aktionen ausführen:
 - Zeigen Sie das Eingabeformular des Arbeitselements an, das fast dem Formular für Workflow-Engines entspricht. Anwenderspezifische Genehmigungsformulare sind automatisch auf dem Mobilgerät ohne Änderung verfügbar. Sie werden für die Wiedergabe auf dem Mobilgerät neu formatiert.
 - Erfahren Sie mehr über das Arbeitselement, indem Sie auf das Ticketsymbol  tippen, um die verknüpften CA SDM-Ticketinformationen anzuzeigen. Diese Informationen können Begründungen aus geschäftlicher Sicht, Implementierungs- und Backout-Vorgänge, Kontakte, Zuständige, Informationen, Priorität, SLA, Relevanz usw. einschließen.
 - Kontaktieren Sie den Anforderer, Zuständigen usw. telefonisch oder per E-Mail, indem Sie auf die Telefonnummer oder auf die E-Mail-Adresse tippen, die für das entsprechende Ticket angegeben ist. Diese Informationen werden nur angezeigt, wenn das CA SDM-Ticket diese Kontaktinformation enthält.
 - Laden Sie Anhänge für das verknüpfte Change-Ticket herunter, und zeigen Sie diese an. Unter Umständen müssen Sie auf Ihrem Mobilgerät zusätzliche Viewersoftware installieren, um das heruntergeladene Dokument öffnen zu können.
- Wichtig!** Um Anhänge über die Webanwendung von CA SDM-Mobile Enabler anzeigen zu können, deaktivieren Sie im Webbrowser die Option zum Blockieren von Popups.
- Hinweis:** Wenn Sie den Anhang in den Android-Pop-Up-Browser herunterladen, wird eine Fehlermeldung angezeigt. Tippen Sie auf den Pfeil auf der linken Seite des Pop-Up-Browsers. Der Pop-Up-Browser wird in den Hauptbrowser konvertiert, und Sie können den Anhang herunterladen.
- Reagieren Sie auf das Arbeitselement, indem Sie die erforderlichen Informationen in das Detailformular eingeben und auf Senden tippen. Die nächste Aufgabe wird automatisch zur Beantwortung geöffnet, wenn mehrere Aufgaben ausstehen. Sie können auch auf den Vorwärtspfeil in der oberen rechten Ecken der Funktion tippen, um das nächste Arbeitselement zu öffnen.

- Aktivieren Sie auf Anforderung des Supports die Debugging-Informationen, indem Sie im Systemmenü "Einstellungen" und dann die funktionsbezogenen Einstellungen auswählen. Tippen Sie auf das Tracing-Dropdown-Menü, um eine Option auszuwählen. Wählen Sie die Option "ein", um die Debugging-Informationen zu aktivieren. Wählen Sie die Option "ausführlich", um ausführlichere Informationen zu erhalten. Sie können die Protokollierungsinformationen im `$NX_ROOT\log\approve.log`-Verzeichnis auf dem CA SDM-Server anzeigen. Wir empfehlen, dass Sie diese Option deaktivieren, um eine zusätzliche Belastung des Servers zu vermeiden, wenn Sie die Support-Sitzung abgeschlossen haben.
- Ändern Sie das Datums- und Uhrzeit-Format, indem Sie im Systemmenü unter "Einstellungen" auf die funktionsbezogenen Einstellungen klicken und das Datums-/Uhrzeitformat wählen. Das geänderte Datums- und Uhrzeit-Format spiegelt sich erst dann wider, wenn Sie die Funktion aktualisieren.
- Aktualisieren Sie die aktuelle Liste der Arbeitselemente, indem Sie in der oberen rechten Ecke der Aufgabenlistenseite auf das Systemmenü tippen und "Aktualisieren" wählen.
- Ändern Sie das Aktualisierungsintervall, das angibt, wie oft die Genehmigungs-Kachel aktualisiert wird, indem Sie das Abfrageintervall auf der Seite mit den funktionsbezogenen Einstellungen ändern.
- Aktivieren Sie die Option für die Antwortzeitüberschreitung, wobei dem angemeldeten Anwender eine Meldung angezeigt wird, wenn die Funktion innerhalb der angegebenen Zeit nicht antwortet. Als angemeldeter Anwender können Sie diese Zeit (in Minuten) im Systemmenü unter "Einstellungen" in den funktionsbezogenen Einstellungen festlegen. Standardmäßig ist die Zeitüberschreitung auf zwei Minuten festgelegt. Sie können die Zeit erhöhen (Pluszeichen (+)) oder verringern (Minuszeichen (-)). Wenn die Funktion nicht innerhalb dieser geplanten Zeitüberschreitung antwortet, wird dem angemeldeten Anwender eine Fehlermeldung angezeigt. Nachdem der Anwender in der Meldung auf "OK" geklickt hat, wird die Anmeldeseite der Genehmigungsfunktion wieder aufgerufen.

Open Space

Die Open Space-Funktion ermöglicht dem angemeldeten Anwender, auf die folgenden Kernfunktionen von CA Open Space auf einem Mobilgerät zuzugreifen:

- Anzeigen der Anzahl der neuesten Fragen, die von [assign the value for openspace in your book] gepostet werden, auf dem Startbildschirm. Die Beiträge werden nach entsprechenden Kennzeichnungen wie "Empfohlen", "Neueste", "Folgen" usw. kategorisiert. Standardmäßig werden die neuesten Fragen angezeigt.

- (Wenn [assign the value for openspace in your book] mit CA SDM konfiguriert ist) Anzeigen der Anzahl von Tickets (Request oder Incident, wie vom Systemadministrator auf dem [assign the value for openspace in your book]-Server konfiguriert), die über diese Funktion von Ihnen erstellt wurden, auf dem Startbildschirm.
- Tippen Sie auf dem Startbildschirm auf die Fragenkachel, um die verknüpften Beiträge anzuzeigen. Aktivieren Sie eine Option, zum Beispiel "Neueste", über das Drow-down-Feld, um nur die neuesten Beiträge anzuzeigen.
- Suchen Sie nach einem Beitrag aus allen Quellen. Geben Sie Ihre Suchkriterien im Feld für den Suchtext ein, und tippen Sie auf die Eingabe-Option. Suchergebnisse aus allen Quellen werden angezeigt. Über das Drow-down-Feld können Sie die Option "Global" auswählen, um in allen Datenquellen zu suchen, die auf dem [assign the value for openspace in your book]-Server aktiviert sind, oder Sie können "Fragen" auswählen, um in den für diese Funktion aufgeführten Fragen zu suchen.
- Suchen Sie nach Requests oder Incidents.
- Tippen Sie auf eine Frage, um den detaillierten Beitrag anzuzeigen. Tippen Sie auf "Weitere Aktionen" (Pfeilsymbol in der oberen rechten Ecke der Funktion), um die folgenden Aktionen auszuführen:
 - Auf den Beitrag antworten
 - Dem Beitrag folgen oder nicht mehr folgen
 - Beitrag freigeben
 - Öffnen Sie ein Service Desk-Ticket, wenn der Beitrag Ihre Fragen nicht beantwortet.

Hinweis: Um dem Request-Formular neue Felder hinzuzufügen, muss der Systemadministrator die Felder auf dem [assign the value for openspace in your book]-Server konfigurieren. Die gleichen konfigurierten Felder werden in der Open Space-Funktion angezeigt. Die Anzahl von Feldern, die auf dem [assign the value for openspace in your book]-Server konfiguriert werden können, ist 5. Weitere Informationen zum Konfigurieren der Felder finden Sie im *CA Open Space-Administrationshandbuch*.

- Ändern Sie das Aktualisierungsintervall (standardmäßig sind vier Minuten festgelegt). Tippen Sie im Systemmenü unter "Einstellungen" auf die funktionsbezogenen Einstellungen. Erhöhen (Pluszeichen (+)) oder verringern (Minuszeichen (-)) Sie das Abfrageintervall.
- Wählen Sie die für diese Funktion anzuzeigenden Funktionen. Der angemeldete Anwender kann zum Beispiel auswählen, dass nur die Fragen angezeigt werden. Gehen Sie zum Fenster "Einstellungen", und tippen Sie auf die Option zum Hinzufügen und Entfernen von Funktionen. Wischen Sie, um eine Funktion zu aktivieren oder zu deaktivieren.

Überprüfen der Voraussetzungen

Überprüfen Sie die folgenden Anforderungen, bevor Sie CA SDM Mobile Enabler konfigurieren:

- [Zertifizierte Mobilgerät-Betriebssysteme](#) (siehe Seite 106)
- Um auf die Funktionen für die Analyst-Warteschlange und Genehmigungen zugreifen zu können, muss CA SDM Version 12.9 installiert und auf dem Server konfiguriert werden, auf dem Sie CA SDM Mobile Enabler installieren wollen. REST wird ebenfalls auf dem gleichen Server installiert und konfiguriert. Weitere Informationen finden Sie im *CA Service Desk Manager Implementierungshandbuch*.
- Um auf die Open Space-Funktion zugreifen zu können, muss CA Open Space r2.0 installiert und auf dem CA SDM-Server konfiguriert werden. Weitere Informationen finden Sie im *CA Open Space Implementierungshandbuch*.
- Den angemeldeten Anwendern für die Analyst-Warteschlange muss die REST-Webservice-API-Rolle zugewiesen sein. Stellen Sie sicher, dass den Funktionen *Administration*, *Sicherheit* und *Referenz* dieser Rolle die Zugriffsebenen zum Anzeigen oder Ändern zugewiesen sind. Weitere Informationen über den Zugriff auf Funktionen, Zugriffsebenen und Rollen finden Sie im *CA Service Desk Manager Administrationshandbuch*.

Zertifizierte Mobilgerät-Betriebssysteme

CA SDM Mobile Enabler ist für die systemeigenen Browser der folgenden Mobilgerät-Betriebssysteme zertifiziert:

- iOS 5.1 und höher
- Android 4.x

Anwenden der Patches auf Open Space

Wenden Sie abhängig von Ihrem Betriebssystem die folgenden Patches auf den [assign the value for openspace in your book]-Server an, bevor Sie CA SDM Mobile Enabler bereitstellen, um auf die Open Space-Funktion zuzugreifen:

Betriebssystem	Patch-Nummer
Windows	RO61737
Linux	RO61738

Aktivieren von CORS-Einstellungen

Aktivieren Sie die Einstellungen für das Cross Origin Resource Sharing (CORS), um die Mobilfunktion von Open Space nutzen zu können.

Wichtig! Dieser Prozess ist nur anwendbar für webbasierte Anwendungen und *nicht* für die systemeigene Anwendung von CA SDM Mobile Enabler.

Gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass Sie die [Patches für Open Space](#) (siehe Seite 106) angewendet haben, bevor Sie die CORS-Einstellungen aktivieren.
2. Melden Sie sich beim Open Space-Server an.
3. Wechseln Sie in das folgende Verzeichnis:
`OSOP_HOME/tomcat.7.xx/webapps/ROOT/WEB-INF`
4. Öffnen Sie die Datei "web.xml".
5. Fügen Sie nach dem letzten `</filter>`-Tag in der XML-Datei den folgenden Inhalt hinzu:

```
<filter>
<filter-name>CORS</filter-name>
<filter-class>com.thetransactioncompany.cors.CORSFilter</filter-class>
<init-param>
<param-name>cors.allowGenericHttpRequests</param-name>
<param-value>true</param-value>
</init-param>

<init-param>
<param-name>cors.allowOrigin</param-name>
<param-value>*</param-value>
</init-param>
<init-param>
<param-name>cors.allowSubdomains</param-name>
<param-value>true</param-value>
</init-param>
<init-param>
<param-name>cors.supportedMethods</param-name>
<param-value>GET, HEAD, POST, OPTIONS, PUT, DELETE</param-value>
</init-param>
```

```
<init-param>
<param-name>cors.supportedHeaders</param-name>
<param-value>Origin, Accept, Authorization, Content-Type,
X-Requested-With</param-value>
</init-param>
<init-param>
<param-name>cors.exposedHeaders</param-name>
<param-value>X-Test-1, X-Test-2</param-value>
</init-param>
<init-param>
<param-name>cors.supportsCredentials</param-name>
<param-value>true</param-value>
</init-param>

<init-param>
<param-name>cors.maxAge</param-name>
<param-value>3600</param-value>
</init-param>
</filter>
<filter-mapping>
<filter-name>CORS</filter-name>
<url-pattern>*</url-pattern>
</filter-mapping>
```

6. (Optional) Wenn Sie möchten, dass eine bestimmte Domäne auf den <osop>-Server zugreift, gehen Sie wie folgt vor:

- a. Suchen Sie die folgende Zeile in der XML-Datei:

```
<init-param>
<param-name>cors.allowOrigin</param-name>
<param-value>*</param-value>
</init-param>
```

- b. Ersetzen Sie den Parameterwert "cors.allowOrigin" durch die folgenden Unterdomänen-Informationen des CA SDM-Servers:

http://<Servername>:<Portnummer>

Hinweis: Sie können mehrere Unterdomänen, durch Leerzeichen getrennt, hinzufügen.

7. Speichern Sie die Datei.
8. Starten Sie den Open Space-Server neu.
Die CORS-Einstellungen sind aktiviert.

(Optional) Festlegen von Formularfeldern als nicht erforderlich

Standardmäßig sind alle Eingabefelder in der Genehmigungs-Funktion, die von der ITPAM-Workflow-Engine abgeleitet werden, obligatorisch. Je nach Ihrer ITPAM-Version kann der Systemadministrator diese Felder als nicht obligatorisch bzw. erforderlich festlegen.

Gehen Sie wie folgt vor:

1. Melden Sie sich beim CA SDM-Server an, und öffnen Sie die Datei "NX.env".
2. Fügen Sie dieser Datei die folgende Variable hinzu:
`NX_MOBILE_WFM_ITPAM_ALL_FIELDS_ARE_REQUIRED`
3. Legen Sie den Variablenwert fest.
4. Speichern Sie die Datei.
5. Abhängig vom Variablenwert und der ITPAM-Version können Sie die folgenden Änderungen anwenden:
 - Wenn die Variable nicht festgelegt wird, sind alle Felder von ITPAM 3.1, 4.0 oder höher standardmäßig obligatorisch.
 - Wenn dieser Variablenwert auf "Ja" festgelegt wird, sind alle Felder von ITPAM 3.1, 4.0 oder höher obligatorisch.
 - Wenn dieser Variablenwert auf "Nein" festgelegt wird, folgen alle Felder von ITPAM 3.1 der minimalen und maximalen Längenbeschränkung. Die minimale und maximale Länge für Zeichenfolgen-Eingabefelder in ITPAM 4.0 oder höher sind in der Genehmigungs-Funktion nicht anwendbar. Daher werden alle Felder nicht obligatorisch, wenn der Variablenwert auf "Nein" festgelegt wird.

(Optional) Erzwingen der Genehmigungsvereinbarkeit nach Aktualisierung

Damit Anwender auf die aktuelle Genehmigungs-Funktion mit den aktuellen Funktionen zugreifen können und eine durchgängige Anwendererfahrung gewährleistet wird, setzen Sie die Variable `NX_MOBILE_WFM_FORCE_CLIENTVERSION_UPGRADE` auf **Ja**.

Wenn diese Option festgelegt ist, werden Anwender, die versuchen, sich bei der Vorgängerversion der Genehmigungs-Funktion anzumelden, dazu aufgefordert, diese Funktion zu aktualisieren, und die Anmeldung kann nicht erfolgen.

Gehen Sie wie folgt vor:

1. Melden Sie sich beim CA SDM-Server an, und öffnen Sie die Datei "NX.env".
2. Fügen Sie dieser Datei die folgende Variable hinzu:
`NX_MOBILE_WFM_FORCE_CLIENTVERSION_UPGRADE`
3. Setzen Sie den Variablenwert auf "Ja".
4. Speichern Sie die Datei.
5. Starten Sie den CA SDM-Server neu.

Zugreifen auf CA SDM-Mobile Enabler

Wenn Sie auf die Webanwendung von CA SDM Mobile Enabler *über Ihr Mobilgerät* zugreifen möchten, verwenden Sie die folgende URL:

`http(s)://<CA_SDM_Servername>:<REST_Portnummer>/casdm`

Hinweis: Informieren Sie die Anwender über diese URL, wenn sie die Webanwendung von CA SDM Mobile Enabler auf ihrem Mobilgerät verwenden wollen.

Wenn Sie CA SDM Mobile Enabler als die *systemeigene mobile Anwendung* auf Ihrem Mobilgerät verwenden wollen, gehen Sie wie folgt vor:

1. Gehen Sie zu Google Play (für Android-Anwender) oder zum App-Store (für iOS-Anwender).
2. Suchen Sie nach CA Service Desk Manager.
3. Installieren Sie die CA Service Desk Manager-App.

Das CA SDM-Symbol wird nach erfolgreicher Installation auf Ihrem Mobiltelefon angezeigt.

Kapitel 5: Definieren der Geschäftsstruktur

Dieses Kapitel enthält folgende Themen:

[Erstellen der Geschäftsstruktur](#) (siehe Seite 112)

[Definieren der Unternehmensinfrastruktur](#) (siehe Seite 125)

[Mehrere Mandanten](#) (siehe Seite 129)

Erstellen der Geschäftsstruktur

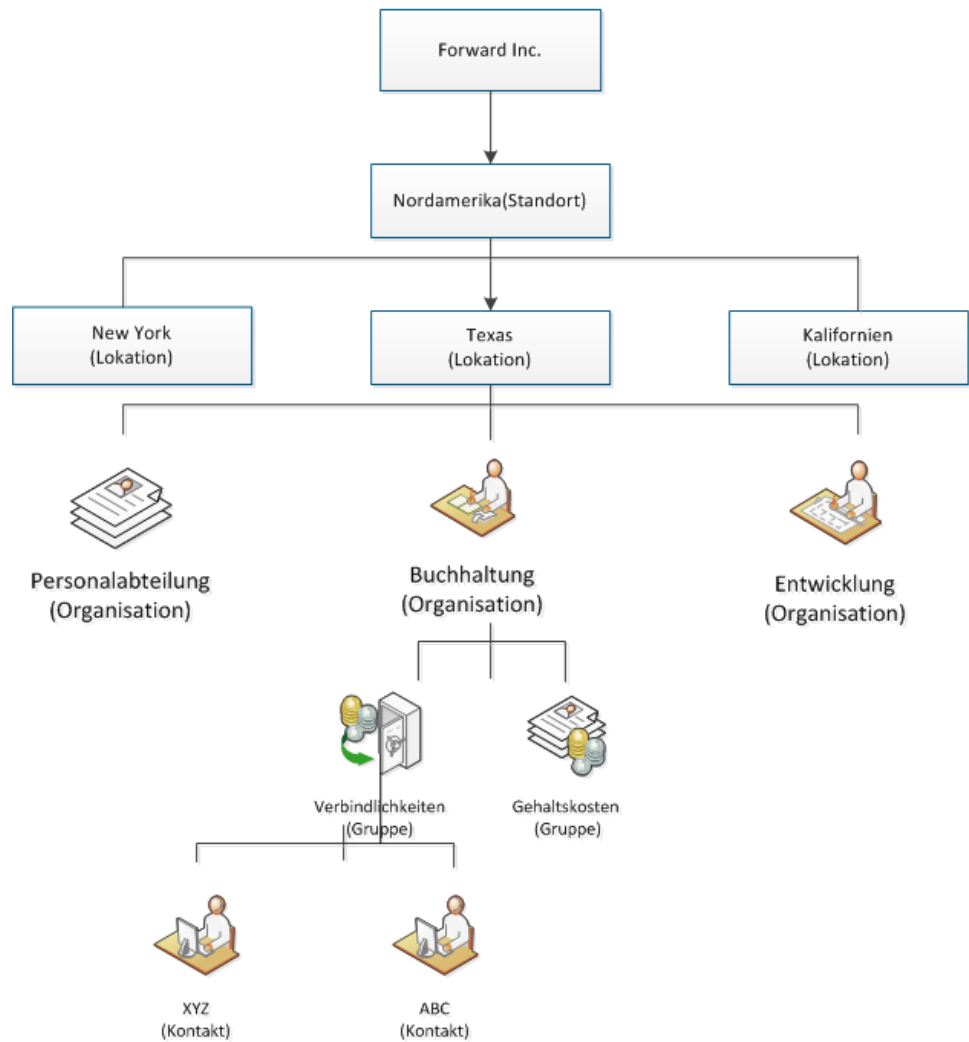
Eine Geschäftsstruktur ist eine angepasste und logische Darstellung Ihres Unternehmens in einer Unicenter Service Desk-Umgebung. Dieses Szenario beschreibt, wie ein Administrator eine Geschäftsstruktur für ein Unternehmen erstellen kann, um Kontakte, Gruppen und Assets an verteilten Lokationen zu verwalten und zu verfolgen. Nachdem Sie eine Geschäftsstruktur erstellt haben, können Sie Berichte generieren, um Requests nach Standort, Organisation oder Gruppe zu analysieren.

Beispiel

Das fiktive Unternehmen "Forward, Inc." verwendet ein System für die Verarbeitung von Requests für mehrere Büros, die über geografische Lokationen verteilt sind. Das Unternehmen plant, Unicenter Service Desk zu implementieren, um die Anzahl und Typen der Requests, die von verschiedenen Geschäftssegmenten generiert werden, zu analysieren.

Folgendes Diagramm veranschaulicht ein Beispiel für eine Geschäftsstruktur auf hoher Ebene, wobei das fiktive Unternehmen "Forward, Inc." verwendet wird.

Beispiel für Geschäftsstruktur



Um eine effektive Nachverfolgung und die Entscheidungsfindung zu erleichtern, muss die Organisation folgende Elemente verfolgen:

- Kontakte, Kontaktgruppen und Lokationen
- Assets an verschiedenen Lokationen

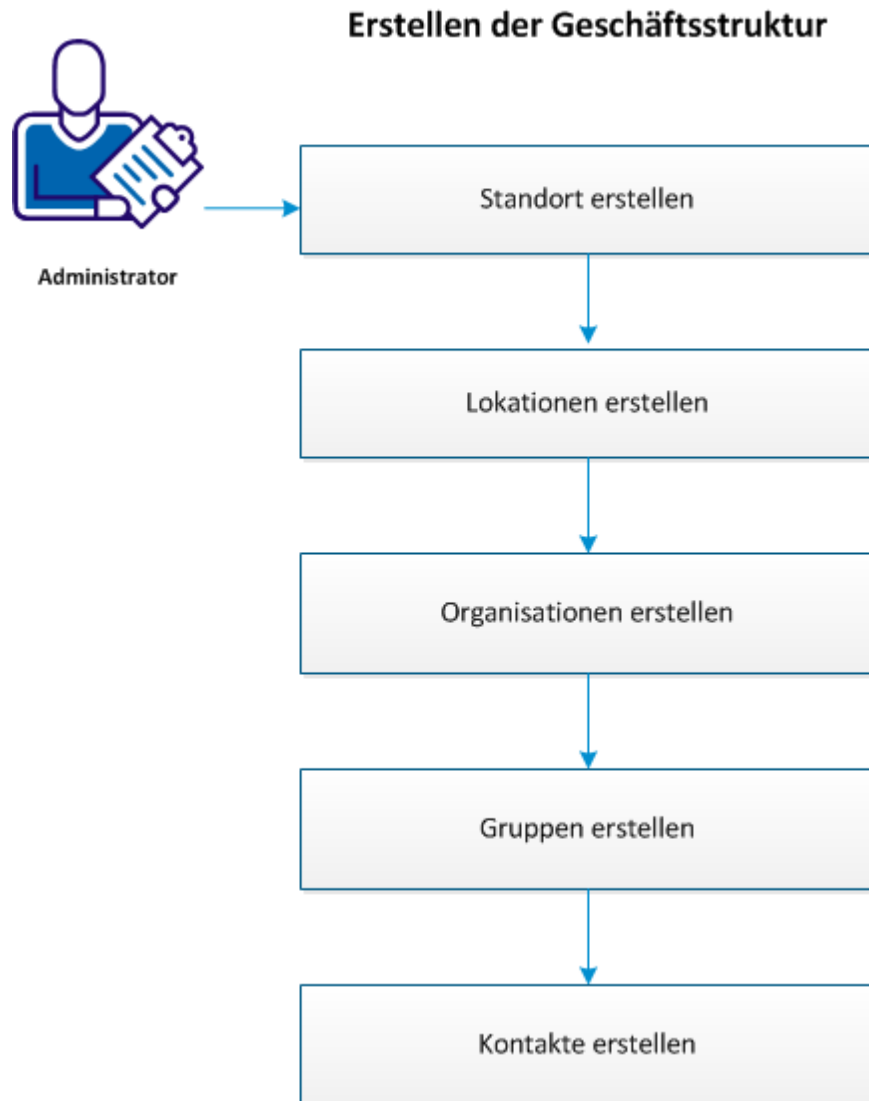
Das Erstellen einer Geschäftsstruktur ermöglicht es dem Verwaltungsteam bei "Forward, Inc.", folgende Aktionen auszuführen:

- Generieren von Berichten, um Requests nach Standort, Organisation und Gruppe zu analysieren
- Vergrößern der allgemeinen Effizienz, indem Korrekturmaßnahmen für Lücken im Request-Prozess implementiert werden

So erstellen Sie die Geschäftsstruktur

Um eine Geschäftsstruktur zu erstellen, definieren Sie eine logische Hierarchie von Standorten und Organisationen innerhalb des Unternehmens, und ordnen Sie dann Kontakte und Gruppen ihren jeweiligen Standorten und Organisationen zu.

Folgendes Diagramm zeigt, wie ein Administrator die Objekte in einer normalen Geschäftsstruktur definieren kann:



Gehen Sie wie folgt vor:

1. [Erstellen von Standorten](#) (siehe Seite 116)
2. [Erstellen von Lokationen](#) (siehe Seite 117)
3. [Erstellen von Organisationen](#) (siehe Seite 118)
4. [Erstellen von Gruppen](#) (siehe Seite 119)
5. [Erstellen von Kontakten](#) (siehe Seite 120)

Erstellen von Standorten

Ein Standort ist eine geografische Region, wo Ihre Organisation eine oder mehrere Lokationen hat.

Zum Beispiel kann Nordamerika ein Standort mit Lokationen (Büros) in New York, Kalifornien und Texas sein.

Hinweis: Wenn die Mandantenfähigkeit aktiviert ist, wählen Sie in der Drop-down-Liste den entsprechenden Mandanten aus.

Gehen Sie wie folgt vor:

1. Wählen Sie in der Menüleiste des Unicenter Service Desk-Scoreboards "Datei", "Neuer Standort".

Das Fenster "Neuen Standort erstellen" wird geöffnet.

2. Geben Sie die Informationen ein, die spezifisch Ihrem Standort entsprechen.
3. Klicken Sie auf "Speichern".

Der Standortdatensatz wird erstellt und gespeichert.

Erstellen von Lokationen

Eine Lokation ist ein physischer Ort, wie z. B. eine Büroadresse. Zum Beispiel können die Adressen der Büros in New York, Kalifornien und Texas Lokationen unter dem Standort "Nordamerika" sein.

Durch das Erstellen von Lokationen können Sie Kontakte und Ressourcen in dieser Lokation verwalten. Nachdem Sie eine Lokation erstellt haben, können Sie sie einem Standort zuweisen.

Gehen Sie wie folgt vor:

1. Wählen Sie der Menüleiste des Scoreboards "Datei", "Neue Lokation".
Die Seite "Neue Lokation erstellen" wird geöffnet.
2. Geben Sie spezifische Informationen zu Ihrer Lokation ein, und konfigurieren Sie dann die Lokation mithilfe der folgenden Steuerelemente auf den Registerkarten:

Adresse

Gibt die physische Adresse der Lokation an.

Automatische Zuweisung

Die Tickets (Requests, Changes und Issues) werden den Mitgliedern in dieser Lokation automatisch zugewiesen.

Anfragebereiche aktualisieren

Wählen Sie die Request-Bereiche aus, die Sie automatisch zu den Mitgliedern der Lokation zuweisen möchten.

Change-Kategorien aktualisieren

Wählen Sie die Change-Bereiche aus, die Sie automatisch zu den Mitgliedern der Lokation zuweisen möchten.

Issue-Kategorien aktualisieren

Wählen Sie die Issue-Bereiche aus, die Sie automatisch zu den Mitgliedern der Lokation zuweisen möchten.

Gruppen aktualisieren

Wählen Sie die Gruppen aus, die Sie für die automatische Zuweisung von Tickets aktualisieren möchten.

Wichtig! Nachdem Sie die Request-Bereiche und Kategorien aktualisiert haben, aktivieren Sie die automatische Zuweisung individuell für jeden Request-Bereich und für jede Kategorie.

3. Klicken Sie auf "Speichern".
Die Lokationsdetails werden gespeichert.
4. (Optional) Wiederholen Sie die Schritte 1 bis 3, um mehr Lokationen hinzuzufügen.

Erstellen von Organisationen

Eine Organisation bezieht sich auf eine interne Abteilung, einen Bereich oder ein externes Unternehmen. Sie können Organisationen zu Tickets, zu Configuration Item-Klassen (CI) und zu Kontakten zuweisen.

Sie können z. B. CIs für Organisationen definieren, um anzugeben, welche Hardware, Software und Services die Organisation nutzt.

Hinweis: Wenn die Mandantenfähigkeit aktiviert ist, wählen Sie in der Drop-down-Liste den entsprechenden Mandanten aus.

Gehen Sie wie folgt vor:

1. Wählen Sie in der Menüleiste des Scoreboards "Datei", "Neue Organisation".
Die Seite "Neue Organisation erstellen" wird geöffnet.
2. Geben Sie die spezifischen Informationen für Ihre Organisation ein, und geben Sie anschließend Organisationsdetails in den folgenden Feldern an:

Adresse

Zeigt die Adresse der Lokation an, mit der Sie die Organisation verknüpfen. Die Felder werden automatisch aufgefüllt, wenn Sie der Organisation eine Lokation zuweisen.

Umgebung

Zeigt die Configuration Items (zum Beispiel Ausstattung, Software und Services) an, die die Organisation verwendet. Sie können die Organisation mit einem oder mehreren Configuration Items verknüpfen. Durch das Zuordnen der CI-Elemente zur Organisation können Administratoren die Ressourcen zu verfolgen, die von den Organisationen in verschiedenen Lokationen verwendet wird.

3. Klicken Sie auf "Speichern".
Die Organisationsdetails werden gespeichert.
4. (Optional) Wiederholen Sie die Schritte 1 bis 3, um mehr Organisationen hinzuzufügen.

Erstellen von Gruppen

Eine Gruppe ist eine Sammlung von Kontakten, die einen bestimmten Verantwortungsbereich darstellt. Durch die Definition von Gruppen können Sie Verantwortung zum Lösen eines Tickets zuweisen, wenn diese Verantwortung von mehreren Personen geteilt wird. Sie können beispielsweise eine Gruppe namens "Dallas Personal" einrichten, die für sämtliche Angelegenheiten des Personals im Büro in Dallas Ihrer Organisation verantwortlich ist. Wenn ein Mitarbeiter in diesem Büro ein Problem hat, können Sie das Problem zur Lösung der Gruppe „Dallas Personal“ zuordnen.

Hinweis: Wenn die Mandantenfähigkeit aktiviert ist, wählen Sie in der Drop-down-Liste den entsprechenden Mandanten aus. Mit der Option "öffentlich (freigegeben)" wird das Objekt für alle Mandanten erstellt.

Gehen Sie wie folgt vor:

1. Wählen Sie in der Menüleiste des Scoreboards die Optionen "Datei", "Neue Gruppe".
Die Seite "Neue Gruppe erstellen" wird geöffnet.
2. Geben Sie die spezifischen Informationen für diese Gruppe und für Ihre Organisation an, indem Sie die Gruppendetails in folgenden Feldern eingeben:

Benachrichtigung

Definiert die Kontaktinformationen und die Methode zum Benachrichtigen der Gruppe.

Adresse

Weist die Gruppe einer Lokation zu.

Organisationsinformationen

Gibt die funktionale oder administrative Organisation, die Abteilung, die Kostenstelle oder die Anbieterinformationen an.

Umgebung

Gibt die Umgebung an (z. B. Geräte, Software und Dienste).

Mitglieder

Fügt Kontakte hinzu oder entfernt Kontakte.

Serviceverträge

Listet Serviceverträge auf, die mit der Gruppe verknüpft sind.

Automatische Zuweisung

Listet automatische, auf der Gruppenmitgliedschaft basierende Zuweisungen von Tickets auf.

Anmerkungen und Spezielle Verarbeitung

Listet Anmerkungen und Typen für die spezielle Verarbeitung auf, z. B. VIP- oder Sicherheitsrisikotypen. Sie können auf Besondere Verarbeitung des Kontakts aktualisieren klicken, um nach Mitgliedern der speziellen Verarbeitung zu suchen.

3. Klicken Sie auf "Speichern".

Der Gruppendatensatz wird gespeichert, und die Seite "Gruppe - Detail" wird geöffnet. Die folgenden Schaltflächen sind jetzt zum Konfigurieren der Gruppe verfügbar:

Umgebung aktualisieren

Klicken Sie unter Kontaktdetails auf der Registerkarte Umgebung auf diese Schaltfläche, um das Fenster Configuration Items - Suche für die Gruppe zu öffnen. Sie können Suchkriterien für die Assets angeben, die Sie auf dieser Seite berücksichtigen möchten. Sie können ein neues Configuration Item erstellen und nach Assets suchen, indem Sie das Fenster "Aktualisieren" des entsprechenden Kontakts verwenden.

Mitglieder aktualisieren

Unter Mitglieder, Serviceverträge, Automatische Zuweisung werden auf der Registerkarte Mitglieder mit dieser Schaltfläche die Kontakte angezeigt. Sie können Kontakte für diese Gruppe hinzufügen und entfernen.

4. (Optional) Wiederholen Sie die Schritte 1-3, um bei Bedarf mehr Gruppen hinzuzufügen.

Erstellen von Kontakten

Ein Kontakt ist eine Person, die Ihr System regelmäßig verwendet, wie z. B. ein Analyst oder ein Kunde. Nachdem Sie die Geschäftsstruktur und Gruppen erstellt haben, erstellen Sie Kontakte und ordnen sie ihrer jeweiligen Lokation und Organisation zu.

Sie können Kontakte folgendermaßen erstellen:

- **Manuelles Erstellen von Kontakten**

Verwenden Sie diese Methode, wenn Sie Kontakte mithilfe des CA SDM-Scoreboards erstellen möchten.

- **Daten aus der LDAP-Datenbank verwenden**

Verwenden Sie diese Methode, wenn Ihre CA SDM-Installation konfiguriert ist, um auf einen LDAP-Server (Lightweight Directory Access Protocol) zuzugreifen und wenn CA SDM die erforderlichen Optionen installiert hat.

Manuelles Erstellen von Kontakten

Wenn Sie kein Active Directory, wie z. B. LDAP, für Ihre Kontakteinformationen verwenden möchten, können Sie die Kontakte in CA SDM manuell erstellen.

Hinweis: Wenn die Mandantenfähigkeit aktiviert ist, wählen Sie in der Drop-down-Liste den entsprechenden Mandanten aus.

Gehen Sie wie folgt vor:

1. Wählen Sie der Menüleiste des Scoreboards "Datei", "Neuer Kontakt".

Das Fenster "Neuen Kontakt erstellen" wird geöffnet.

2. Füllen Sie folgende Felder nach Wunsch für den Kontakt aus:

Mandant

Gibt den Mandanten an, mit dem der Kontakt verknüpft ist (für Installationen für mehrere Mandanten).

ID kontaktieren

Gibt eine eindeutige Kennung für den Kontakt an. Bei Verwendung der Standard-Anwenderauthentifizierung dient der Wert in diesem Feld als Kennwort für die Anwenderanmeldung.

Anwender-ID

Gibt den Anwendernamen des Kontakts an. Der Kontakt verwendet diesen zur Anmeldung im System.

Diensttyp

Gibt die Support-Ebene an, die der Kontakt erhalten hat.

Datenaufteilung

Gibt die Datenpartition für diesen Kontakt an. Dieser Wert bestimmt, auf welche Datensätze dieser Kontakt zugreifen kann.

Zugriffstyp

Gibt den Zugriffstyp an. Der Zugriffstyp bestimmt die Systemfunktionen, auf die der Kontakt zugreifen kann.

Verfügbar

Zeigt an, ob der Kontakt für Ticketzuweisungen verfügbar ist.

Self-Service-Speicherung bestätigen

Zeigt an, ob der Kontakt eine Bestätigung erhält, wenn ein Datensatz über die Self-Service-Schnittstelle gespeichert wird.

Mandantengruppe des Analysten

(Nur Kontakttyp "Analyst") Gibt die Mandantengruppe an, für die der Analyst verantwortlich ist.

3. Um den Kontakt zu konfigurieren, verwenden Sie folgende Steuerelemente, die auf den Registerkarten verfügbar sind.

Benachrichtigung

Definiert die Kontaktinformationen und die Methode zum Benachrichtigen des Kontakts.

- Markieren Sie die Benachrichtigungsmethode, die Sie für jede Dringlichkeitsstufe für diesen Kontakt verwenden möchten.

Beispiel: Sie wollen diesen Kontakt bei Meldungen normaler Dringlichkeitsstufe per E-Mail benachrichtigen, aber im Notfall wollen Sie ihn über die Benachrichtigungsmethode Pager-E-Mail benachrichtigen.

- Wählen Sie die Schicht, die für die verschiedenen Dringlichkeitsstufen der Benachrichtigung gilt.

Zum Beispiel können Sie einer normalen Benachrichtigung eine reguläre Schicht (5-Tage Woche, 8-Stunden-Tag) zuweisen und einer Notfallbenachrichtigung eine 24-Stunden-Schicht.

Adresse

Gibt den Standort des Kontakts an.

Organisationsinformationen

Gibt die funktionale oder administrative Organisation, Abteilung, Kostenstelle oder die Anbieterinformationen des Kontakts an.

Umgebung

Gibt die Umgebung des Kontakts an, etwa Ausrüstung, Software und Services.

Gruppen

Weist einen Kontakt einer Gruppe (einer Sammlung von Kontakten mit einem gemeinsamen Verantwortungsbereich) zu.

Rollen

Weist den Kontakt einer oder mehreren Rollen zu.

Serviceverträge

Zeigt die mit dem Kontakt verknüpften Serviceverträge an (sofern vorhanden).

Spezielle Verarbeitung

Listet die Kontakte auf, die einer besonderen Behandlung bedürfen, und ermöglicht Ihnen die Zuweisung von Kontakten zu speziellen Verarbeitungstypen, wie etwa Besucher oder Sicherheitsrisiko.

Event-Protokoll

Listet mit dem Kontakt verknüpfte Events auf, etwa Self-Service- und Knowledge-Aktivitäten.

Aktivitäten

Zeigt das Aktivitätsprotokoll des Kontakts an.

4. Klicken Sie auf "Speichern".

Die Kontaktinformationen wurden gespeichert.

Kontakte aus der LDAP-Datenbank verwenden

Wenn Ihre Produktinstallation für den Zugriff auf einen LDAP-Server (Lightweight Directory Access Protocol) konfiguriert ist und auch die erforderlichen Optionen installiert sind, können Sie Kontakte über die Daten aus der LDAP-Datenbank erstellen und aktualisieren. Dadurch können Kontakte sehr einfach mit den Netzanwenderdaten synchronisiert werden.

Gehen Sie folgendermaßen vor:

1. Wählen Sie der Menüleiste des Scoreboards "Datei", "Neuer Kontakt von LDAP".
Die Seite "LDAP-Verzeichnis - Suche" wird geöffnet.
2. Geben Sie einen oder mehrere Filter an, um die Liste "LDAP-Eintrag" auf spezifische Datensätze zu beschränken, die für Sie von Interesse sind.
3. Klicken Sie auf "Suchen".
Die Seite "LDAP-Einträge - Liste" zeigt die Datensätze an, die Ihren Filterkriterien entsprechen.
4. Klicken Sie auf den LDAP-Eintrag, um einen Kontakt zu erstellen.
Die Seite "Neuen Kontakt erstellen" wird geöffnet, auf der die LDAP-Daten bereits teilweise ausgefüllt sind.
5. Geben Sie je nach Bedarf weitere Informationen ein.
6. Um den Kontakt zu konfigurieren, verwenden Sie folgende Steuerelemente, die auf den Registerkarten verfügbar sind.

Benachrichtigung

Definiert die Kontaktinformationen und die Methode zum Benachrichtigen des Kontakts.

Adresse

Gibt die Adresse der Lokation an, mit der Sie die Organisation verknüpfen.

Organisationsinformationen

Gibt die funktionale oder administrative Organisation, Abteilung, Kostenstelle oder die Anbieterinformationen des Kontakts an.

Umgebung

Gibt die Umgebung des Kontakts an, etwa Ausrüstung, Software and Services.

Gruppen

Weist einen Kontakt einer Gruppe (einer Sammlung von Kontakten mit einem gemeinsamen Verantwortungsbereich) zu.

Rollen

Weist den Kontakt einer oder mehreren Rollen zu.

Serviceverträge

Zeigt die mit dem Kontakt verknüpften Serviceverträge an (sofern vorhanden).

Spezielle Verarbeitung

Listet Kontakte auf, die eine spezielle Verarbeitung benötigen. Sie können auch nach Kontakten suchen oder einen Kontakt mit einem speziellen Verarbeitungstyp verknüpfen, wie z. B. ein Besucher oder ein Sicherheitsrisikotyp.

Event-Protokoll

Listet mit dem Kontakt verknüpfte Events auf, etwa Self-Service- und Knowledge-Aktivitäten.

Aktivitäten

Zeigt das Aktivitätsprotokoll des Kontakts an.

7. Klicken Sie auf "Speichern".

Die Kontaktinformationen wurden gespeichert.

8. (Optional) Wiederholen Sie die Schritte 1 bis 7, um mehr Kontakte hinzuzufügen.

Sie haben eine Geschäftsstruktur erfolgreich erstellt und mit Kontakten und Gruppen verknüpft. Sie können jetzt Berichte generieren, um Requests nach Standort, Organisation oder Gruppe zu analysieren.

Definieren der Unternehmensinfrastruktur

Ein wichtiger Aspekt bei der Implementierung Ihres Service Desk mit CA SDM ist die Definition Ihrer Unternehmensinfrastruktur. Hierzu richten Sie folgende Objekte ein:

- Konfigurieren von Elementfamilien und -Klassen
- Hersteller und Modelle
- Dienststatus
- Anbieter und Anbietertypen

Folgende Informationen liefern eine allgemeine Beschreibung zu jedem Objekt und erläutern, wie das Objekt im Produkt verwendet wird.

Hinweis: Weitere Informationen zur Definition der einzelnen Objekte finden Sie in der *Online-Hilfe*.

Objektdefinitionsreihenfolge

Beim Definieren von Objekten beginnen Sie auf den unteren Ebenen der Objekthierarchie. Auf diese Weise können Sie beim Definieren von Objekten auf höheren Ebenen unter vorhandenen Objekten auf den unteren Hierarchieebenen auswählen. Da eine Klasse eine Familie (Bezüge) hat, definieren Sie beispielsweise zuerst Familien und dann Klassen. Bei Configuration Items wird ähnlich verfahren: Da sich diese oben in der Hierarchie befinden, definieren Sie sie zum Schluss, nachdem Sie alle Unterstützungsobjekte definiert haben. Datenobjekte werden daher in der folgenden Reihenfolge definiert:

Zuerst zu definieren	Als Nächstes zu definieren	Zum Schluss zu definieren
Familien	Klassen	Configuration Items
Hersteller	Modelle	Configuration Items
Dienststatus	Configuration Items	
Anbietertypen	Anbieter	Configuration Items

Configuration Item-Familien und -Klassen

Familien klassifizieren Configuration Items nach Typ und weisen jedem einzelnen Element sinnvolle Attribute zu. *Klassen* identifizieren allgemeine Kategorien von Configuration Items, die in Ihrem Unternehmen unterstützt werden. Familien sind breit angelegte Kategorien von Configuration Items, wie zum Beispiel Hardware, Software und Dienste. Klassen sind spezifischere Kategorien innerhalb der breiteren Familienkategorie. Zum Beispiel kann die Familie "Hardware" Klassen wie "Modem", "Router", "Repeater" und "Bridge" enthalten.

Indem Sie Ihre Configuration Items in Familien und Klassen unterteilen, können Sie sie leichter verwalten. Zum Beispiel können Sie eine Liste von Configuration Items generieren, die einer bestimmten Familie oder Klasse angehören.

Hersteller und Modelle

Hersteller identifizieren die Hersteller der verschiedenen Configuration Items, die für Ihr Unternehmen relevant sind. *Modelle* enthalten bestimmte Informationen über die Produkte, die ein bestimmter Hersteller Ihrem Unternehmen bereitstellt. Zum Beispiel können Sie als Hersteller eine bestimmte Softwarefirma definieren. Anschließend definieren Sie als Modelle jede der Anwendungen, die diese Firma Ihrem Unternehmen bereitstellt.

Indem Sie Hersteller und Modelle definieren, können Sie Ihre Configuration Items leichter verwalten. Zum Beispiel können Sie eine Liste von Modellen generieren, die von einem bestimmten Hersteller bereitgestellt werden. Außerdem können Sie eine Liste von Configuration Items eines bestimmten Modells generieren.

Dienststatus

Servicestatus zeigt die Funktionsbereitschaft von Configuration Items an. Beispielwerte für den Servicestatus sind *In Betrieb*, *In Reparatur* oder *Ausgesetzt*. Wenn Sie Servicestatus festlegen, können Sie die Verfügbarkeit und die Verwendung von Configuration Items in Ihrem Unternehmen verfolgen. Zum Beispiel können Sie eine Liste der Configuration Items generieren, die momentan in Reparatur sind.

Anbietertypen und Anbieter

Anbietertypen sind Klassifizierungen für Anbieter, die die Art der Firma angeben, die Configuration Items anbietet. Zum Beispiel können Sie Anbieter, von denen Sie Configuration Items leasen, als Leasinggeber klassifizieren, während Sie Anbieter, die Ihnen Dienste bieten, als Dienstanbieter klassifizieren.

Anbieter identifizieren die Firmen, die Ihrem Unternehmen Lieferungen oder Leistungen bieten, einschließlich der Art der Firma und eines primären Kontakts. Sie können auf einen Anbieter nicht nur durch Configuration Items, sondern auch im Kontaktdatensatz eines Benutzers verweisen.

Die Definition von Anbietertypen und Anbietern ist eine günstige Methode, Ihre Configuration Items zu organisieren. Zum Beispiel können Sie eine Liste der Anbieter generieren, die einem bestimmten Anbietertyp angehören, oder Sie können eine Liste der Configuration Items eines bestimmten Anbieters generieren.

Configuration Items

Configuration Items sind die Geräte, Software und Dienste, die Ihre Unternehmensinfrastruktur bilden. Mit den Informationen, die mit einem Configuration Item verknüpft sind, kann ein Configuration Item eindeutig identifiziert und seine genaue Position festgestellt werden. Configuration Items können Kontakten (private Configuration Items) und Organisationen (gemeinsam genutzte Configuration Items) zugeordnet werden. Mit Hilfe von Configuration Items können Sie Folgendes identifizieren, anzeigen und angeben:

- Configuration Items nach Name, Klasse und Familie identifizieren.
- Bestandsinformationen angeben.
- Zusätzliche Eigenschaften zur Definition des Configuration Item angeben.
- Mit dem Configuration Item verbundene Kommentare protokollieren und anzeigen.
- Standortinformationen für das Configuration Item angeben.
- Dienstinformationen, zum Beispiel einen Dienstyp, für das Configuration Item angeben.
- Dem Configuration Item zugewiesene Kontakte und Organisationen anzeigen und definieren.
- Hierarchie- und Peer-to-Peer-Beziehungen zwischen Configuration Items angeben.
- Mit dem Configuration Item verknüpfte Tickets anzeigen.

Sie müssen nicht alle diese Informationen für Configuration Items definieren. Es ist jedoch ratsam, so viele Informationen wie möglich für Configuration Items zu definieren, da Sie dadurch ein eindeutigeres Bild bekommen, wenn eine Auswirkungsanalyse für die IT-Organisation durchgeführt wird.

Weitere Informationen:

[Erstellen von Configuration Items](#) (siehe Seite 610)

[Configuration Items: Kontakt, Standort und Organisation](#) (siehe Seite 614)

[CI Relationships](#) (siehe Seite 617)

Externe Anlagenverwaltungstools

Sie können Ihre CA SDM-Installation in andere Asset Management-Tools wie CA NSM, CA Asset Management und CA APM integrieren. Nachstehend finden Sie eine Liste der Asset Management-Funktionen dieser CA SDM-Tools:

- CA NSM stellt das pdm_nsmimp-Dienstprogramm (nur für Windows) bereit, mit dem CA SDM Asset-Informationen hinzugefügt werden können.

- CA Asset Management bietet einen vollständigen Satz von Hardware und Software-Bestandsfunktionen. Wird ein CI im CA SDM-Client angezeigt, können Sie auf die Schaltfläche "Asset-Viewer" klicken, um Zusatzinformationen zu dem Asset anzuzeigen.

Die Integration zwischen CA SDM und CA Asset Management wird aktiviert, wenn die Produkte in der gleichen MDB installiert sind.

- CA Asset Portfolio Management stellt eine umfassende Zusammenstellung von Funktionen für den gesamten Lebenszyklus von Assets bereit. Wird ein CI im CA SDM-Client angezeigt, können Sie auf die Schaltfläche "Asset-Viewer" klicken, um Zusatzinformationen zu dem Asset anzuzeigen.

Die Integration zwischen CA SDM und CA Asset Management wird aktiviert, wenn die Produkte auf derselben MDB installiert sind.

Hinweis: Weitere Informationen zum Integrieren Ihrer CA SDM-Installation in andere Asset-Verwaltungstools finden Sie im *Implementierungshandbuch*.

Mehrere Mandanten

Mit *Mandantenfähigkeit* können mehrere unabhängige Mandanten (und ihre Anwender) eine einzige Implementierung von CA SDM gemeinsam nutzen. Mandantenanwender interagieren nur auf definierte Art und Weise miteinander, wie durch ihre *Rollen* und *Mandantenhierarchien* angegeben. Außer wenn Zugriff von einer Rolle oder Hierarchie gewährt wird, sieht jeder Mandant die CA SDM-Implementierung typischerweise allein für den Eigennutzen und kann Daten eines anderen Mandanten nicht aktualisieren oder anzeigen.

Durch Mandantenfähigkeit können Mandanten Hardware- und Anwendungs-Support-Ressourcen gemeinsam nutzen. Dadurch werden Kosten für beide gespart und gleichzeitig viele Vorteile einer unabhängigen Implementierung erzielt.

Hinweis: Weitere Informationen zum Installieren und Konfigurieren der Mandantenfähigkeit finden Sie im *Implementierungshandbuch*.

Service Provider

Der *Service Provider* ist der erste Mandant (Eigentümer) in einer CA SDM Installation mit mehreren Mandanten. Der erste zu einer CA SDM-Installation hinzugefügte Mandant ist immer der Mandant "Service Provider". Der Mandant "Service Provider" kann keinen übergeordneten Mandanten haben.

CA SDM ordnet den privilegierten Benutzer (typischerweise ServiceDesk auf Windows, oder srvcdesk auf Linux/UNIX) dem Mandanten "Service Provider" zu.

Nur der Mandant "Service Provider" kann eine der folgenden CA SDM-Aufgaben ausführen:

- Festlegen von CA SDM-Optionen
- Festlegen von Knowledge Management-Optionen
- Festlegen von Support-Automatisierung-Optionen
- Erstellen von Tabellen oder Spalten
- Erstellen, Bearbeiten oder Löschen von Mandanten
- Mandanten gestatten, untergeordnete Mandanten zu haben
- Aktualisieren öffentlicher Daten

Hinweis: Ein Administrator kann Mandantenbenutzern Zugriff auf Daten auch von anderen gewähren. Service Provider-fremde Mandanten-Analysten haben nur Zugriff auf ihren eigenen Mandanten und ihre eigenen untergeordneten Mandanten, außer ihr Zugriff auf Funktion wird so aktualisiert, dass der Mandant des Analysten eingeschlossen ist. Zum Beispiel kann eine Rollendefinition separaten Schreib- und Lesezugriff auf bestimmte Mandantengruppen für Benutzer innerhalb dieser Rolle festlegen.

Wichtig: Der erste erstellte Mandant wird als Service Provider festgelegt. Danach sind das Kontrollkästchen "Service Provider" und das Feld "Datensatz-Status" schreibgeschützt.

Weitere Informationen:

[Service Provider-Verwaltung](#) (siehe Seite 131)

[Mandantenzugriff](#) (siehe Seite 134)

[Erstellen eines Mandanten](#) (siehe Seite 144)

Service Provider-Verwaltung

Der Service Provider kann Mandanten gestatten, ihre eigenen Einstellungen zu verwalten. Mandantenadministratoren haben Zugriff auf einen Teilsatz von Administrationsaufgaben, der für alle Mandanten gleich ist, so dass die ADMIN_TREE-Tabelle selbst nicht mit Mandanten versehen ist. Statt dessen, definiert die Standard-Mandantenadministrator-Rolle die Verwaltungsfunktionen, die für Mandantenadministratoren verfügbar sind.

Um einen Benutzer als einen Mandantenadministrator festzulegen, wählen Sie den Mandantenadministrator für die Rolle dieses Benutzers aus.

Wie Multi-Tenancy funktioniert

Wenn die Option "Mehrere Mandanten" aktiv ist, können Sie jedem Kontakt Zugriff auf alle Mandanten (öffentlich), einen einzelnen Mandanten oder eine Gruppe von Mandanten (benutzerdefiniert oder produktverwaltet) gewähren. Die Rolle eines Kontaktes steuert den Zugriff, wobei Lese- und Schreibzugriff unabhängig voneinander festgelegt sind. Da der Mandantenzugriff rollenabhängig ist und ein Kontakt während einer Sitzung verschiedene Rollen einnehmen kann, kann sich der Kontaktmandantenzugriff auch ändern.

Wenn Mandantenfähigkeit installiert wird, schließen die meisten CA SDM-Objekte ein Mandantenattribut mit ein, das angibt, zu welchem Mandant das Objekt gehört. Objekte fallen in drei Gruppen. Die jeweilige Gruppe hängt vom Mandantenattribut und seiner Verwendung ab:

Ohne Mandant

Definiert Objekte ohne ein Mandantenattribut. Alle Daten in diesen Objekten sind öffentlich.

Beispiele: Priorität und Dringlichkeit.

Mandant erforderlich

Definiert Objekte mit einem Mandantenattribut, das nicht NULL sein kann (die wird von CA SDM, nicht der DBMS, durchgesetzt). Alle Daten in diesen Objekten sind mit individuellen Mandanten verbunden. Es gibt keine öffentlichen Daten.

Beispiele: Tickettabellen (Request, Issue und Change)

Mandant optional

Definiert Objekte mit einem Mandantenattribut, das NULL sein kann. Einige der Daten in diesen Objekten sind öffentlich, andere sind mit bestimmten Mandanten verknüpft. Mandanten sehen Objekte als eine Zusammenführung öffentlicher Daten und deren zugeordneten mandantenspezifischen Daten.

Beispiele: Kategorie und Lokation

Wenn ein Benutzer die Datenbank abfragt, beschränkt CA SDM die Ergebnisse auf Objekte, auf die der Benutzer zugreifen darf. Diese Beschränkung gilt zusätzlich zu den geltenden Beschränkungen in Bezug Datenpartitionen. Das heißt, dass Sie niemals Daten in Tabellen vom Typ "Mandant erforderlich" und "Mandant optional" sehen können, mit Ausnahme der Daten, die zu Mandanten gehören, auf die Sie Zugriff haben.

Wenn ein Mandantenbenutzer darum bittet, ein Datenbankobjekt zu erstellen oder zu aktualisieren, überprüft CA SDM, dass das Objekt zu einem Mandanten gehört, den der Benutzer aufgrund seiner aktuellen Rolle aktualisieren darf und dass alle Fremdschlüsselreferenzen (SREL) des Objektes zu anderen Objekten wie folgt sind: zu öffentlichen Objekten (ohne Mandant), zu Objekten desselben Mandanten oder zu Objekten von Mandanten innerhalb der Mandantenhierarchie, die über dem Mandanten des Objekts stehen. Das heißt, Ein Mandantenobjekt darf sich auf solche Objekte beziehen, die sich auf seinen übergeordneten Mandanten beziehen, auf dessen übergeordneten Mandanten usw.

Wenn ein Anwender, der ein Objekt erstellt, Aktualisierungszugriff auf mehrfache Mandanten hat, muss der Anwender den Mandanten explizit angeben, entweder direkt oder indirekt.

Hinweis: Es gibt eine Ausnahme zu der Einschränkung von SREL-Referenzen. Manche SREL-Referenzen (wie z. B. der Zuständige eines Incidents) dürfen sich auf Objekte zu beziehen, die zu Mandanten in der Mandantenhierarchie ihres Objekts gehören. Solche Referenzen werden im CA SDM-Objektschema (Majic) als SERVICE_PROVIDER_ELIGIBLE bezeichnet. Das Flag SERVICE_PROVIDER_ELIGIBLE wirkt sich nur dann aus, wenn sich der Service Provider-Mandant in der Mandantenhierarchie nicht über dem Mandantenobjekt befindet. Wenn sich der Service Provider-Mandant in der Hierarchie befindet, erlauben die Mandantenvvalidierungsregeln das Erstellen von Service Provider-Referenzen.

Ein Service Provider-Benutzer, der darum bittet, ein Objekt zu erstellen oder zu aktualisieren, unterliegt den gleichen Beschränkungen wie Mandantenbenutzer, außer dass es Service Provider-Benutzern genehmigt werden kann, öffentliche Objekte zu erstellen oder zu aktualisieren. Die aktive Rolle des Service Provider-Anwender steuert diese Autorisierung.

Hinweis: Wenn CA SDM einen Benutzer bei der Aktualisierung von Mandantendaten beschränkt, kann eine Fehlermeldung eine Beschränkung der Datenpartition ankündigen. Wenn Sie diese Fehlermeldung erhalten, bestehen entweder Datenpartitions- oder Mandantenfähigkeits-Beschränkungen.

Die Option "Mandantenfähigkeit".

Sie aktivieren die Mandantenfähigkeit durch Installieren einer der folgenden Mandantenfähigkeits-Optionen:

- **Deaktiviert** - Die Mandantenfähigkeit wird nicht verwendet. Mandantenfähigkeits-Merkmale sind nicht verfügbar, und Objekte haben kein Attribut "Mandant". Diese Option ist die Standardeinstellung einer neuen CA SDM-Installation.
- **Aufbau**: Mandantenfähigkeits-Merkmale bestehen für Administratoren, so dass mandantenbezogene Objekte und Attribute sichtbar und editierbar sind. CA SDM setzt allerdings keine Mandantenbeschränkung durch, und Benutzer ohne Administratorrechte sehen keine Änderungen. Diese Einstellung ermöglicht es Administratoren, sich auf die Mandantenfähigkeit einzurichten, indem Sie z. B. Mandanten definieren oder Objekte zu Mandanten zuordnen ohne den normalen Gebrauch von CA SDM zu beeinträchtigen.
- **Aktiviert** - Die Mandantenfähigkeit ist voll einsatzbereit. Alle Benutzer sehen die für Sie geltenden Änderungen der Benutzeroberfläche, und CA SDM erzwingt Mandantenbeschränkungen.

Hinweis: Weitere Informationen zum Installieren und Implementieren der Mandantenfähigkeit, einschließlich zusätzlicher Optionen für das Erzwingen dieser Features finden Sie im *Implementierungshandbuch*.

Informationen für Mandanten

Sie erstellen und aktualisieren Mandanten wenn Sie die Mandantenfähigkeit installieren (entweder im Aufbaumodus oder im Modus "vollständige Durchsetzung"). Informationen, die für einen Mandanten verwaltet werden, ähneln den Informationen über Organisationen, mit Ausnahme der folgenden zwei Attribute:

Logo

Fügt einer Bilddatei eines Mandanten mit einem Logo eine URL hinzu. Das Logo wird auf der Mandantendetailseite selbst sowie als ein Ersatz für das CA-Logo auf Webformularen, die von Mandantenbenutzern aufgerufen werden, angezeigt. Es kann auch ein dem Mandantenbenutzer zugeordnetes Objekt angezeigt werden.

Service Provider

Zeigt an, ob ein Mandant der Service Provider ist. Der Service Provider-Mandant ist immer der erste hinzugefügte Mandant. Wenn der Administrator den ersten Mandanten hinzufügt, tritt das Folgende auf:

- Der erste Mandant wird der Service Provider. Diese Zuordnung kann nicht geändert werden.
- Für den berechtigten Benutzer (meist ServiceDesk) und alle Systemkontakte (z. B. System_AHD_Generated) wird festgelegt, dass sie dem neuen Service Provider-Mandanten angehören

Hinweis: Der Systembenutzer "Administrator" wird nur in Windows hinzugefügt und ihm wird kein Mandant zugewiesen. Der privilegierte Benutzer muss einen Mandanten einem Administrator manuell zuweisen.

Mandantenzugriff

Die Rolle eines CA SDM-Anwenders bestimmt sowohl die Zugriffsautorisierung als auch die Benutzerschnittstelle. Der Satz an Rollen, die Anwendern zur Verfügung stehen, hängt von deren Zugriffstyp ab. Mit Mandantenfähigkeit können Sie den Mandanten oder die Mandantengruppe steuern, auf die ein Anwender innerhalb der Rolle zugreifen darf.

Die Seite "Rolle - Detail" verfügt über die Dropdown-Listen "Mandantenzugriff" und "Mandantenschreibzugriff" auf der Registerkarte "Autorisierung". Mandantenzugriff ist schreibgeschützt, und Mandantenschreibzugriff ermöglicht zusätzlich die Erstellung und Aktualisierung.

Sie können Rollen folgende Zuordnungen zuweisen:

Identisch mit Mandantenzugriff (Nur Mandantenschreibzugriff)

Legt fest, dass der Mandantenschreibzugriff identisch mit der Einstellung "Mandantenzugriff" ist. Standard für Mandantenschreibzugriff und nur gültig für Mandantenschreibzugriff.

Alle Mandanten

Entfernt Mandanteneinschränkungen. CA SDM erlaubt einem Anwender in einer Rolle mit diesem Zugriff, ein beliebiges Objekt in der Datenbank anzuzeigen (Lesezugriff) oder ein beliebiges Objekt mit Mandanten zu erstellen und zu aktualisieren (Schreibzugriff). Wenn Anwender mit "Alle Mandanten"-Zugriff ein Objekt erstellen, müssen sie für CA SDM den Mandanten des neuen Objekts auswählen.

Einzelner Mandant

Legt den Mandantenzugriff einer Rolle auf einen benannten Mandanten fest. Wenn diese <Option ausgewählt wird, erscheint ein zweites Feld auf der Web-Oberfläche, mit dem ein bestimmter Mandant ausgewählt werden kann. CA SDM beschränkt einen Anwender in einer Rolle mit diesem Zugriff darauf, nur solche Objekte anzuzeigen (Lesezugriff) oder zu erstellen und zu aktualisieren (Schreibzugriff), die dem benannten Mandanten zugeordnet sind. Diese Auswahl ist für Mandantenzugriff oder Mandantenschreibzugriff gültig.

Mandantengruppe

Legt den Mandantenzugriff einer Rolle auf eine anwenderspezifische oder vom System gepflegte Mandantengruppe fest. Wenn die Mandantengruppen-Möglichkeit ausgewählt ist, erscheint ein zweites Feld auf der Web-Oberfläche, mit einer bestimmten Mandantengruppe ausgewählt werden kann. CA SDM beschränkt einen Anwender mit der Rolle darauf, nur solche Objekte anzuzeigen (Lesezugriff) oder zu erstellen und zu aktualisieren (Schreibzugriff), die einer der Mandanten in der Gruppe zugeordnet sind. Wenn ein Anwender mit Mandantengruppenzugriff ein Objekt erstellt, muss er für CA SDM den Mandanten für das neue Objekt auswählen. Diese Auswahl ist für Mandantenzugriff oder Mandantenschreibzugriff gültig.

Mandant des Kontakts

Legt den Mandantenzugriff einer Rolle auf den Mandanten des benutzenden Kontakts fest. CA SDM beschränkt einen Anwender in einer Rolle mit diesem Zugriff darauf, nur solche Objekte anzuzeigen (Lesezugriff) oder zu erstellen und zu aktualisieren (Schreibzugriff), die ihrem eigenen Mandanten zugeordnet sind. Diese Auswahl ist für Mandantenzugriff oder Mandantenschreibzugriff gültig.

Mandantengruppe des Kontakts (Nur Analyst)

Legt den Rollzugriff eines Analysten auf die Mandantengruppe fest, mit der der Analyst arbeitet, wie auf dem Kontaktdatensatz des Analysten angegeben. Wenn der Anwender mit der Rolle kein Analyst ist, hat diese Auswahl die gleiche Wirkung wie Mandant des Kontakts. Sie gilt sowohl für Mandantenzugriff als auch für Mandantenschreibzugriff.

Untergeordnete Mandantengruppe des Kontakts

Legt den Mandantenzugriff einer Rolle zur untergeordneten Mandantengruppe des benutzenden Kontakts fest. CA SDM beschränkt einen Anwender in einer Rolle mit diesem Zugriff darauf, nur solche Objekte anzuzeigen (Lesezugriff) oder zu erstellen und zu aktualisieren (Schreibzugriff), die ihrer eigenen untergeordneten Mandantengruppe zugeordnet sind. Diese Auswahl ist für Mandantenzugriff oder Mandantenschreibzugriff gültig.

Untergeordnete Mandantengruppe des Kontakts

Legt den Mandantenzugriff einer Rolle zur untergeordneten Mandantengruppe des benutzenden Kontakts fest. CA SDM beschränkt einen Anwender in einer Rolle mit diesem Zugriff darauf, nur solche Objekte anzuzeigen (Lesezugriff) oder zu erstellen und zu aktualisieren (Schreibzugriff), die ihrer eigenen übergeordneten Mandantengruppe zugeordnet sind. Diese Auswahl ist für Mandantenzugriff oder Mandantenschreibzugriff gültig.

Verwandte Mandantengruppe des Kontakts

Legt den Mandantenzugriff einer Rolle zur verwandten Mandantengruppe des benutzenden Kontakts fest. CA SDM beschränkt einen Anwender in einer Rolle mit diesem Zugriff darauf, nur solche Objekte anzuzeigen (Lesezugriff) oder zu erstellen und zu aktualisieren (Schreibzugriff), die ihrer eigenen verwandten Mandantengruppe zugeordnet sind. Diese Auswahl ist für Mandantenzugriff oder Mandantenschreibzugriff gültig.

Alle Anwender können öffentliche Daten ungeachtet der Zugriffsrechte ihrer gegenwärtigen Rolle anzeigen. Das Kontrollkästchen "Öffentlich aktualisieren" steuert, ob ein Anwender des Service Providers in der Rolle öffentliche Daten erstellen oder aktualisieren darf. Mandantenanwender (Anwender, die einem anderen Mandanten angehören als dem Service Provider) können unabhängig von ihrer Rolle keine öffentlichen Daten aktualisieren.

Weitere Informationen:

[Bearbeiten des Mandantenzugriffs für eine Rolle](#) (siehe Seite 136)

Bearbeiten des Mandantenzugriffs für eine Rolle

Sie können den Mandantenzugriff für eine Rolle zuweisen oder bearbeiten.

So bearbeiten Sie den Mandantenzugriff für eine Rolle:

1. Navigieren Sie zu "Sicherheits- und Rollenmanagement" > "Rollenmanagement" > "Rollenliste".

Die Rollenliste wird angezeigt.

2. Klicken Sie auf eine Rolle.

Die Seite "Rolle - Detail" wird angezeigt.

3. Klicken Sie auf "Bearbeiten".

Die Seite "Rolle aktualisieren" wird angezeigt.

4. Wählen Sie die Optionen für "Mandantenzugriff" und "Mandantenschreibzugriff" aus.

Hinweis: Gehen Sie mit Vorsicht vor, wenn Sie unterschiedliche Optionen für diese Einstellungen auswählen.

5. Klicken Sie auf "Speichern".

Die aktualisierten Optionen für den Mandantenzugriff werden für die Rolle gespeichert.

Mandanten-Nutzungsbedingungen

Wenn sich der Endbenutzer bei CA SDM anmeldet, wird zunächst eine Seite mit den Nutzungsbedingungen angezeigt. Die Nutzungsbedingungen weisen den Benutzer auf die ordnungsgemäße Nutzung des Produkts hin. Der Benutzer muss den Bedingungen zustimmen, bevor er mit der Anmeldung bei CA SDM fortfahren kann. Nach jedem Anmeldeversuch werden in das Standardprotokoll und das Benutzerereignisprotokoll geschrieben.

Für die Nutzungsbedingungen können Sie folgende Aktionen ausführen:

- Sie können Nutzungsbedingungen erstellen, aktualisieren und löschen.
- Sie können Nutzungsbedingungen mit einem Mandanten verknüpfen.

Hinweis: Sie müssen die Mandantenfähigkeit aktivieren und mindestens einen Mandanten konfigurieren, bevor Sie einem Mandanten Nutzungsbedingungen zuordnen können.

- Sie können die Annahme der Nutzungsbedingungen durch den Endbenutzer bei jeder Anmeldung erzwingen.
- Sie können die erste Seite leer lassen, so dass der Endbenutzer die Nutzungsbedingungen ignoriert.

Weitere Informationen:

[So konfigurieren Sie die Nutzungsbedingungen](#) (siehe Seite 138)

So konfigurieren Sie die Nutzungsbedingungen

Wenn sich der Endbenutzer bei CA SDM anmeldet, wird zunächst eine Seite mit den Nutzungsbedingungen angezeigt. Die Nutzungsbedingungen weisen den Benutzer auf die ordnungsgemäße Nutzung des Produkts hin. Der Benutzer muss den Bedingungen zustimmen, bevor er mit der Anmeldung bei CA SDM fortfahren kann. Wenn der Endbenutzer die Nutzungsbedingungen akzeptiert, fährt CA SDM mit der Anmeldung fort und zeigt das Hauptformular an. Wenn der Benutzer die Nutzungsbedingungen nicht akzeptiert, weist CA SDM die Anmeldung zurück. Nach jedem Anmeldeversuch werden in das Standardprotokoll und das Benutzerereignisprotokoll geschrieben.

I. d. R. konfigurieren Sie den Kontakt als Mandanten der Nutzungsbedingungen. Wenn der Kontakt als Mandant mit inaktiven Nutzungsbedingungen konfiguriert wird oder wenn in der Dropdownliste "Nutzungsbedingungen" der Wert <empty> ausgewählt wird, zeigt CA SDM die Nutzungsbedingungen der direkt und indirekt übergeordneten Elemente des Mandanten an. Wenn auf diese Weise keine Nutzungsbedingungen gefunden werden, fährt CA SDM mit der Anmeldung fort. Wenn Sie einen Mandanten mit leeren Nutzungsbedingungen konfigurieren, fährt CA SDM mit der Anmeldung fort und zeigt das Hauptformular an.

Sie können Nutzungsbedingungen folgendermaßen konfigurieren:

1. Aktivieren Sie mehrere Mandanten.
2. Konfigurieren Sie einen oder mehrere Mandanten.
3. Definieren Sie Nutzungsbedingungen.
4. Aktualisieren Sie einen Mandanten, um die speziellen Nutzungsbedingungen zu verwenden.

Hinweis: Detailinformationen zum Erstellen und Ändern von Nutzungsbedingungen finden Sie in der *Online-Hilfe*.

Auswirkung auf die Benutzerschnittstelle

Durch die Installation der Mandantenfähigkeitsfunktion ändert sich die Benutzerschnittstelle, je nach Autorisierung und Mandantenzugriff, der der Rolle des Benutzers zugeordnet ist. Die Änderungen wirken sich sowohl auf Mandantenbenutzer als auch auf Service Provider-Benutzer aus.

Mandantenbenutzer

Wenn die Rolle eines Benutzers auf einen einzelnen Mandanten beschränkt wird und der Benutzer kein Administrator ist, können Sie das Standard-CA Technologies-Logo auf allen Seiten durch ein benutzerdefiniertes Mandantenlogo ersetzen. Diese Ersetzung hängt davon ab, ob ein Logo auf der Mandantendetailseite für den Mandanten definiert wird; dies ist je nach Mandant optional.

Die einzige Benutzerschnittstellenänderung für Mandantenbenutzer, die keine Administratoren sind, ist, dass Menüelemente oder -schaltflächen mit der Möglichkeit zur Aktualisierung oder Bearbeitung (Schaltfläche "Bearbeiten" oder Schaltfläche "Neu erstellen" auf der Listenseite) für öffentliche Objekte deaktiviert werden, da Mandantenbenutzer nicht autorisiert sind, öffentliche Objekte zu aktualisieren.

Mandantenadministratoren

Mandantenadministratoren mit Zugriff für einen einzigen Mandanten, die mandantenoptionale Objekte anzeigen, werden eine zusätzliche Änderung an der Benutzerschnittstelle bemerken. Listenseiten für diese Objekte beinhalten automatisch eine Spalte "Öffentlich", die angibt, ob die Listenzeile öffentliche Daten enthält. Außerdem ist das erste Element im Suchfilter eine Dropdown-Liste mit öffentlichen Daten, die folgenden Auswahlen enthält:

- Einschließen (Standard)
- Ausschließen
- Nur

Ein Mandantenadministrator mit Zugriff auf mehrere Mandanten bekommt eine Spalte "Mandant" auf Listenseite für beliebige Objekte mit Mandanten angezeigt. Diese Spalte nimmt den Platz der Spalte "Öffentlich" in Listen mit mandantenoptionalen Tabellen ein.

Benutzer, die eine Mandantengruppe anzeigen können

Wenn die Rolle eines Benutzers den Zugriff zum Anzeigen von mehreren Mandanten gestattet oder ein Service Provider-Benutzer die Autorisierung "Öffentlich aktualisieren" besitzt, ändern sich die CA SDM-Listenformulare folgendermaßen:

Objekte ohne Mandant

Objekte ohne Mandant enthalten nur öffentliche Daten. Ein Service Provider-Benutzer darf ein Objekt ohne Mandant nur erstellen oder aktualisieren, wenn dessen Rolle eine Autorisierung "Öffentlich aktualisieren" aufweist. Andernfalls deaktiviert die Benutzerschnittstelle Menüelemente und -schaltfläche zur Aktualisierung oder Bearbeitung, wie z. B. die Schaltfläche "Bearbeiten" an sich, oder die Schaltfläche "Neu erstellen" auf einer Listenseite. Mandantenbenutzer können keine öffentlichen Objekte aktualisieren, und diese Benutzer sehen niemals eine Schaltfläche "Bearbeiten" oder "Neu erstellen" auf einer Listenseite für ein Objekt ohne Mandant.

Mandantenabhängige Objekte

Mandantenabhängige Objekte enthalten nur Daten, die mit einem bestimmten Mandant verknüpft sind. Listenformulare für diese Objekte enthalten automatisch eine Spalte "Mandant" nach der letzten Verknüpfungsspalte. Außerdem enthält der Suchfilter eine Mieterauswahl, die dem Benutzer ermöglicht, eine Liste auf einen einzigen Mandanten zu beschränken.

Objekte mit optionalem Mandant

Objekte mit optionalem Mandant enthalten sowohl öffentliche als auch mandantenspezifische Daten. Listenformulare für diese Objekte enthalten automatisch eine Spalte "Mandant" (ein leerer Mandant bedeutet ein öffentliches Objekt). Außerdem enthält der Suchfilter sowohl eine Mandantenauswahl als auch eine Dropdown-Liste "Öffentliche Daten" (die gleiche, den auch Mandantenadministratoren sehen).

Hinweis: Wenn Tabellen erforderlicher Mandanten fälschlicherweise Daten ohne Mandanten in einem System mit mehreren Mandanten enthalten, erscheint eine Dropdown-Liste mit öffentlichen Daten in Tabellen erforderlicher Mandanten und Sie erhalten folgende Meldung: "AHD05358 Es gab nn aktive xxx-Objekte ohne Mandant beim Start von Service-Desk."

Benutzer mit der Möglichkeit zur Aktualisierung von mehreren Mandanten

Wenn es die Rolle des Benutzers ermöglicht, auf mehrere Mandanten zuzugreifen, oder die Benutzerrolle eines Service Providers eine Autorisierung "Öffentlich aktualisieren" hat (typisch für einen Analysten, der für einen Service Provider arbeitet), ändern sich Detailseiten folgendermaßen:

Objekte ohne Mandant

Objekte ohne Mandant enthalten nur öffentliche Daten. Es gibt keine Änderungen ihrer Detailseiten für einen Benutzer des Service Providers mit einer Autorisierung "Öffentlich aktualisieren". Wenn der Benutzer eine Rolle ohne Autorisierung "Öffentlich aktualisieren" besitzt oder nicht zum Service Provider gehört, haben schreibgeschützte Seiten für Objekte ohne Mandant keine Schaltfläche "Bearbeiten".

Vorhandene Objekte erforderlicher Mandanten

Mandantenabhängige Objekte enthalten nur Daten, die mit einem bestimmten Mandant verknüpft sind. Detailseiten für vorhandene Objekte erforderlicher Mandanten zeigen den Mandanten des Objekts als Teil des Standard-Seiten-Headers.

Objekte mit optionalem Mandant

Objekte mit optionalem Mandant enthalten sowohl öffentliche als auch mandantenspezifische Daten. Die Detailseite für diese Objekte hängt davon ab, ob der Benutzer zum Service Provider gehört und eine Rolle mit Autorisierung "Öffentlich aktualisieren" besitzt:

- Wenn die Rolle eines Benutzers des Service Providers eine Autorisierung "Öffentlich aktualisieren" besitzt, ist die Detailseite identisch mit der Seite für Objekte erforderlicher Mandanten.
- Wenn die Rolle des Benutzers keine Autorisierung "Öffentlich aktualisieren" haben oder der Benutzer nicht zum Service Provider gehört, haben Detailseiten für öffentliche Objekte keine Schaltfläche "Bearbeiten". Andere Detailseiten sind mit denen für Objekte erforderlicher Mandanten identisch.

Support-Automatisierung-Auswirkung

Die Auswirkung von Mandantenfähigkeit auf Ihrer Support-Umgebung hängt von Mandanten- und Rollenbeschränkungen ab, die Endbenutzern und Analysten auferlegt wurden. Der Service Provider verwaltet die Lese-/Schreibberechtigungen sowohl für öffentliche als auch mandantenspezifische Daten. Zum Beispiel kann ein Analyst Unterstützungssitzungen von der öffentlichen Warteschlange und einer mandantenspezifischen Warteschlange verarbeiten, aber der Analyst kann nur Live-Unterstützungs-Tools verwenden, die für jeden Mandanten aktiviert sind.

Passen Sie bei Endbenutzern mit Support-Automatisierung-Zugriff die Konfiguration nicht so an, dass Schreibzugriff auf einen Mandanten haben, der kein untergeordneter Mandant des besitzenden Mandanten des Endbenutzers ist, es sei denn, die FK-Gruppe (Fremdschlüssel) wird so verändert, dass sie den besitzenden Mandanten einschließt. Wenn der Endbenutzer einen Anmeldemandanten auswählt oder über ein Ticket in einem Mandanten, der dieses Kriterium nicht erfüllt, eingeladen wird, erhält er beim Versuch, auf den Support-Automatisierung-Endbenutzer-Client zuzugreifen, eine Fehlermeldung. Diese Beschränkung gilt nicht, wenn der besitzende Mandant des Endbenutzers der Mandant des Service Providers ist.

Passen Sie bei Analysten mit Support-Automatisierung-Zugriff die Konfiguration so an, dass der Analyst Schreibzugriff auf einen Mandanten hat, der kein untergeordneter Mandant des besitzenden Mandanten des Analysten ist, es sei denn, die FK-Gruppe (Fremdschlüssel) wird so verändert, dass sie den besitzenden Mandant einschließt. Wenn der Analyst versucht, in einem Mandanten, der diese Kriterien nicht erfüllt, einen Endbenutzer zu verarbeiten oder einen Endbenutzer von einem Ticket einzuladen, erhält der Analyst eine Fehlermeldung.

Analysten und Endbenutzer ohne Lesezugriff auf ihren Mandanten können den Support-Automatisierung-Client nicht starten. Bei Analysten wird in diesem Fall eine Warnmeldung in CA SDM so wie von der Haupt-Registerkarte der Support-Automatisierung angezeigt.

Sie können die folgenden Rollen benutzen, um Support-Automatisierung-Benutzer zu verwalten:

Support-Automatisierung-Analyst

Bietet Endbenutzer-Support mit Hilfe der Live-Unterstützung. Der Service Provider legt den geeigneten Mandantenzugriff fest und kann Live-Unterstützungs-Tools und den Lese-/Schreibzugriff auf automatisierte Aufgaben aktivieren.

Wichtig! Wenn ein Analyst, der nicht dem Service Provider angehört, Schreibzugriff auf einen übergeordneten, Zwillings- oder beziehungslosen Mandanten hat, muss die Funktion für diesen Mandanten aktualisiert werden. Analysten ohne Lesezugriff auf ihren Mandanten können den Analysten-Client der Support-Automatisierung nicht starten, und in CA SDM wird eine Warnmeldung angezeigt, beispielsweise von der Hauptregisterkarte der Support-Automatisierung oder einem Ticket.

Support-Automatisierung-Administrator

Konfiguriert die Support-Automatisierung-Umgebung für Analysten und Endbenutzer. Der Service Provider legt Ihren Mandantenzugriff fest und ermöglicht Ihnen, eine Mandanten-Dropdown-Liste auf Listen- und Detailformularen anzuzeigen. Mit diesen Formularen können Sie bestimmte Mandanten oder öffentliche Daten bei der Suche, Erstellung und Änderung von Support-Automatisierung-Daten in einer Umgebung für mehrere Mandanten auswählen.

Hinweis: Objekte wie Warteschlangen, Privatsphären-Ebenen und Chat-Voreinstellungen sind mandantenoptional.

Auswirkung auf Knowledge Management

Die Auswirkung von Mandantenfähigkeit auf Ihre Knowledge-Umgebung hängt von den Mandanteneinschränkungen ab, die an Benutzer vergeben werden:

Mandantenbenutzer

Ersetzt das Logo des Mandanten gegen den Standard, wenn die Rolle auf einen einzigen Mandanten beschränkt wird.

Mandantenadministratoren

Ermöglicht Administratoren, sowohl öffentliche als auch mandantenspezifische Daten anzuzeigen. Listenseiten für diese Objekte enthalten automatisch eine Spalte "Öffentlich", die angibt, ob die Listenzeile öffentlich ist oder nicht.

Wenn Sie nach Wissen suchen, enthält der Filter eine Dropdown-Liste "Öffentliche Daten" mit den Auswahlmöglichkeiten "Einschließen" (Standard), "Ausschließen" und "Nur".

Hinweis: Objekte wie Genehmigungsvorgangsvorlagen, Kategorien, Dokumente, Dateien und Foren sind mandantenoptional.

Knowledge-Kategorien und Dokumente

Knowledge-Dokumente und Knowledge-Kategorien sind beide vom Typ "Mandant optional". Beachten Sie die folgende Informationen für öffentliche Objekte und für Objekte vom Typ "Mandant optional":

- Öffentliche Knowledge-Dokumente können ausschließlich öffentlichen Knowledge-Kategorien hinzugefügt werden.
- Öffentliche Knowledge-Kategorien können ausschließlich öffentlichen Kategorien hinzugefügt werden.

- Mandantenkategorien können öffentlichen Kategorien und den Kategorien eines Mandanten hinzugefügt werden.
- Nur Mandantendokumente können Mandantenkategorien hinzugefügt werden.
- Öffentliche Dokumente und Mandantendokumente können öffentlichen Kategorien hinzugefügt werden.

Hinweis: Die Funktionalität "Kategorie ausschneiden/kopieren/einfügen" ist nur dann zulässig, wenn die Quelle und das Ziel den gleichen Mandanten haben oder wenn der Bestimmungsort öffentlich ist.

Respositorys werden als "Mandant optional" gekennzeichnet, so dass der Administrator unterschiedliche Respositorys für unterschiedliche Mandanten erstellen kann.

Eingebettete Bilder sind nur zulässig, wenn das Dokument und das Bild demselben Mandanten zugeordnet sind. Anhangsordner, Anhänge und Anhänge an Dokumentverknüpfungen sind ebenso als "Mandant optional" definiert.

FAQ-Einstufung

Wenn man die FAQ-Bewertung für Mandantenbenutzer ansieht, beachten Sie die folgende Informationen zu öffentlichen Dokumenten:

- Öffentliche Dokumente werden von einer größeren Zielgruppe angesehen – nicht nur von Mandantenbenutzern.
Die FAQ-Bewertung von öffentlichen Dokumenten ist höher als die eines bestimmten Mandantendokuments.
- Jeder Mandant hat verschiedene Anforderungen, weshalb sind Verwendungsmuster zwischen Mandanten unterschiedlich sind.

Die "Besten Lösungen" auf den CA SDM-Self-Service-Startseiten zeigen die relevantesten fünf öffentlichen Dokumente, sowie die relevantesten fünf Dokumente des Mandanten an.

Sie können die "Besten Lösungen" konfigurieren, indem Sie zu Knowledge, Lösungsumfrage und FAQ-Einstellungen auf der Registerkarte "Administration" navigieren.

Knowledge-Berichtskarte

Die Knowledge-Berichtskarte erlaubt es Analysten und Administratoren, verschiedene Indikatoren, wie Dokumentenerstellung, Veröffentlichung, Treffer und Abstimmungen anzuzeigen. Dieser Bericht gilt für einen vorbestimmten Zeitraum, pro Analyst, Kategorie und Organisation.

Wenn Sie die Knowledge-Berichtskarte verwenden, um Informationen für eine Rolle mit individuellem Mandantenzugriff verfügbar zu machen, werden die Daten von den Mandantenkriterien beschränkt.

Verwenden von Multi-Tenancy

Wenden Sie das folgende Verfahren an, um CA SDM-Mandantenfähigkeitsmerkmale zu verwalten.

Anzeigen von Mandanten

Sie können Mandanten aus jeder beliebigen Mandantenliste anzeigen.

Hinweis: Diese Funktion ist nur verfügbar, wenn Mandantenfähigkeit installiert wird (im Aktiviert- oder Setup-Modus).

So zeigen Sie einen Mandanten an:

1. Wählen Sie auf der Registerkarte "Administration" die Option "Sicherheits- und Rollenmanagement" aus.
2. Klicken Sie auf "Mandanten".

Die Mandantenliste wird angezeigt.

3. (Optional) Wählen Sie einen Mandanten aus der Mandantenliste aus.

Die Seite "Mandant - Detail" wird angezeigt.

Hinweis: Mandantenlisten werden auch auf Seiten wie "Mandantengruppe - Detail" und "Von CI betroffene Mandanten" angezeigt.

Erstellen eines Mandanten

Sie können das Produkt verwenden, um einen Mandanten zu erstellen.

So erstellen Sie einen Mandanten:

1. Wählen Sie auf der Registerkarte "Administration" die Option "Sicherheits- und Rollenmanagement" > "Mandanten" aus.

Die Seite "Mandanten - Liste" wird angezeigt.

Hinweis: Die Option "Sicherheit und Rollenmanagement" > "Mandanten" ist nur verfügbar, wenn Mandantenfähigkeit installiert ist (aktiviert oder Setup).

2. Klicken Sie auf "Neu erstellen".

Die Seite "Neuer Mandant" wird angezeigt.

3. Füllen Sie die bearbeitbaren Felder aus, wenn erforderlich:

Name

Zeigt den Namen des Mandanten an.

Service Provider

Gibt an, ob der Mandant ein Service Provider ist. Der erste erstellte Mandant ist immer der Service Provider.

Mandantennummer

(Nur zur Information) Zeigt die Mandantennummer an. Dieses Feld ist wird nicht von CA SDM verwendet.

Datensatzstatus

Setzt den Mandanten auf "Aktiv" oder "Inaktiv".

Übergeordneter Mandant

Gibt einen Mandanten an, der diesem Mandanten übergeordnet ist. Dadurch wird dieser Mandant in einer Mandantenhierarchie zum *untergeordneten Mandanten*.

Untergeordnete Mandanten zulässig

Lässt zu, dass dieser Mandant untergeordnete Mandanten hat. Der Mandant kann die Einstellungen nicht ändern.

Mandantentiefe

(Nur zur Information) Gibt die Mandantentiefe dieses Mandanten an.

Übergeordnete Mandantengruppe

(Nur zur Information) Gibt die vom System verwaltete Mandantengruppe an, die diesen Mandanten und alle übergeordneten Mandanten der Mandantenhierarchie enthält.

Untergeordnete Mandantengruppe

(Nur zur Information) Gibt die vom System verwaltete Mandantengruppe an, die diesen Mandanten und alle untergeordneten Mandanten der Mandantenhierarchie enthält.

Fremde Schlüsselgruppe

(Nur zur Information) Gibt die vom System verwaltete Mandantengruppe an, die Mandanten enthält, die von SREL in Daten referenziert werden kann, die zu diesem Mandanten gehören. Die fremde Schlüsselgruppe ist die gleiche wie die übergeordnete Mandantengruppe.

Verwandte Mandantengruppe

(Nur zur Information) Gibt die vom System verwaltete Mandantengruppe an, die aus der übergeordneten und der untergeordneten Gruppe für diesen Mandanten besteht.

Nutzungsbedingungen

Legt die Nutzungsbedingungen für den Mandanten fest.

Logo

Gibt den URL für die Logodatei des Mandanten an. Bei der Datei kann es sich um jede Art von Bilddatei für das Internet handeln.

Standort

Zeigt die Seite zur Suche von Lokationen an.

Kontakt

Zeigt die Seite zur Suche von Kontakten an.

Hinweis: Wenn kein Kontakt mit dem jeweiligen Mandanten verknüpft ist, dann sind die Felder "E-Mail-Adresse" und "Pager-E-Mail-Adresse" inaktiv.

4. Klicken Sie auf "Speichern".

Der Mandant wurde erstellt.

5. Schließen Sie das Fenster.

6. Klicken Sie mit der rechten Maustaste auf die Mandantenliste und anschließend auf "Aktualisieren".

Die Mandantenliste wird aktualisiert und zeigt den erstellten Mandanten an.

7. (Optional) Um diesen Mandanten einer anwenderspezifischen Mandantengruppe zuzuweisen, klicken Sie auf der Registerkarte "Mandantengruppen" auf "Mandantengruppen aktualisieren".

Bearbeiten eines Mandanten

Sie können von der Registerkarte "Administration" aus einen Mandanten bearbeiten.

Hinweis: Diese Funktion ist nur verfügbar, wenn Mandantenfähigkeit installiert wird (im Aktiviert- oder Setup-Modus).

So bearbeiten Sie einen Mandanten:

1. Wählen Sie auf der Registerkarte "Administration" die Option "Sicherheits- und Rollenmanagement" aus.

2. Klicken Sie auf "Mandanten".

Die Mandantenliste wird angezeigt.

3. Klicken Sie mit der rechten Maustaste auf einen Mandanten, und klicken Sie auf "Bearbeiten".

Die Seite "Mandanten aktualisieren" wird angezeigt.

Hinweis: Wenn Sie einen existierenden Mandanten bearbeiten, werden die Registerkarten "Untergeordnete Mandanten" und "Configuration Items" angezeigt.

4. Nehmen Sie die gewünschten Änderungen vor, und klicken Sie auf "Speichern".
5. Schließen Sie die Seite "Mandanten aktualisieren".
Die Mandantenliste wird angezeigt.
6. Klicken Sie mit der rechten Maustaste, und wählen Sie die Option "Aktualisieren".
Die aktualisierte Liste der Mandanten wird angezeigt.

Mandantenhierarchien

Eine *Mandantenhierarchie* ist eine strukturierte Mandantengruppe, die vom System erstellt oder geändert wird, wenn ein *übergeordneter Mandant* einem Mandanten zugewiesen wird. Der Mandant wird zu einem *untergeordneten Mandanten* des übergeordneten und ggf. höheren Mandanten innerhalb dieser Hierarchie.

Hinweis: Der Service Provider kann mehrere nicht verwandte Hierarchien erstellen oder gar keine. Auch in einem System mit Mandantenhierarchien können Sie eigenständige Mandanten definieren.

Ein untergeordneter Mandant repräsentiert normalerweise eine Unterabteilung innerhalb seiner *übergeordneten Mandanten*. Ein untergeordneter Mandant kann eigene Geschäftsregeln und -daten haben. Daten übergeordneter Mandanten werden automatisch an den untergeordneten Mandanten übertragen, auf die dieser nur Schreibzugriff hat.

CA SDM unterstützt eine Mandantenhierarchie von unbegrenzter Tiefe. Allerdings kann der *Service Provider* die Gesamtzahl von Mandanten begrenzen und die Tiefe von Mandantenhierarchien festlegen (standardmäßig vier Stufen). Der Service Provider entscheidet auch, ob einzelne Mandanten untergeordnete Mandanten haben können.

Hinweis: Der Service Provider kann Teil von Mandantenhierarchien sein, dies ist jedoch nicht erforderlich. Der Service Provider kann keinen übergeordneten Mandanten haben.

Erstellen von untergeordneten Mandanten

Untergeordnete Mandanten ermöglichen Ihnen die Erstellung und Änderung von Mandantenstrukturen zu organisatorischen Zwecken und zur gemeinsamen Datenverwendung. Um einen Mandanten in eine Mandantenstruktur aufzunehmen, weisen Sie ihm einen übergeordneten Mandanten zu.

So erstellen Sie einen untergeordneten Mandanten:

1. Wählen Sie auf der Registerkarte "Administration" die Option "Sicherheits- und Rollenmanagement" > "Mandanten" aus.

Die Mandantenliste wird angezeigt.

Hinweis: Die Option "Sicherheits- und Rollenmanagement > "Mandanten" ist nur bei aktivierter Option für mehrere Mandanten verfügbar.

2. Klicken Sie auf einen vorhandenen Mandanten, um ihn zu bearbeiten, oder klicken Sie auf "Neu erstellen".

Die Seite "Mandant - Detail" wird angezeigt. Geben Sie die erforderlichen Daten oder Änderungen ein.

3. Wählen Sie einen übergeordneten Mandanten aus.

Hinweis: Die Dropdownliste "Übergeordneter Mandant" zeigt nur Mandanten an, für die untergeordnete Mandanten zulässig sind.

4. Klicken Sie auf "Speichern".

Der Mandant ist ein untergeordneter Mandant des übergeordneten Mandanten.

Hinweis: Wenn ein Mandant ein untergeordneter Mandant ist, gehört er sowie seine untergeordneten Mandanten (sofern vorhanden) zur untergeordneten Mandantengruppe des übergeordneten Mandanten. Der übergeordnete Mandant sowie dessen übergeordnete Mandanten (sofern vorhanden) gehören zur übergeordneten Mandantengruppe des untergeordneten Mandanten. All diese Mandanten gehören jeweils zur verwandten Mandantengruppe jedes dieser Mandanten.

Systemverwaltete Mandantengruppen

CA SDM erstellt und verwaltet automatisch drei Mandantengruppen für jeden Mandanten in einer Mandantenhierarchie (*Mandant* ist der Name in einer Mandantenhierarchie):

- "*tenant_subtenants*" (Mandanten, deren untergeordnete Objekte sowie deren untergeordnete Mandanten)
- "*tenant_supertenants*" (Mandant, dessen übergeordneter Mandant und dessen übergeordnete Mandanten)
- "*tenant_relatedtenants*" (die gesamte einzelne Hierarchie)

Systemverwaltete Mandantengruppen können wie benutzerdefinierte Mandantengruppen verwendet werden. Allerdings können nur ihre Namen und Beschreibungen verändert werden.

Anzeigen der Mandantengruppen

Sie können Informationen zu Mandantengruppen anzeigen, um Gruppenmitglieder zu zeigen.

Hinweis: Diese Funktion ist nur verfügbar, wenn Mandantenfähigkeit installiert wird (im Aktiviert- oder Setup-Modus).

So zeigen Sie die Liste der Mandantengruppe an:

1. Wählen Sie auf der Registerkarte "Administration" die Option "Sicherheits- und Rollenmanagement" aus.

2. Klicken Sie auf "Mandantengruppe".
Die Liste der Mandantengruppen wird angezeigt.
Hinweis: Sie können systemverwaltete Mandantengruppen ein- oder ausblenden.
3. (Optional) Wählen Sie eine Mandantengruppe aus der Liste aus.
Die Mandantengruppeninformationen werden angezeigt.
4. Ändern Sie die Mandantengruppe im Bedarfsfall.

Erstellen einer Mandantengruppe

Sie können das Produkt verwenden, um eine Mandantengruppe zu erstellen.

So erstellen Sie eine Mandantengruppe:

1. Wählen Sie auf der Registerkarte "Administration" die Option "Sicherheits- und Rollenmanagement" aus.
2. Klicken Sie auf "Mandantengruppe".
Die Liste der Mandantengruppen wird angezeigt.
Hinweis: Die Option "Sicherheits- und Rollenmanagement" > "Mandantengruppen" ist nur verfügbar, wenn Mandantenfähigkeit installiert ist (aktiviert oder eingerichtet).
3. Klicken Sie auf "Neu erstellen".
Die Seite "Neue Mandantengruppe erstellen" wird angezeigt.
4. Füllen Sie die folgenden Felder aus:
Name der Mandantengruppe
Zeigt den Namen der ausgewählten Gruppe an.
Datensatzstatus
Legt die Mandantengruppe als "Aktiv" oder "Inaktiv" fest.
Beschreibung
Zeigt eine Beschreibung der Mandantengruppe an.
5. Klicken Sie auf "Speichern".
Die Mandantengruppe wird erstellt.
6. Schließen Sie das Fenster.
Die Liste der Mandantengruppen wird angezeigt.

7. Klicken Sie mit der rechten Maustaste auf die Mandantenliste und anschließend auf "Aktualisieren".

Die Liste der Mandantengruppe wird aktualisiert.

8. Klicken Sie auf der Seite "Mandantengruppe - Detail" auf "Mandanten aktualisieren", um der Gruppe Mandantenmitglieder hinzuzufügen.

Bearbeiten von Mandantengruppen

Sie können eine Mandantengruppe bearbeiten, um ihre Mitglieder und Detailinformationen zu verwalten.

Hinweis: Diese Funktion ist nur verfügbar, wenn Mandantenfähigkeit installiert wird (im Aktiviert- oder Setup-Modus).

So bearbeiten Sie eine Mandantengruppe:

1. Wählen Sie auf der Registerkarte "Administration" die Option "Sicherheits- und Rollenmanagement" aus.
2. Klicken Sie auf "Mandantengruppe".
Die Liste der Mandantengruppen wird angezeigt.
3. Klicken Sie mit der rechten Maustaste auf eine Mandantengruppe, und klicken Sie auf "Bearbeiten".
Die Seite "Mandantengruppe aktualisieren" wird angezeigt.
4. Nehmen Sie die gewünschten Änderungen vor, und klicken Sie auf "Speichern".
5. Schließen Sie das Fenster.
Die Liste der Mandantengruppen wird angezeigt.
6. Klicken Sie mit der rechten Maustaste in das Protokollfenster, und wählen Sie "Aktualisieren" aus.

Die aktualisierte Liste der Mandantengruppen wird angezeigt.

Mandantendatenzuweisungen

CA SDM zeigt den Mandanten im gleichen Format sowohl in der Version "Ansicht" als auch in der Version "Bearbeiten" einer Detailseite für ein vorhandenes Objekt, da der Mandant für ein bestehendes Objekt nicht von der Web-Schnittstelle aus geändert werden kann.

Wenn Sie ein Objekt mit Mandanten bearbeiten, werden Dropdown-Listen auf der Bearbeitungsseite automatisch auf Werte beschränkt, die öffentlich sind und deren Eigentümer der gleiche Mandant wie der des Grundobjekts sind oder beliebige Mandanten darüber in der Mandantenhierarchie oder aber deren Eigentümer der Service Provider ist (falls die Dropdown-Liste für ein SERVICE_PROVIDER_ELIGIBLE-Attribut gilt).

Es gibt keine Änderungen auf der Detailseite für Suchfelder, die einem Objekt mit Mandant zugeordnet sind. Wenn ein Benutzer mit Zugriff auf mehrere Mandanten auf eine Suchverknüpfung zu einer Mandantentabelle klickt, beschränkt die Web-Engine die Suche automatisch auf für das Attribut geeignete Werte und zeigt auf dem Popup-Suchformular oder der Listenseite eine Bannermeldung an.

Hinweis: Mandantenbeschränkungen werden nicht im Suchfilter angezeigt, und sie können nicht vom Benutzer verändert werden.

Mandant wird zur Auswahl (entweder ein Suchfeld oder eine Dropdown-Liste), wenn Sie die Erstellung eines Objekts erforderlicher Mandanten anfordern.

Wenn das Feld "Mandant" leer ist, können Sie einen Mandantenwert direkt durch Eintragen in das Feld angeben oder indirekt durch Angabe eines Wert für ein Mandanten implizierendes Attribut (wie Betroffener Endbenutzer) angeben. Die Schnittstelle zeigt die folgenden Suffixe an:

(T)

Gibt ein Attribut an, das Mandanten implizierend ist; das ein Suchfeld in einer Tabelle erforderlicher Mandanten ist.

(TO)

Gibt ein Attribut an, das optional Mandanten impliziert ist, also, ein Suchfeld in einer Tabelle erforderlicher Mandanten.

web.cfg-Eigenschaften steuern den Text dieser Indikatoren.

Außer dem Mandantenattribut selbst werden Mandanten implizierende Attribute immer als Suchfelder angezeigt, selbst wenn Sie mit einem dtlDropdown-Makro erstellt wurden.

CA SDM legt automatisch den Mandanten fest, wenn Sie einen Mandantenwert suchen oder in ein beliebiges Mandanten implizierendes Feld automatisch einfügen (mit der Ausnahme, dass durch die Eingabe eines Verweises auf Service Provider-Objekt in ein SERVICE_PROVIDER_ELIGIBLE-Feld der Mandant nicht gesetzt wird. Nachdem der Mandant festgelegt wurde, sind Suchen nach Mandanten implizierenden Feldern auf die gleiche Weise beschränkt wie Suchen nach vorhandenen Mandantenobjekten.

Hinweis: Bis Sie das Objekt speichern, bleibt das Mandantenfeld bearbeitbar, und Sie können den Mandanten durch direktes Aktualisieren ändern. Wenn Sie den Mandanten ändern, löscht CA SDM automatisch alle Mandanten implizierende Felder, die Verweise auf Objekte enthalten, welche zum vorherigen Mandanten gehören.

CA SDM initialisiert die Mandantenauswahl normalerweise als leer. Sie können dieses Verhalten auf verschiedene Art und Weise verändern:

- Durch Öffnen der Seite "Neu erstellen" auf einer Seite wie z. B. "Ad-hoc-Profil", das ein Mandanten implizierendes Feld im Vorfeld ausfüllt
- Durch Festlegen der Benutzervoreinstellung "Mandant beibehalten"
Dies ist eine neue Benutzervoreinstellung, die den Mandanten für neue Objekte auf denselben Mandanten wie die zuletzt angezeigte oder aktualisierte Seite initialisiert oder in der Suchfilterbeschränkung der letzten Listenseite.
- Durch Öffnen der Seite mit einer URL, die explizit einen Mandanten angibt
Dies wird in einer vordefinierten URL nicht angegeben, ist aber verfügbar, damit Standorte Menüelemente oder Schaltflächen erstellen können, die einen Mandanten spezifizieren.

Hinweis: Wenn Sie Configuration Items aus einem anderen CA Technologies-Produkt (z. B. CA APM) oder aus der Befehlszeilenschnittstelle erstellen, ist das Objekt öffentlich.

Weitere Informationen:

[Erstellen eines Mandantenobjekts](#) (siehe Seite 152)

Erstellen eines Mandantenobjekts

Der Dienstleister kann mandantenspezifische Daten zu Objekten, wie Issues, Anfragen, Changes usw., hinzufügen. Sie können einen Mandanten zu einem Ticket (z. B. Incident) hinzufügen, das von einer Scoreboard-Registerkarte erstellt wurde.

So fügen Sie Mandantendaten einem Incident hinzu:

1. Klicken Sie auf "Datei" > "Neuer Incident".
2. Führen Sie die folgenden Schritte durch:
 - a. Wählen Sie den Mandanten aus der Dropdown-Liste für Mandanten aus.
 - b. Klicken Sie auf "Betroffener Endbenutzer" (oder auf irgendein anderes Feld, das den Mandanten einbezieht).
Die Seite "Kontakt – Suche" wird angezeigt. Suchen Sie nach einem Benutzer. Sie können die Suche nach Mandant filtern.
 - c. Geben Sie einen Namen in das Feld "Betroffener Endbenutzer" ein.
Die Mandantendaten werden automatisch ausgefüllt.
3. Fahren Sie mit dem Erstellen des Incidents fort.

Aktivitätsbenachrichtigungen

Aktivitätsbenachrichtigungen steuern sowohl den Inhalt von Benachrichtigungen als auch die Kontakte, die Benachrichtigungen für verschiedene Ereignisse in der Geschichte eines Tickets erhalten.

In einer Umgebung für mehrere Mandanten ist die Benachrichtigungsregel ein mandantenoptionales Objekt. Öffentliche Benachrichtigungsregeln gelten für alle Tickets; Mandantenregeln gelten nur für Tickets mit dem gleichen Mandanten als Regel oder für Mandanten mit ihrer untergeordneten Mandantenhierarchie. Die Mandantenbeschränkung wird zusätzlich zu Bedingungen angewandt, die mit der Regel selbst angegeben werden.

Weitere Informationen:

[Kopien von Benachrichtigungsregeln](#) (siehe Seite 153)

Kopien von Benachrichtigungsregeln

Standardbenachrichtigungsregeln werden als öffentliche Objekte gespeichert. Wenn Mandantenfähigkeit installiert wird, müssen Sie eine Kopie der Benachrichtigungsregel für jeden der Mandanten erstellen. Andernfalls ist die Option "Kontakte aktualisieren" gesperrt.

So kopieren Sie eine Benachrichtigungsregel:

1. Navigieren Sie zu "Benachrichtigungen" > "Benachrichtigungsregeln" auf der Registerkarte "Administration".

Es wird die Liste der Benachrichtigungsregeln angezeigt.

2. Klicken Sie in der Spalte "Symbol" auf eine Regel.

Die Seite "Benachrichtigungsregeln - Detail" wird angezeigt.

3. Klicken Sie auf "Datei" > "Kopieren".

Fahren Sie mit der Aktualisierung der Benachrichtigungsregel fort.

Repositorys

Das Repository-Objekt (doc_rep) ist mandantenoptional. Mandanten können ihre eigenen Repositorys definieren, und es ist möglich, öffentliche Repositorys für Objekte wie Anhänge von öffentlichen Knowledge-Dokumenten zu definieren. Jeder Mandant kann über sein eigenes Standard-Repository verfügen; außerdem können Sie ein öffentliches Standard-Repository angeben.

Alle Anhänge sind entweder öffentlich oder einem einzigen Mandanten zugeordnet. Wenn ein Mandant kein eigenes Standard-Repository hat, wird das öffentliche Repository als Standard für seine Objekte mit Mandanten angezeigt.

Kapitel 6: Integrieren mehrerer Suchmaschinen mithilfe von föderierter Suche

Die föderierte Suchfunktion erweitert die Funktionen der CA SDM-integrierten Knowledge Base.

- Wenn ein Anwender eine Knowledge-Suche ausführt, dann werden die Ergebnisse aus der internen Knowledge-Datenbank durch Ergebnisse aus externen Suchmaschinen ergänzt. Wir stellen eine standardmäßige Suchadapterkonfiguration für CA Open Space, Microsoft SharePoint und Google bereit.
- Die Architektur "Föderierte Suche" ist flexibel. Die Unterstützung von anderen Suchmaschinen kann hinzugefügt werden, indem ein anwenderspezifischer Suchadapter mithilfe von "CA Federated Search SDK" entwickelt wird. Die SDK-Schnittstelle enthält Informationen und Quellcodebeispiele für die Erweiterbarkeit der föderierten Suche.
- Informationen, die in den CA SDM-Tickets und in den KB-Artikeln enthalten sind, können auch mit einer externen Suchmaschine gesucht werden. Die neue Komponente der Crawler-Oberfläche ermöglicht es einem externen Suchmaschinen-Crawler, die CA SDM-Informationen einfach zu finden. Der Crawler speichert diese Informationen im Repository. Diese indizierten Informationen können mithilfe von "Föderierte Suche" gesucht werden. Anhänge für Tickets und KB-Artikel werden auch unterstützt.

Hauptkomponenten der Funktion für föderierte Suche sind:

- Föderierte Suche konfigurieren
- Crawler konfigurieren
- Anwenderspezifischer Suchadapter von SDK

Föderierte Suche konfigurieren

Die Funktion "Föderierte Suche" besteht aus folgenden Komponenten:

UI-Komponenten

Ermöglicht es CA SDM-Analyst-Anwendern, Suchargumente einzugeben und die Suchanfrage an den Server der föderierten Suche zu übergeben.

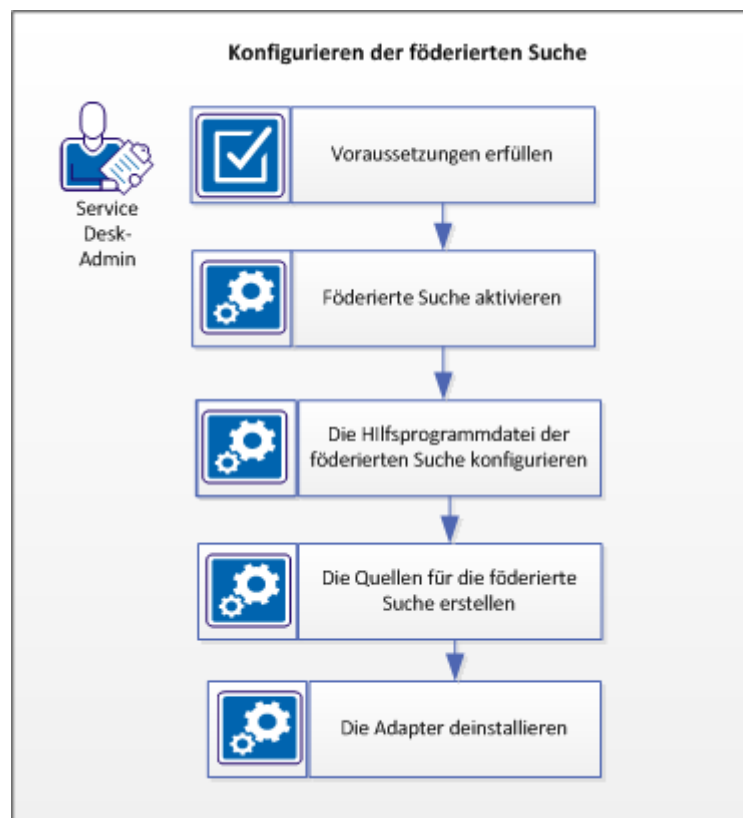
CAFedSearch-Servlet

Hauptkomponente der föderierten Suchfunktion, und es wird eine REST-Schnittstelle verwendet. Das Servlet "Föderierte Suche" wird auf einer dedizierten Tomcat-Instanz innerhalb der CA SDM-Anwendung ausgeführt.

Plug-in-Suchadapter

Der Plug-in-Suchadapter bildet eine Schnittstelle der CA SDM-Anwendung zu einer externen Suchmaschine. Der Adapter übersetzt die generischen Suchanfragen in ein proprietäres Format der Suchmaschine, und die Suchmaschine wird aufgerufen. Das Servlet für föderierte Suche gibt die konfigurierten Suchmaschinenergebnisse an die UI-Komponente von CA SDM zurück.

Folgendes Diagramm zeigt an, wie die föderierte Suche mit der CA SDM-Anwendung konfiguriert wird:



Gehen Sie wie folgt vor:

1. [Erfüllen der Voraussetzungen](#) (siehe Seite 157)
2. [Aktivieren Sie die föderierte Suche](#) (siehe Seite 158)
3. [Konfigurieren Sie die Hilfsprogrammdatei der föderierten Suche](#) (siehe Seite 159)
4. [Erstellen der Quellen der föderierten Suche in CA SDM](#) (siehe Seite 166)

Erfüllen der Voraussetzungen

Folgende Voraussetzungen müssen erfüllt werden:

- Stellen Sie sicher, dass Sie während der Installation der CA SDM-Anwendung die Option "Föderierte Suche" im Assistenten "Föderierte Suche konfigurieren" auswählen.
- Sie sollten die Suchmaschinen kennen, die Sie für die föderierte Suche verwenden möchten.
- Stellen Sie sicher, dass Sie ein aktives Google-Konto für das Konfigurieren des Google-Plug-In-Suchadapters haben. Ein Google API-Schlüssel und eine anwenderspezifische Suchmaschinen-ID von Google sind auch erforderlich. Weitere Informationen finden Sie in der anwenderspezifischen Suche von Google unter <https://www.google.com/cse/all>
- Stellen Sie sicher, dass IIS auf dem SharePoint-Server mit der Basisauthentifizierung konfiguriert ist. Der Microsoft SharePoint-Adapter benötigt Basisauthentifizierung. Standardmäßig ist Basisauthentifizierung in SharePoint deaktiviert. Weitere Informationen dazu, wie Sie die Basisauthentifizierung in SharePoint aktivieren, finden Sie in der Microsoft SharePoint-Dokumentation.
Hinweis: Aktivieren Sie Basisauthentifizierung für "_vti_bin" in IIS.
- Für die Integration mit CA Open Space ist Version 2.0 SP1-On-Premise-Lösung erforderlich. Weitere Informationen finden Sie in der CA Open Space-Dokumentation. Das CA Open Space SaaS-Angebot wird derzeit nicht unterstützt.

Aktivieren Sie die föderierte Suche

Eine dedizierte Tomcat-Instanz ist installiert, um die Servlets "CAFedSearch" und "FSCrawl" zu hosten. Die föderierte Suche von Tomcat wird über den Daemon-Manager gesteuert. Tomcat wird automatisch gestartet und angehalten, wenn CA SDM ausgeführt bzw. heruntergefahren wird.

Konfigurieren Sie Tomcat für föderierte Suche (FS) mit den folgenden Installationsoptionen:

Föderierte Suche konfigurieren

Stellen Sie sicher, dass diese Option ausgewählt ist, wenn Sie die CA SDM-Anwendung installieren. Die Tomcat-Optionen sind erst verfügbar, nachdem Sie diese Option ausgewählt haben.

Tomcat-Port

Gibt den Tomcat-Port für föderierte Suche an. Standardport= 8040.

Tomcat-Endpoint

Gibt den Endpoint für das Servlet "Föderierte Suche" an. Standardport= 8045.

Generieren der XML-Dateien der Konfiguration für föderierte Suche

Um die föderierte Suche zu konfigurieren und um Bearbeitungsfehler zu verringern, wird die Hilfsprogrammdatei "fs_adapters_cli" zur Verfügung gestellt. Es wird eine Batch-Datei für Windows und ein Shell-Skript für Linux und Unix bereitgestellt. Die Hilfsprogrammdatei ist eine Java-Anwendung, die in zwei jar-Dateien enthalten ist.

Drei Vorlagendateien werden für CA Open Space-, Google- und SharePoint-Adapter bereitgestellt. Die Datei "adapters-config.xml" wird sowohl für die Eingabe als auch für die Ausgabe zum Hilfsprogramm verwendet. Die Datei "adapters.properties" wird als Eingabe zum Hilfsprogramm verwendet. Diese Datei enthält alle notwendigen Konfigurationsparameter für die Adapter. Die Datei "jfedsearch.log" enthält die Informationen der Protokolldatei.

Das "fs_adapters_cli"-Hilfsprogramm wird verwendet, um die Datei "adapters-config.xml" zu konfigurieren. Die Hilfsprogrammdatei installiert und deinstalliert die Adapter, indem Eingaben aus der Datei "adapters-config.xml" hinzugefügt oder entfernt werden. Individuelle XML-Konfigurationsdateien des Adapters werden generiert. Diese Dateien werden dann in die Datei "adapters-config.xml" mit der `<import>`-Bean-Direktive eingeschlossen. Stellen Sie sicher, dass Sie über eine saubere Kopie der Datei "adapters-config.xml" verfügen.

- Um einen Adapter zu installieren, werden zwei Eingaben für das Registrieren und Importieren des Adapters in der Datei "adapters-config.xml" hinzugefügt
- Um einen Adapter zu deinstallieren, werden zwei Eingaben für das Registrieren und Importieren des Adapters aus der Datei "adapters-config.xml" entfernt.

Weitere Informationen über das Verwenden der Hilfsprogrammdatei finden Sie unter Hilfsprogrammdateien der föderierten Suche und Abrufen der Hilfsprogrammdatei zur Konfiguration der Suchadapter.

Hilfsprogrammdateien der föderierten Suche

Die Hilfsprogrammdatei "fs_adapters_cli" befindet sich im CA SDM-Verzeichnis "\$NX_ROOT\samples\cafedsearch". Folgende Komponenten der Hilfsprogrammdatei sind in dieser Lokation verfügbar:

- Skriptdateien:
 - fs_adapters_cli.bat (für Windows)
 - fs_adapters_cli.sh (für Nicht-Windows)
- JAR-Dateien:
 - fs_adapters_config_cli.jar
 - fs_adapters_config_schema.jar
- Vorlagen:
 - openspace-tmpl.xml
 - google-tmpl.xml
 - sharepoint-tmpl.xml
- Eigenschaften:
 - adapters.properties

Um die Hilfsprogrammdatei der föderierten Suche zu installieren, führen Sie folgenden Befehl aus:

```
fs_adapters_cli -i -k <key> -b <bean> -t <filename> -p <filename> -o <filename> [-c <filename>]
```

Verwenden Sie die Option "fs_adapters_cli -h", um Hilfe für die Hilfsprogrammdatei zu erhalten. Folgende Attributoptionen stehen zur Verfügung:

-b (Optional)

Attributwert, um Adapter zuzuordnen. Bezieht sich auf eine tatsächliche ID einer Adapter-Bean. Wenn nicht angegeben, dann wird der Wert von -k für den Wert für -b gehalten.

-c (Optional)

Die Haupt-XML-Datei, die alle konfigurierten Adapter enthält.

-h (Optional)

Stellt Hilfe für das Hilfsprogramm der föderierten Suche bereit.

-i

Gibt die Option an, die für die Installation des Adapters verwendet wird.

-k

Gibt das Schlüsselattribut des Adapters an.

-o

Gibt den zu generierenden XML-Dateinamen der Ausgabe an. Name der XML-Datei, um den zusammengeführten Inhalt von der XML-Vorlage und der SharePoint-Eigenschaftsdatei zu erstellen und zu aktualisieren.

-p (Optional)

Gibt den Eigenschaftsdateinamen an, der mit der XML-Vorlage der Adapterdefinition zusammengeführt werden soll.

-t

Gibt den Namen der XML-Vorlagendatei für das Definieren eines Adapters an.

-u

Gibt den Namen der XML-Datei des Adapters an, um den Adapter zu deinstallieren.

Abrufen der Hilfsprogrammdatei zur Konfiguration der Suchadapter

Eine Suchmaschine benötigt speziell kodierte Plug-in-Adapter. Ein Plug-in-Suchadapter übersetzt generische Suchanfragen in ein proprietäres Format der Suchmaschine, die Suchmaschine wird aufgerufen, und die Suchanfragen werden zurückgegeben.

Hinweis: Wenn CA SDM für mehrere Mandanten konfiguriert ist, dann wird Ihr Mandant an die Suchmaschine übergeben. Die föderierte Suche verfügt über integrierte Unterstützung für mehrere Mandanten. Sie können dies verwenden, um Daten nach einem Mandanten in einer einzelnen SharePoint-Implementierung zu isolieren.

Wichtig! Verwenden Sie keine Ampersand-Zeichen (&) oder Leerzeichen in der Datei "adapters.properties".

Gehen Sie wie folgt vor:

1. Verschlüsseln Sie Kennwörter für Suchadapter mithilfe des Hilfsprogramms zum Verschlüssen von Kennwörtern. Um Kennwörter zu verschlüsseln, navigieren Sie in das folgende CA SDM-Verzeichnis:

`$NXROOT\bin`

2. Führen Sie folgenden Befehl aus, um verschlüsselte Kennwörter zu generieren:

`encrypt_pwd [-e] <search engine password>`

Die Standardoption ist -e.

3. Öffnen Sie die Datei "adapters.properties" im folgenden CA SDM-Verzeichnis:

`$NX_ROOT\samples\cafedsearch`

4. Bearbeiten Sie die Datei "adapters.properties". Geben Sie die entsprechenden Parameter für die Adapter an, die Sie konfigurieren möchten.
5. Aktualisieren Sie für SharePoint die folgenden Werte in der Datei "adapters.properties":

sharepoint_username=

Geben Sie den Anwendernamen für den SharePoint-Zugriff ein.

sharepoint_password=

Geben Sie das verschlüsselte Kennwort für den SharePoint-Zugriff, wie in Schritt 1 angezeigt, ein.

sharepoint_hostname=

Geben Sie den Hostnamen ein.

sharepoint_domainName=

Geben Sie den Domänennamen ein.

sharepoint_protocol=

Geben Sie das Kommunikationsprotokoll ein (http oder https)

sharepoint_portNumber=

Geben Sie die Portnummer ein. Standard ist 80.

6. Aktualisieren Sie für Google die folgenden Werte in der Datei "adapters.properties":

google_googleCx=

Geben Sie einen eindeutigen Schlüssel ein, den Google für die Auswahl des Google Custom Search Accounts verwendet.

google_googleApiKey=

Geben Sie den eindeutigen Schlüsselwert ein, der Google dabei hilft, die Identität einer Anwendung zu bestimmen. Um den Schlüssel in der API-Konsole abzurufen, aktivieren Sie die API der anwenderdefinierten Suche von JSON/Atom. Diese API gibt einen neuen API-Schlüssel für den einfachen API-Zugriff an.

7. Aktualisieren Sie für CA Open Space die folgenden Werte in der Datei "adapters.properties":

openspace_protocol=

Geben Sie das Kommunikationsprotokoll ein (http oder https)

openspace_portNumber=

Geben Sie die Portnummer für CA Open Space ein. Standard ist 8686.

openspace_default_tenant_userName=

Wenn CA SDM nicht mit mehreren Mandanten konfiguriert ist, geben Sie einen Anwendernamen ein, um die Suche in CA Open Space auszuführen.

openspace_default_tenant_password=

Geben Sie das CA Open Space-verschlüsselte Kennwort ein. Weitere Informationen finden Sie unter Step1.

openspace_default_tenant_companyHost=

Geben Sie die Hostdetails des Mandantenunternehmens ein.

- a. Fügen Sie im Fall von CA SDM-Mandantenfähigkeit eine Eingabe für jeden Mandanten in der Datei "openspace-tmpl.xml" hinzu:

Wenn CA SDM Mandantennamen wie z. B. "Mandant 1" enthält, müssen Sie folgende Werte in der Datei "openspace-tmpl.xml" angeben:

```
<entry key="Tenant1">
    <bean
class="com.ca.ServicePlus.cafedsearch.adapters.openspace.OpenSpaceCompanyDetail">
        <property name="userName"
value="$(openspace_tenant1_userName)"/>
        <property name="password"
value="$(openspace_tenant1_password)"/>
        <property name="companyHost"
value="$(openspace_tenant1_companyHost)"/>
    </bean>
</entry>
```

- b. Fügen Sie folgende Eingaben für "Mandant 1" in der Datei "adapters.properties" hinzu:

```
openspace_tenant1_userName=
openspace_tenant1_password=
openspace_tenant1_companyHost=
```

Wiederholen Sie die Schritte a und b für alle erforderlichen Mandanten in der Datei "openspace-tmpl.xml".

8. Rufen Sie "fs_adapters_cli" einmal für jeden Adapter auf, den Sie konfigurieren möchten.
- Wenn Sie einen CA Open Space-Adapter konfigurieren möchten, verwenden Sie den Bean-Wert als "OpenSpaceSearchAdapter" und die Vorlage als "openspace-tmpl.xml", wie im folgenden Beispiel angezeigt:

```
fs_adapters_cli -i -k OpenSpace -b OpenSpaceSearchAdapter -t "openspace-tmpl.xml" -o "openspace.xml"
```
 - Um einen Google-Adapter zu konfigurieren, stellen Sie den Bean-Wert als "GoogleSearchAdapter" und die Vorlage als "google-tmpl.xml" bereit, wie im folgenden Beispiel angezeigt:

```
fs_adapters_cli -i -k Google -b GoogleSearchAdapter -t "google-tmpl.xml" -o "google.xml"
```
 - Wenn Sie einen SharePoint-Adapter konfigurieren möchten, verwenden Sie den Bean-Wert als "SharePointSearchAdapter" und die Vorlage als "sharepoint-tmpl.xml", wie im folgenden Beispiel angezeigt:


```
fs_adapters_cli -i -k SharePoint -b SharePointSearchAdapter -t
"sharepoint-tmpl.xml" -o "sharepoint.xml"
```

Ändern Sie die Attributwerte "-k" und "-o" mit einem Namen Ihrer Wahl. Weitere Informationen zur Hilfsprogrammdatei für föderierte Suche und Attribute finden Sie unter Hilfsprogrammdateien der föderierten Suche.

9. Wenn nach der Installation Fehler vorhanden sind, überprüfen Sie die Protokolldatei im CA SDM-Verzeichnis:
\$NXROOT\log\jfedsearch.log
10. Optional können Sie auch Ihre eigene XML-Datei für die Registrierung erstellen. Alle Adaptereingaben sind in der Datei "adapters-config.xml" im folgenden Verzeichnis registriert:

```
$NX_ROOT\samples\cafedsearch
```

11. Um Ihre eigene XML-Datei für die Registrierung zu erstellen, können Sie auch eine Kopie aus dem vorhandenen Dateinamen "adapters-config.xml" erstellen (optionaler Schritt). Geben Sie der geänderten Datei "adapters-config.xml" einen Namen Ihrer Wahl. Zum Beispiel Datei "xyz.xml".

Verwenden Sie die Option "-c" mit der geänderten XML-Datei (xyz.xml), um Adapter zu registrieren.

12. Ändern Sie den Ressourcenwert in bean.xml <import resource="adapters-config.xml"/>.
13. Kopieren Sie "adapters-config.xml" oder die geänderte Datei "xyz.xml" (Schritt 11) und zugeordnete adapterspezifische XML-Dateien für Google (google.xml), CA Open Space (openspace.xml), SharePoint (sharepoint.xml) im folgenden CA SDM-Verzeichnis:

```
$NX_ROOT\bopcfg\www\CATALINA_BASE_FS\webapps\cafedsearch\WEB-INF
```

14. Starten Sie das Servlet "Tomcat für föderierte Suche" neu:

```
pdm_tomcat_nxd -c STOP -t FS
```

```
pdm_tomcat_nxd -c START -t FS
```

Die Adapter für föderierte Suche sind konfiguriert.

15. Überprüfen Sie die Fehlerprotokolldateien im CA SDM-Verzeichnis:

```
$NX_ROOT\log\jfedsearch.log
```

Erstellen der Quellen der föderierten Suche in CA SDM

Die CA SDM-Web-Benutzeroberfläche ist mit dem CAFedSearch-Servlet lose verbunden. Konfigurieren Sie Suchquellen in CA SDM, um einen neuen Datensatz zu erstellen.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei der CA SDM-Anwendung als Service Desk-Administrator an.
2. Wählen Sie Administration, Knowledge, Föderierte Suche, Suchquelle aus, um einen neuen Datensatz zu erstellen, der eine Maschine für föderierte Suche darstellt.

Die Suchquelle enthält den Namen der Quelle für föderierte Suche, die den Anwendern angezeigt wird.

Hinweis: Der Codewert muss mit dem Schlüsselwertattribut einer Eingabe in der Datei "adapters-config.xml" übereinstimmen.

Suchen der Knowledge-Lösung mithilfe des neuen anwenderspezifischen Suchadapters

Suchen Sie nach Knowledge-Dokumenten und Artikeln in der CA SDM-Anwendung, indem Sie den neuen anwenderspezifischen Suchadapter verwenden.

Gehen Sie wie folgt vor:

1. Melden Sie sich als Service Desk-Administrator von CA SDM an.
2. Navigieren Sie zu Administration, Knowledge, Föderierte Suche, Suchquellen.
3. Fügen Sie einen neuen Code-Schlüsselwert für die Suchquelle hinzu.
4. Klicken Sie auf "Speichern".
5. Navigieren Sie mithilfe eines neuen oder vorhandenen Tickets zu Knowledge Management.
6. Suchen Sie nach der Knowledge-Quelle, die Sie erstellt haben. Klicken Sie auf Filter anzeigen, um die Suchkriterien einzugeben, und klicken Sie auf Suchen.

Daraufhin werden Suchinformationen angezeigt.

Deinstallieren der Suchadapter

Um die Suchadapter zu deinstallieren, verwenden Sie den Hilfsprogrammbefehl "fs_search_cli" mit der Option "-u". Verwenden Sie den folgenden Dateibefehl des Hilfsprogramms:

```
fs_adapters_cli -u -k <key> -b <bean> [-c <filename>] -f <filename>]
```

-u

Geben Sie die Option "-u" an, um die Suchadapter zu deinstallieren.

-k

Geben Sie den Schlüsselnamenswert an, der bei der Installation angegeben wurde.

-b

Geben Sie den Bean-Wert an, der bei der Installation angegeben wurde.

-c

Geben Sie den Namen der neuen Konfigurations-XML des Suchadapters an, sofern Sie eine erstellt haben, während Sie die Suchadapter mit dem Hilfsprogramm konfigurieren.

-f

Gibt den generierten Ausgabedateinamen bei der Installation an.

Weitere Informationen finden Sie unter Konfigurieren von Suchadaptern unter Verwendung des Hilfsprogramms.

Wenn Sie zum Beispiel den Google-Suchadapter deinstallieren möchten, führen Sie Folgendes aus:

Gehen Sie wie folgt vor:

1. Führen Sie den Dateibefehl des Hilfsprogramms mit der Option "-u" für die Deinstallation des Google-Suchadapters aus:

```
fs_adapters_cli -u -k Google-b GoogleAdapter-f Google.xml
```

2. Stellen Sie sicher, dass "adapters-config.xml" die Registrierung für Google entfernt.
3. Die Datei "Google.xml" wird aus folgendem CA SDM-Verzeichnis gelöscht:

```
$NX_ROOT\samples\cafedsearch
```

4. Kopieren Sie "adapters-config.xml" in das folgende Verzeichnis:

```
$NX_ROOT\samples\cafedsearch\WEB-INF
```

Löschen Sie die Datei "google.xml" aus diesem Speicherort.

5. Starten Sie FS-Tomcat neu:

```
pdm_tomcat_nxd -c STOP -t FS
```

```
pdm_tomcat_nxd -c START -t FS
```

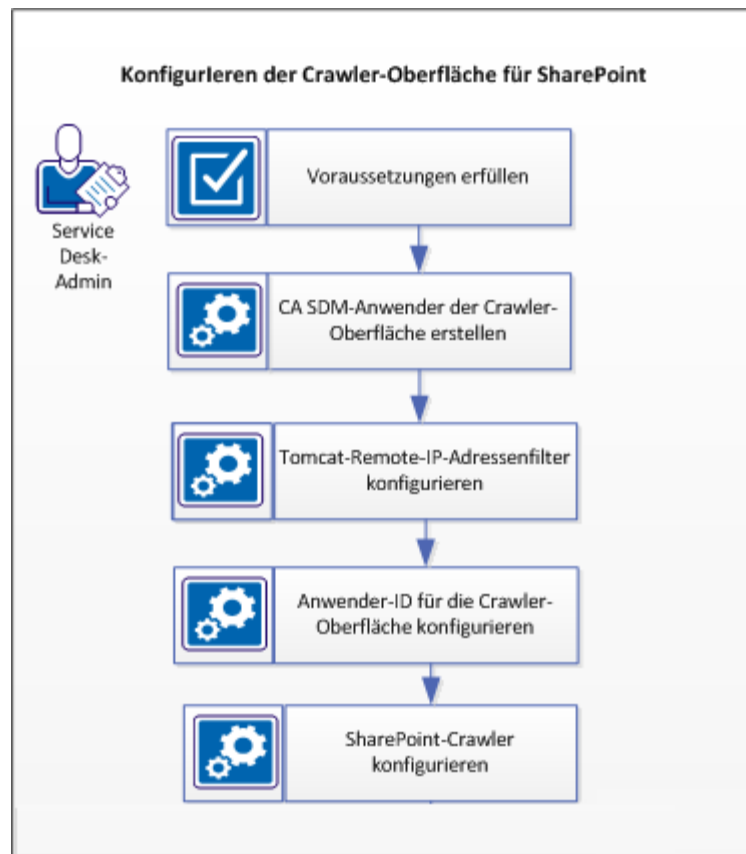
6. Überprüfen Sie auf der CA SDM-Benutzeroberfläche die Quelleneingabe "Activate Search" für diesen Adapter (in diesem Fall für Google).
7. Um andere externe Suchadapter zu deinstallieren, wiederholen Sie die Schritte 1 bis 6.

Konfigurieren der Crawlers-Oberfläche

Ein Crawler ist Teil einer Suchmaschine, die automatisch das Internet durchsucht, um Suchbegriffe zu indizieren. Die Crawler-Oberfläche ist eine neue schreibgeschützte webbasierte Schnittstelle für die CA Service Desk Manager-Anwendung. Externe Suchmaschinen können Informationen mithilfe von JSP-Technologie (Java Server Page) erkennen. Die Crawler-Oberfläche enthält Informationen im Nur-Text-Format und stellt auch individuelle Hyperlinks zu Tickets und Knowledge-Dokumenten bereit. Folgen Sie den Hyperlinks, um Informationsdetails zu erkennen. Microsoft SharePoint 2010 und SharePoint 2013 kann verwendet werden, um die Crawler-Oberfläche zu durchsuchen. Die Hauptkomponente der Crawler-Oberfläche ist das FSCrawl-Servlet.

Hinweis: Der CA Service Desk Manager-Informationsinhalt, der einem Crawler angezeigt wird, kann über eine Konfigurationsdatei angepasst werden. Es sind keine Formularänderungen erforderlich.

Folgendes Diagramm zeigt, wie die Crawler-Web-Oberfläche für SharePoint konfiguriert wird:



Gehen Sie wie folgt vor:

1. [Erfüllen der Voraussetzungen](#) (siehe Seite 170)
2. [Erstellen der Crawler-Oberfläche für den CA Service Desk Manager-Anwender](#) (siehe Seite 170)
3. [Konfigurieren des Tomcat Remote IP Address Filter](#) (siehe Seite 171)
4. [Konfigurieren der Anwender-ID für die Crawler-Oberfläche](#) (siehe Seite 173)
5. [Konfigurieren des SharePoint-Crawlers](#) (siehe Seite 180)

Erfüllen der Voraussetzungen

Erfüllen Sie folgende Voraussetzungen, bevor Sie mit der Konfiguration der Crawler-Oberfläche für einen Microsoft SharePoint-Server beginnen:

- Aktivieren Sie die Option "Föderierte Suche konfigurieren", während Sie die CA SDM-Anwendung installieren.
- Halten Sie eine dedizierte Anwender-ID bereit, um auf die Informationen der Suchergebnisse zuzugreifen. Die Anwender-ID steuert die Informationen, die auf der Crawler-Oberfläche vorhanden sind. Erstellen Sie für die Konfiguration der CA SDM-Mandantenfähigkeit zusätzliche Anwender-IDs, um die Trennung von Mandanteninformationen zu ermöglichen.

Erstellen der Crawler-Oberfläche für den CA SDM-Anwender

Erstellen Sie in der CA SDM-Konfiguration Anwenderidentitäten, um Informationen nach Mandanten zu trennen.

Der Prozess der Erstellung einer Anwender-ID für die Crawler-Oberfläche entspricht der Erstellung von CA SDM-Anwenderidentitäten für normale Anwender. Erstellen Sie einen Kontakt mit Zugriffstyp und Rolle als "Crawler" in der CA SDM-Anwendung. Weitere Informationen über das Erstellen eines Kontakts finden Sie in der Online-Hilfe für CA Service Desk Manager-Administratoren.

Der Zugriffstyp und die Rolle "Crawler" stellen einen schreibgeschützten Zugriff auf die CA SDM-Daten für den Anwender bereit.

Konfigurieren des Tomcat Remote IP Address Filter

Ändern Sie die Einstellung "Tomcat remote IP address filter", sodass diese auf das Remote-System hinweist, das den SharePoint-Server hostet. Die IPV4- und IPV6-Adressen werden unterstützt.

Die Crawler-Oberfläche verwendet den Mechanismus "Tomcat Remote IP Address Filter", um auf CA SDM-Informationen zuzugreifen. Der Tomcat-Filtermechanismus verwendet ein IP-Adressmuster (vom CA SDM-Administrator verwaltet), das mit autorisierten IP-Adressen übereinstimmen soll. Standardmäßig wird der Filter für Remote-IP-Adressen mit der Loopbackadapter-IP-Adresse 127.0.0.1 konfiguriert. In einer Produktionsumgebung für sichere Kommunikation sollten Sie die Verwendung von SSL zwischen dem Crawler und der Crawler-Oberfläche in Betracht ziehen.

Gehen Sie wie folgt vor:

1. Melden Sie sich abhängig von Ihrer CA SDM-Konfiguration bei folgendem Server an:
 - Konventionell: Primärserver oder Sekundärserver
 - Erweiterte Verfügbarkeit: Anwendungsserver

2. Öffnen Sie die Datei "web.xml" im folgenden CA SDM-Verzeichnis:

```
$NX_ROOT\bopcfg\www\CATALINA_BASE_FS\webapps\fscrawl\WEB-INF
```

3. Erstellen Sie eine Sicherungskopie der Datei "web.xml".
4. Suchen Sie den Abschnitt `<filter-name>Remote Address Filter</filter-name>`. Ändern Sie das Muster in `<param-value>` im `<filter>`.

Dieser Parameter ermöglicht die Angabe eines Bereichs von IP-Adress-Mustern. Stellen Sie auch den Zugriff vom Remote-Rechner bereit, der SharePoint hostet. Weitere Informationen zum Tomcat Remote IP Address Filter finden Sie in der Apache Tomcat-Dokumentation.

5. Speichern Sie die XML-Datei.
6. Starten Sie das Servlet "Föderierte Suche" neu.

Hinweis: Wenn Sie "Tomcat für föderierte Suche" neu starten, können Sie keine föderierte Suche ausführen.

7. Der Wert des Tomcat Remote IP Address Filters wird geändert, und auf die Crawler-Oberfläche kann jetzt vom Remote-Rechner zugegriffen werden.

Hinweis: Greifen Sie nicht auf die Crawler-Oberfläche über eine nicht konfigurierte IP-Adresse zu. Sie werden an die CA SDM-Benutzeroberfläche umgeleitet.

8. Der Zugriff auf die Crawler-Oberfläche erfolgt über eine URL wie bei jeder anderen Webanwendung. Um SharePoint-Protokollierung zu validieren, geben Sie folgende URL in einen Browser ein:

```
http://<sdmhostname>:<FS_TOMCAT_PORT>/fscrawl/index.jsp?farm=<FarmName>
```

Hinweis: Bei allen Elementen der URL ist Groß- und Kleinschreibung zu beachten.

hostname

Gibt den vollqualifizierten Domännennamen für "Tomcat für föderierte Suche" an

Portnummer

Definiert die standardmäßige Portnummer, die zu "Tomcat für föderierte Suche" bei der Installation und Konfiguration der CA SDM-Anwendung zugewiesen wurde. Wird verwendet, um auf "Tomcat für föderierte Suche" zuzugreifen.

fscrawl

Gibt den Namen des Servlet an. Bei Servletnamen sind Groß- und Kleinschreibung zu berücksichtigen. Geben Sie immer "fscrawl" an.

index.jsp

Gibt den Namen der Seite an, die für das Testen der Konfiguration der Crawler-Oberfläche verwendet werden kann.

<FarmName>

Jedes <farm> in "crawler_surface_config.xml" enthält eine <sdm_user>-Eingabe. Muss mit dem authentifizierten Anwender übereinstimmen. Requests werden an die CA SDM-Web-Benutzeroberfläche für eine fehlgeschlagene Anwenderauthentifizierung umgeleitet. <sdm_user> steuert den Datenzugriff auf der Ebene der CA SDM-Objekt-Manager. Diese Sicherheitsschicht der <farm>-Ebene verhindert, dass ein Mandant auf andere Mandantendaten zugreift.

Konfigurieren der Anwender-ID für die Crawler-Oberfläche

Konfigurieren Sie die Anwender-ID für die Crawler-Oberfläche in der Datei "crawler_surface_config.xml", um die Crawler-Oberfläche zu ändern.

Wichtig! Machen Sie sich mit den Spracheinstellungen Ihres Browsers vertraut. SharePoint berücksichtigt die Sprache, die in der Suchanfrage verwendet wird.

Gehen Sie wie folgt vor:

1. Melden Sie sich beim folgenden CA SDM-Server an, der die Crawler-Oberfläche abhängig von Ihrer Installationskonfiguration hostet:
 - Konventionell: Primärserver oder Sekundärserver
 - Erweiterte Verfügbarkeit: Anwendungsserver
2. Öffnen Sie die Datei "crawler_surface_config.xml" im folgenden CA SDM-Verzeichnis:

\$NX_ROOT\bopcfg\www\CATALINA_BASE_FS\webapps\fscrawl\WEB-INF

3. Erstellen Sie eine Sicherung der Datei "crawler_surface_config.xml".

Wichtig! Führen Sie alle XML-Dateiänderungen in einer Testumgebung durch, bevor Sie die letzten Änderungen auf einen Betriebsserver durchführen.

4. Suchen Sie in der ursprünglichen Datei `<sdm_user>CHANGE_THIS</sdm_user>` unter jedem `<farm>`-Abschnitt, und ersetzen Sie "CHANGE_THIS" durch die Crawler-Anwender-ID, die Sie zuvor erstellt haben.
5. Sie können die XML-Objektattribute abhängig von Ihren Anforderungen weiter ändern und beschränken.

Hinweis: Weitere Informationen finden Sie unter XML-Konfigurationsdatei der Crawler-Oberfläche.

6. Speichern Sie die XML-Datei.
7. Starten Sie das Servlet "Föderierte Suche" neu, um die Datei neu zu laden.

Die Crawler-Oberflächen-XML-Datei wird geändert.

Crawler-Oberflächen-XML-Konfigurationsdatei

Die Datei "crawler_surface_config.xml" enthält die folgenden XML-Abschnitte:

<objects>

Enthält die Informationen zu den Objekten und Attributen, die die Crawler-Oberfläche für ein Objekt freigibt. Der `<objects>`-Abschnitt beschreibt das Layout einer Detailseite für jeden Objekttyp, der einem Crawler ausgesetzt wird. Dieser Abschnitt kontrolliert jedoch nicht die Auswahl von einzelnen Datensätzen. Der `<objects>`-Abschnitt ist eine Sammlung von Anmeldeinfos-Abschnitten.

Jedes Objekt wird in einem Anmeldeinfos-Abschnitt definiert. Die Standardangaben für diese Objekte lauten folgendermaßen:

KD

Gibt Knowledge-Dokumente an.

chg

Gibt Changes an.

Iss

Gibt Issues an.

in

Gibt Incidents an.

pr

Gibt Probleme an.

cr

Gibt Requests an.

Die XML-Datei enthält die folgenden Abschnitte, die den <head>-Abschnitt einer Detailseite in CA SDM erstellen:

<name>

Geben Sie den Majic-Objektnamen des angezeigten Objekts an.

<note>

Geben Sie eine kurze Beschreibung des Objekts an. Dieses Element ist nur für Dokumentationszwecke gedacht und wird von der Crawler-Oberfläche ignoriert.

<last_mod_dt>

Geben Sie den Attributnamen an, der das Datum und die Uhrzeit der letzten Änderung speichert. Dieser Zeitstempel wird dem Suchmaschinen-Crawler bereitgestellt, damit dieser feststellen kann, ob der Datensatz aktualisiert worden ist. Viele Crawler verwenden diesen Zeitstempel während eines inkrementellen Crawls. Ein aktualisierter Zeitstempel signalisiert, dass der Datensatz seit dem letzten Crawl geändert worden ist. Der Suchmaschinencrawler überspringt den Crawl, wenn der Datensatz seit dem letzten Crawl nicht aktualisiert worden ist.

<title>

Geben Sie das Attribut an, das für den Titel der Detailseite verwendet wird. Die Suchmaschinen verwenden dieses Element als Titel des Dokuments, das in Suchergebnissen zurückgegeben wird. Dieser Elementeintrag generiert einen HTML-<title>-Tag im <head> der Detailseite. Bei Knowledge-Dokumenten wird als Titel standardmäßig der Titel des Knowledge-Dokuments verwendet. Die Zusammenfassung wird für den Titel bei Incidents, Problemen, Requests, Changes und Issues verwendet.

<meta_data>

Geben Sie einzelne oder mehrere Eigenschaften an, die als Metadaten angezeigt werden. Metadaten ermöglichen einer Suchmaschine, zusätzliche Merkmale des Dokuments in seinem Index zu speichern. Metadaten werden nicht direkt durchsucht, sondern als Filter der Suchergebnisse angewandt. Dieser Abschnitt generiert HTML-`<meta>`-Tags im `<head>` der Detailseite.

Jeder Eintrag im `<meta_data>`-Abschnitt enthält einzelne oder mehrere `<property>`-Einträge. Jedes `<property>`-Element besteht aus einem `<name>`-Element und einem `<content>`-Element.

<name>

Geben Sie den Namen der Metadateneigenschaft an.

<content>

Geben Sie das Attribut des Objekts an, das als Wert für die Metadaten verwendet wird.

Zusammen generiert jedes Elementpaar aus `<name>` und `<content>` einer `<property>` einen HTML-`<meta>`-Tag. Die Suchmaschinen-Crawler verwenden standardmäßig die folgenden beiden Metadateneigenschaften:

Beschreibung

Geben Sie die Metadateneigenschaft einer Suchmaschine an, die eine kurze Zusammenfassung des Dokuments speichert.

Author

Geben Sie den Verfasser des Dokuments an.

Die CASDMTENANT-Metadateneigenschaft wird auch standardmäßig für jedes Objekt konfiguriert. Diese Eigenschaft ist eine für CA SDM spezifische Metadateneigenschaft. Wenn CA SDM für Mandantenfähigkeit konfiguriert wird, verwendet die Crawler-Oberfläche diese Eigenschaft, um den Mandanten-Namen des Objekts dem Crawler der Suchmaschine zu exponieren. Später, während einer Föderierten Suche, werden die von der Suchmaschine zurückgegebenen Ergebnisse auf Basis dieser Metadateneigenschaft gefiltert.

Die XML-Datei enthält die folgenden Abschnitte, die den <body>-Abschnitt einer Detailseite in CA SDM ausmachen:

<additional_attributes_to_index>

Zeigt eine Liste von Attributen von dem Objekt an, das die Crawler-Oberfläche exponiert. Trennen Sie Mehrfachangaben mit einem Komma und einem Leerzeichen. Zum Beispiel, PROBLEM, LÖSUNG, SD_ASSET_ID.name.

<activity_logs>

Zeigt Informationen an, die der Crawler-Oberfläche von Aktivitätsprotokollen für Objekte exponiert werden, die über Aktivitätsprotokolle verfügen. Der <activity_logs>-Abschnitt enthält die Elemente Anmeldeinfos, <select_criteria>, <rel_attr> und <attributes>.

Anmeldeinfos

Gibt den Objektnamen an, der die Aktivitätsprotokolleinträge für das Objekt enthält. Zum Beispiel das Aktivitätsprotokollobjekt für:

- Incidents, Probleme und Requests ist *alg*.
- Changes ist *chgalg*.
- Issues ist *issalg*.
- Knowledge-Dokumente ist *O_COMMENTS*.

<select_criteria>

Ermöglicht es Ihnen, die exponierten Aktivitätsprotokollobjekte zu filtern. Dieses Element ist wichtig, um die Relevanz Ihrer Suchergebnisse zu vergrößern, indem häufig auftretende Wörter eliminiert werden. Zum Beispiel enthält das <select_criteria> für chgalg die folgende magische WHERE-Klausel:

```
"type IN ( 'ST' , 'UPD_RISK' , 'CB' , 'RS' , 'LOG' , 'TR' , 'ESC' , 'NF' , 'UPD_SCHED' ) "
```

Dieses Kriterium schließt nur Aktivitätsprotokolleinträge ein, die es einem Anwender ermöglichen, Kommentare einzugeben, und eliminiert Aktivitätsprotokolleinträge mit festem Text wie "Anfänglich" oder "Dokument anhängen".

<rel_attr>

Gibt an, wie ein Aktivitätsprotokolleintrag sich auf sein übergeordnetes Objekt bezieht. Der <rel_attr>-Unterabschnitt enthält die Elemente <parent_obj_attr>- und <join_attr>.

<parent_obj_attr>

Zeigt ein Attribut eines Aktivitätsprotokolls an, das einen SREL (oder Fremdschlüssel-Pointer) zum übergeordneten Objekt enthält. Zum Beispiel ist change_id das Attribut von chgalg.

<join_attr>

Zeigt das relationale Attribut (Rel Attr) des übergeordneten Objekts an, das in <parent_obj_attr> gespeichert wird. Zum Beispiel ist das <join_attr> für chgalg "id". Sie können diese Werte anhand des folgenden Befehls verifizieren:

```
bop_sinfo -df chgalg
```

Sie können beide dieser Werte durch die Verwendung des Befehls "bop_sinfo -df chgalg" verifizieren. Die Ausgabe muss zeigen, dass der Wert für change_id *SREL* -> *chg.id* und für ISS *SREL* -> *iss.persistent_id* ist.

<attachments>

Dieser Unterabschnitt ermöglicht es Ihnen, dem Crawler der Suchmaschine Anhänge auszusetzen, sodass ihr Inhalt zusammen mit dem übergeordneten Objekt indiziert werden kann. Der <attachments>-Abschnitt ist nur für Objekte zugelassen, die über Anhänge verfügen.

Anhänge werden auf besondere Art und Weise von der Crawler-Oberfläche verarbeitet. Anstatt dem Crawler den Inhalt eines jeden Anhangs von der Crawler-Oberfläche zu senden, exponiert die Crawler-Oberfläche statt dessen einen Hyperlink, dem der Crawler folgen kann, um den Anhang von CA SDM herunterzuladen. Wird später während einer föderierten Suche auf den Hyperlink eines in den Suchergebnisse eingeschlossenen Anhangs geklickt, wird der Anwender zum übergeordneten Objekt anstelle direkt zum Anhang geleitet.

Der <attachments>-Abschnitt enthält die Elemente Anmeldeinfos, <rel_attr>, <attmnt_id> und <is_parent_updated>.

Anmeldeinfos

Dieses Element gibt das Majic-Objekt an, das den Anhang mit seinem übergeordneten Objekt verbindet.

<rel_attr>

Dieser Unterabschnitt funktioniert genauso wie bei den Aktivitätsprotokollen. Er gibt an, wie das übergeordnete Objekt sich auf dieses Objekt bezieht, das das übergeordnete Objekt mit dem Anhang verbindet.

<attmnt_id>

Dieses Element gibt das Attribut dieses Verbindungsobjekts an, das auf den Anhang hinweist.

<is_parent_updated>

Gibt der Crawler-Oberfläche an, wie das Datum der letzten Änderung für das Objekt angezeigt werden soll. Für einige Objekte wie Knowledge-Dokumente (KDs) wird bei Hinzufügen eines Anhangs das Datum der letzten Änderung des Knowledge-Dokuments nicht aktualisiert. Das Datum der letzten Änderung ist wichtig, wenn die Suchmaschine einen inkrementellen Crawl durchführt.

<configuration_items>

Dieser Abschnitt wird für Objekte verwendet, die eine Liste der Configuration Items enthalten. Dieser Abschnitt enthält die Elemente Anmeldeinfos, <rel_attr> und <attributes>.

Anmeldeinfos

Entspricht denen in Aktivitätsprotokollen und Anhängen.

<rel_attr>

Entspricht denen in Aktivitätsprotokollen und Anhängen.

<attributes>

Dieses Element entspricht dem in Anhängen.

<multi-farm_datasets>

Nach dem <objects>-Abschnitt kommt der <multi-farm_datasets>-Abschnitt. Während der <objects>-Abschnitt die CA SDM-Objekte und -Attribute definiert, die von der Crawler-Oberfläche angezeigt werden können, gibt <multi-farm_datasets> an, wie Datensätze ausgewählt werden. Der <multi-farm_datasets>-Abschnitt ist eine Sammlung von <farm>-Abschnitten.

<farm>

Jeder <farm>-Abschnitt kontrolliert die CA SDM-Informationen, die einem Crawler exponiert werden. Wird ein Crawler konfiguriert, wird der <farm>-Abschnitt in der URL angegeben. Nur die im <farm>-Abschnitt angegebenen Informationen werden dem Crawler exponiert. Jeder <farm>-Abschnitt enthält die Elemente <name>, <data_sets>, <sdm_user> und <name>.

Hinweis: Dieser Wert beachtet Groß- und Kleinschreibung.

<data_sets>

Geben Sie die angezeigten Objekte an, und geben Sie an, wie ihre Datensätze ausgewählt werden. Dieser Unterabschnitt enthält einzelne oder mehrere Anmeldeinfos-Elemente. Jedes Objektelelement enthält ein <name>- und ein <select_criteria>-Element.

<name>

Verweist das Anmeldeinfos, das im <objects>-Abschnitt definiert ist.

<select_criteria>

Dieses Element gibt eine Majic an, die verwendet wird, um die Datensätze des Objekts auszuwählen.

<sdm_user>

Dieses Element gibt die CA SDM-Anwender-ID an, die verwendet werden muss, wenn auf diese Farm zugegriffen wird. Diese Anwender-ID muss Zugriffstyp=crawler und Rolle=crawler haben.

sdm_domsrvr_name

Bei einer großen Menge an Indizierungsdaten sollten Sie einen Objektmanager für die Crawler-Oberfläche zuordnen. Standard ist domsrvr.

sharepoint_properties_file

Dieser Wert ist der Name der SharePoint-Eigenschaftsdatei, die standardmäßig im CA SDM-Verzeichnis verfügbar ist:

NX_ROOT\CATALINA_BASE_FS\lib

Enthält einen Konfigurationsparameter, der sowohl von der föderierten Suche als auch von der Crawler-Oberfläche verwendet wird, wenn CA SDM für mehrere Mandanten konfiguriert ist.

Hinweis: Wenn CA SDM für mehrere Mandanten konfiguriert ist, aktualisieren Sie den Parameter "sharepoint_version" in dieser Datei, um Ihre SharePoint-Version anzugeben.

<list_form_number_of_records_per_object>

Verwenden Sie diesen Parameter für die Konfiguration der Anzahl von Hyperlinks, die die Crawler-Oberfläche auf einer Listenseite für ein Objekt angibt.

<send_wait_timeout>

Dieser Wert steuert die Anzahl der Sekunden, die die Crawler-Oberfläche auf eine Antwort vom Objektmanager wartet, bevor das Zeitlimit überschritten wird.

Konfigurieren des SharePoint-Crawlers

Konfigurieren Sie Crawler, um Inhalte in SharePoint zu durchsuchen.

Der Crawler ist eine mehrfädige Anwendung mit hohem Durchsatz und kann manchmal negative Auswirkungen auf die CA SDM-Performance haben. Um dies zu vermeiden, stellen Sie Folgendes sicher:

- Beschränken Sie die Anzahl der gleichzeitigen SharePoint-Crawler, die gleichzeitig auf die Crawler-Oberfläche zugreifen.
- Verwenden Sie Auswirkungsregeln für SharePoint-Crawler, um Crawler zu drosseln
- Planen Sie die Crawls zu Tageszeiten mit geringem Datenverkehr
- Ordnen Sie einen Objektmanager <sdm_domsrvr_name> zur Crawler-Oberfläche in "crawler_surface_config.xml" zu. Weitere Informationen finden Sie unter XML-Konfigurationsdatei der Crawler-Oberfläche.
- Ordnen Sie für die erweiterte Verfügbarkeit von CA SDM einen gesamten Anwendungsserver zur Crawler-Oberfläche zu.

Gehen Sie wie folgt vor:

1. [Erstellen Sie die Inhaltsquelle in SharePoint](#) (siehe Seite 181)
2. [Erstellen von Crawler-Regeln](#) (siehe Seite 182)
3. [Führen Sie den Crawler in SharePoint aus](#) (siehe Seite 183)
4. [Konfigurieren Sie die Metadaten in SharePoint](#) (siehe Seite 184)
5. [Verifizieren Sie die Crawl-Daten in SharePoint](#) (siehe Seite 185)

Erstellen Sie die Inhaltsquelle in SharePoint

Hinweis: Die Namen der SharePoint-spezifischen Einstellungen können abhängig von der SharePoint-Version variieren. Weitere Informationen zur Erstellung von Inhaltsquellen in SharePoint finden Sie in der Microsoft SharePoint-Dokumentation.

Erstellen Sie Inhaltsquellen, um den Inhaltstyp zu identifizieren, den der SharePoint-Crawler bearbeitet.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei der Konsole "MS SharePoint Central Administration" an.
2. Klicken Sie auf Dienstanwendung verwalten, Suchdienstanwendung.
3. Klicken Sie auf Inhaltsquelle für das Erstellen von neuen Inhaltsquellen:
4. Geben Sie den Datennamen für die Inhaltsquelle in Name als CA SDM ein.
5. Legen Sie für "Inhaltsquellentyp" den Wert "Websites" fest.
6. Geben Sie folgende URL in Startadresse ein.
`http://<sdmhostname>:<FS_TOMCAT_PORT>/fscrawl/listObject.jsp?farm=<Farm Name>`
7. Damit sich der Crawler nicht von der Crawler-Oberfläche entfernt, sollten Sie es in Betracht ziehen, die Seitentiefe auf 2 und die Serverwechsel auf 1 zu beschränken. Empfohlene Mindestwerte, um das Durchsuchen von Anhängen zu erlauben.
8. Klicken Sie auf "Speichern".

Erstellen von Crawlregeln

Crawlregeln definieren, wie die URL der SharePoint-Web-Crawler-Oberfläche durchsucht wird. Definieren Sie folgende Crawl-Regeln:

- Eine Crawlregel, mit der SharePoint die Crawler-Oberfläche durchsuchen kann.
- Eine Crawlregel, die es SharePoint ermöglicht, auf Anhänge zuzugreifen.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei der Konsole "MS SharePoint Central Administration" an.
2. Klicken Sie auf Dienstanwendung verwalten, Suchdienstanwendung.
3. Klicken Sie auf Crawlregel. Erstellen Sie eine neue Crawlregel.
4. Geben Sie folgende URL in den Browser ein:

`http://<sdmhostname>:<FS_Tomcat_Port>/fscrawl/*farm=<farm-name>*`

Wichtig! Bei der Crawler-Oberflächen-URL muss Groß-/Kleinschreibung beachtet werden. SharePoint ändert großgeschriebene Hostnamen in Kleinbuchstaben. Stellen Sie bei SharePoint 2010 sicher, dass das Kontrollkästchen "Groß-/Kleinschreibung beachten" aktiviert ist.

5. Wählen Sie "Alle Einträge in diesem Pfad einschließen" aus, um den Crawler zu konfigurieren.
6. Wählen Sie "Komplexe URLs (URLs mit Fragezeichen (?)) durchforsten" aus.
7. Wählen Sie "Geben Sie ein anderes Konto für den Inhaltzugriff an" aus.
8. Geben Sie den CA SDM-Anwenderkontonamen und das Kennwort für die Crawler-Oberfläche ein.
9. Erstellen Sie eine zweite Crawlerregel für die CA SDM-Anhänge:

`http://<sdmhostname>:<FS_TOMCAT_PORT>/CAisd/*`

10. Geben Sie die Standardauthentifizierung an:

Hinweis: Die Crawler-Oberfläche verwendet Basisauthentifizierung. Der CA SDM-Repository-Daemon verwendet proprietäre BOPSID-Sicherheit, die von SharePoint nicht direkt unterstützt wird. Geben Sie ein beliebige Anwender-ID und ein Kennwort an, oder wählen Sie "Anonymer Zugriff" aus, wenn diese Option in Ihrer SharePoint-Version verfügbar ist.

- Wählen Sie für SharePoint 2013 die Option "Geben Sie ein anderes Konto für den Inhaltzugriff an" aus. Wählen Sie die Option "Anonymer Zugriff" aus.
- Verwenden Sie für SharePoint 2010 das Standardinhaltszugriffskonto (NT AUTHORITY\NETWORK SERVICE).

Die Microsoft SharePoint-Crawlregel ist erstellt.

Starten eines Crawl in SharePoint

Starten Sie einen vollständigen oder inkrementellen Crawl der Inhaltsquellen in SharePoint, um den Suchinhalt zu indizieren.

Gehen Sie wie folgt vor:

1. Navigieren Sie zur Seite "Microsoft SharePoint Central Administrator".
2. Klicken Sie auf Dienstanwendung verwalten, Suchdienstanwendung.
3. Klicken Sie auf Inhaltsquellen. Wählen Sie die Inhaltsquelle aus, die Sie für die SharePoint-Crawler-Oberfläche konfiguriert haben.
4. Wählen Sie "**Vollständigen Crawl starten**" oder "**Inkrementellen Crawl starten**" aus.

Ein voller Crawl durchsucht den gesamten Inhalt unter einer Inhaltsquelle. Volle Crawls nehmen mehr Zeit und Ressourcen in Anspruch als inkrementelle Crawls.

Bei einem inkrementellen Crawl bleibt der Index intakt, und der Crawler durchsucht nur den Inhalt, der seit dem letzten erfolgreichen Crawl hinzugefügt oder geändert wurde. Weitere Informationen finden Sie in der Microsoft SharePoint-Dokumentation.

Konfigurieren Sie die Metadaten in SharePoint

Hinweis: Dieses Thema trifft nur auf Umgebungen für CA SDM mit mehreren Mandanten zu.

Wenn der Crawler CA SDM-Metadaten findet, werden die Metadaten in SharePoint als "Gecrawlte Eigenschaften" gespeichert. Diese Eigenschaften werden während des ersten vollständigen Crawls der CA SDM-Crawler-Oberfläche entdeckt. Der SharePoint-Crawler entdeckt die Metadaten und erstellt die "Crawled Eigenschaften".

Metadaten werden verwendet, um dem Crawler zusätzliche Informationen in den Detailseiten mithilfe des <meta>-Tags im <head>-Abschnitt zu übergeben. Diese Informationen sind für das Suchen und Filtern verfügbar. Wenn CA SDM für Mandantenfähigkeit konfiguriert wird, stellt die Crawler-Oberfläche nur die Mandantenmetadateninformationen dar.

Wenn Sie eine föderierte Suche ausführen, wird der Mandantenname der Suchmaschine übergeben, um die Ergebnisse entsprechend zu filtern.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei der Konsole "MS SharePoint Central Administration" an.
2. Klicken Sie auf Dienstanwendung verwalten, Suchdienstanwendung, Metadaten (SharePoint 2010) oder Suchschema (SharePoint 2013).
3. Stellen Sie sicher, dass SharePoint-Crawling auf den CA SDM-Daten erfolgreich war.
4. Klicken Sie auf Verwaltete Eigenschaften.
5. Klicken Sie auf Neue verwaltete Eigenschaft.
6. Geben Sie CASDMTENANT als Eigenschaftsname ein.
CASDMTENANT gibt den Mandantennamen für das CA SDM-Objekt an. Die Informationen des untergeordneten Mandanten werden nicht angezeigt.
7. Wählen Sie Text als Eigenschaftstyp aus.
8. Scrollen Sie nach unten. Klicken Sie auf "Neue Zuordnung hinzufügen".
9. Suchen Sie nach der Crawl-Eigenschaft "CASDMTENANT", und wählen Sie sie aus.
10. Klicken Sie auf "OK", um die neue verwaltete Eigenschaft zu speichern.

Die Metadaten in SharePoint sind konfiguriert.

Verifizieren Sie die Crawl-Daten in SharePoint

Verifizieren Sie die Crawler-Daten in SharePoint, um Suchergebnisse anzuzeigen.

Gehen Sie wie folgt vor:

1. Melden Sie sich als Service Desk-Administrator von CA SDM an.
2. Klicken Sie auf die Registerkarte "Knowledge Management" für ein neues oder ein vorhandenes Ticket.
3. Wählen Sie "SharePoint-Suche" aus.
4. Geben Sie den Suchschlüssel ein. Klicken Sie auf "Suchen".

Der Crawler zeigt die Suchergebnisse an.

Fehlerbehebung

Die Crawler-Oberfläche hat das übliche Array von Protokolldateien:

1. Wenn Sie die Debug-Funktion für föderierte Suche aktivieren wollen, navigieren Sie zum folgenden CA SDM-Verzeichnis:

`$NX_ROOT\bopcfg\www\CATALINA_BASE_FS\webapps\cafedsearch\WEB-INF`

2. Öffnen Sie die Datei `log4j.properties` und ändern Sie die Info auf den Debug-Modus.
3. Um Debug für `fscrawl` zu aktivieren, navigieren Sie zum folgenden CA SDM-Verzeichnis:

`$NX_ROOT\bopcfg\www\CATALINA_BASE_FS\webapps\fscrawl\WEB-INF`

4. Öffnen Sie die Datei `log4j.properties` und ändern Sie die Info auf den Debug-Modus.
5. Um Syntaxfehler zu korrigieren, die während der Konfiguration der SharePoint-Crawler-Oberfläche auftreten, öffnen Sie die `jfscrawl`-Protokolldatei vom CA SDM-Verzeichnis:

`$NX_ROOT\logs directory`

6. Wenn Sie Syntaxfehler finden, korrigieren Sie die XML-Datei, und starten Sie "Tomcat für föderierte Suche" neu. Das Protokoll befinden sich in

`$NX_ROOT\logs\jfscrawl.log`

Wenn zum Beispiel ein `<meta_data>`-Tag versehentlich beschädigt wird, dann zeigt das Protokoll folgenden Fehler an:

```
08/06 15:43:52,624 [pool-2-thread-1] ERROR FSCrawlApplicationListener 302
XmlException::Problem loading
config_file::C:\PROGRA~2\CA\SERVIC~1\bopcfg\www\CATALINA_BASE_FS\webapps\fscrawl\WEB-INF\crawler_surface_config.xml:274:8: error: </meta_dataxxxx> does not close tag <meta_data>
```

```
08/06 15:43:52,625 [pool-2-thread-1] ERROR FSCrawlApplicationListener 144
crawler_surface_config.xml could not be loaded, cannot read.
```

7. Wenn keine Syntaxfehler vorhanden sind, dann wird folgende Meldung angezeigt:

```
08/06 15:46:27,924 [pool-2-thread-1] INFO FSCrawlApplicationListener 58 fscrawl
context had been loaded successfully.
```

8. Korrigieren Sie andere Fehler, die nicht angezeigt werden, bis Sie versuchen, auf CA SDM zuzugreifen.

Zum Beispiel wurde angefordert, das unbekannte Attribut `xxxxx` für Incidents im `<additional_attributes_to_index>`-Element der `crawler_surface_config.xml` anzugeben. Die Crawler-Oberflächen-Anwendung entdeckt den Fehler nicht. Wenn die Crawler-Oberfläche den Request an den Objektmanager sendet, wird der Fehler festgestellt und in der `stdlog.x`-Datei folgendermaßen berichtet:

```
08/06 15:51:23.92 SDMSERVER domsrvr 10860 ERROR domset.c 8049 Unknown attribute
"xxxxx" requested from domset MLIST_STATIC of factory
```

9. Verwenden Sie den Befehl "bop_sinfo -d", um den Fehler zu beheben.
10. Ändern Sie die Datei "global_sd.xml"
11. Starten Sie das Servlet "Föderierte Suche" neu.

Die Crawler-Oberflächen-Objekte werden ohne Fehler konfiguriert.

Erstellen Sie einen neuen anwenderspezifischen Adapter mithilfe der SDK-Schnittstelle

Wichtig! CA Federated SDK-Beispielquellcode wird Kunden zur Verfügung gestellt, um alternative anwenderspezifische Adapter zu erstellen und bereitzustellen. Allerdings wird CA Support keinen Support bereitstellen, um den eigentlichen anwenderspezifischen Code zu schreiben. Wir unterstützen nicht aktiv die Erstellung und Bereitstellung von zusätzlichen Adaptern jenseits der mit der CA Service Desk Manager-Anwendung versendeten SDK-Quellcodebeispiele.

Die CA Federated Search SDK-Architektur ist für Erweiterbarkeit entworfen. Das SDK enthält alle notwendigen JAR-Dateien, um einen anwenderspezifischen Adapter zu entwickeln. Beispiel-Eclipse-Projekte können importiert werden, und Ant-Build-Ziele werden auch angegeben, um anwenderspezifische Suchadapter zu erstellen. Das SDK befindet sich im CA SDM-Verzeichnis:

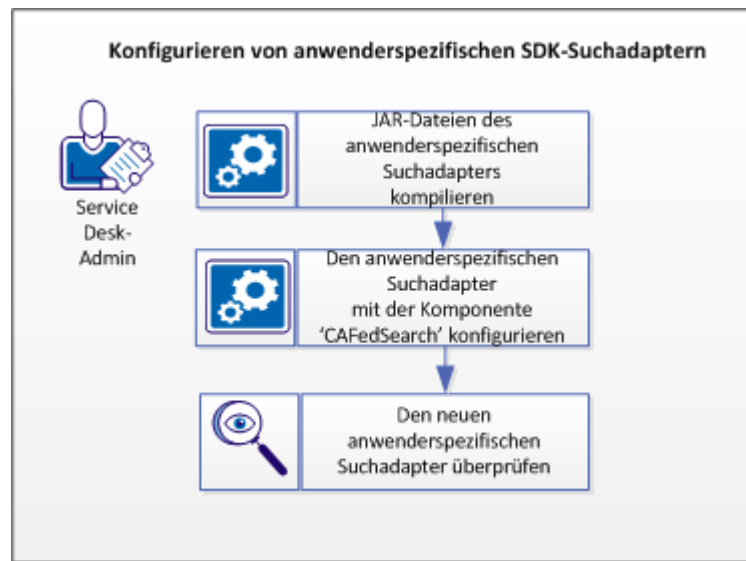
```
$NX_ROOT\samples\sdk\fedsearch\adapters-source.tar.gz
```

Der Quellcode der folgenden Adapter kann verwendet werden, um zusätzliche anwenderspezifische Adapter zu schreiben:

- Google
- CA Open Space
- Microsoft Share Point

Hinweis: Quellcode für das CAFedSearch-Servlet, der zugehörige Basisrahmen und die Sicherheitsfilter werden nicht bereitgestellt. Es wird kein Quellcode für Komponenten der Crawler-Oberfläche bereitgestellt.

Die SDK-Komponente ist in Java geschrieben und wird als jar-Datei freigegeben (cafedsearch-adapter-sdk-1.0.0.jar). Das SDK stellt eine einfache Schnittstelle bereit, um es Kunden zu ermöglichen, ihre eigenen Suchadapter zu entwickeln und bereitzustellen.



Gehen Sie wie folgt vor:

1. [Kompilieren Sie die JAR-Dateien des anwenderspezifischen Suchadapters](#) (siehe Seite 190)
2. [Konfigurieren Sie den neuen anwenderspezifischen Suchadapter mit der Komponente "CAFedSearch"](#) (siehe Seite 193)
3. [Verifizieren des neuen anwenderspezifischen Suchadapters](#) (siehe Seite 195)

Kompilieren der JAR-Dateien des neuen anwenderspezifischen Adapters

Kompilieren Sie die JAR-Dateien des anwenderspezifischen Adapters erfolgreich.

Gehen Sie wie folgt vor:

1. Kompilieren Sie die neuen anwenderspezifischen Suchadapter. Stellen Sie sicher, dass Sie folgende jar-Dateien in Ihrem Java-Klassenpfad haben:

jsr311-api-1.0.jar

Diese jar-Datei ist im CA SDM-Verzeichnis verfügbar:

%NX_ROOT%\java\lib\CXF\

cafedsearch-core.jar

Diese Datei ist im Verzeichnis verfügbar:

%NX_ROOT%\bopcfg\www\CATALINA_BASE_FS\webapps\cafedsearch\WEB-INF\lib

cafedsearch-adapter-sdk-1.0.0.jar

Diese Datei ist im Verzeichnis verfügbar:

%NX_ROOT%\bopcfg\www\CATALINA_BASE_FS\webapps\cafedsearch\WEB-INF\lib

log4j-1.2.15.jar (optional)

Diese Datei ist im Verzeichnis verfügbar:

%NX_ROOT%\java\lib

2. Schreiben Sie eine neue Java-Klasse, die die Klasse "SearchAdapter" erweitert und eine Implementierung für die abstrakte Methode angibt.

Suche

Die Komponente "CAFedSearch" ruft die Suchmethodenparameter auf und gibt sie weiter. Diese Parameter werden im Parameter "SearchOptions" für jede Suchanfrage vom Client eingebettet.

Hinweis: Stellen Sie sicher, dass Ihre Implementierung Thread-sicher ist, da die Komponente "CAFedSearch" nur eine Instanz der Java-Klasse verwaltet. Für jeden Suchvorgang wird das Suchverfahren auf der gleichen Instanz aufgerufen

3. Der Parameter "SearchOptions" für das Suchverfahren hat folgende Methoden:

getSearchTerms()

Gibt die Methode für das Abrufen der Suchzeichenfolge an.

getStartIndex()

Gibt die Startindexmethode an, d. h. die Zahl, ab der der Client Elemente suchen möchte. Der Index beginnt mit 1.

getItemsPerPage()

Gibt die Höchstanzahl der Suchergebnisse an, die der Client erwartet.

Hinweis: Sie können auch andere Java-Klassen-Methoden verwenden. Zum Beispiel: `getUserId()`

4. Senden Sie die erfassten Informationen an die externe Suchmaschinen-API für das Abrufen der Suchergebnisse.

Hinweis: Weitere Informationen über Java-Klassen-Methoden finden Sie in der Java-Dokumentation.

5. Die Suchmethode gibt eine Instanz der `ResultCollection`-Klasse zurück. Erstellen Sie eine Instanz der `ResultCollection`, und stellen Sie Werte mithilfe der folgenden Methoden bereit:

`setSources(String name)`

Gibt den Namen des Suchadapters an. Namen unterscheiden zwischen Groß- und Kleinschreibung und müssen genau mit dem Namen übereinstimmen, der in der Konfigurationsdatei des Hilfsprogramms angegeben wird. Aus Zweckmäßigkeitsgründen stellt `SearchAdapter` die Methode `"getName()"` bereit, die verwendet werden sollte.

Beispiel:

```
results.setSources(getName());
```

`setTotalResults(int total)`

Gibt die Gesamtanzahl der Suchergebnisse an.

`setStartIndex(int startIndex)`

Gibt einen Startindex von Ergebnissen an. Geben Sie diesen Wert gemäß den Ergebnissen von Ihrer Suchmaschine ein.

```
results.setStartIndex(startIndex);
```

6. Eine Sammlung von `"ResultItems"` muss in das Objekt `"ResultCollection"` durch Aufruf der Methode `"setSearchResultItems"` übergeben werden. Um gleichzeitig eine Instanz von `"ResultItem"` hinzuzufügen, verwenden Sie die Methode `"addSearchResultItem()"`.

Hinweis: Weitere Informationen zur Java-Klasse `"ResultCollection"` finden Sie in der Java-Dokumentation.

7. Die `ResultItem`-Klasse hat die folgenden wichtigen Methoden, die für jedes Suchergebniselement (Zeile) gefüllt werden müssen.

`setContentText(String txt)`

Gibt eine Methode für das Festlegen des tatsächlichen Inhalts der Suchergebnisse an.

`setContentHTML(String txt)`

Gibt eine Methode zur Festlegung des HTML-Inhalts an (kann HTML-Tags enthalten). Wenn die Suchmaschine HTML hervorhebt, dann legen Sie den hervorgehobenen Text mithilfe dieser Methode fest.

Hinweis: Verfügt Ihre Suchmaschine nicht über diese Funktion, können Sie zur Hervorhebung des Texts eine einfache Java-Klassenmethode schreiben. Der CA Open Space-Adapter hat eine einfache Methode, um Bedingungen in den Suchergebnissen in Fettschrift zu setzen.

setTitleHTML(String titleHTML)

Methode zur Festlegung des HTML-Titels (kann die HTML-Tags enthalten).

setTitleText(String titleText)

Methode zur Festlegung eines einfachen Titels (kann keine HTML-Tags enthalten).

setSource(String source)

Methode zur Festlegung des Quellenattributs. Ein typischer Aufruf wäre "item setSource(getName());"

Hinweis: Wenn der Suchadapter mehr JAR-Dateien benötigt, passen Sie build.xml an, um eine JAR-Datei des Adapters zu kompilieren und vorzubereiten. Ant-Binärdateien sind erforderlich, um build.xml zu verwenden. Verwenden Sie "Ant", um die Ziele in build.xml auszuführen, um die JAR-Dateien zu kompilieren und zu erstellen. Halten Sie build.xml mit Ihrem Quellordner (src) zusammen. Die build.properties-Datei ist optional. Weitere Informationen über Ant-Binärdateien finden Sie in der Ant-Hilfe.

Die JAT-Datei ist erfolgreich kompiliert.

Konfigurieren Sie den neuen anwenderspezifischen Suchadapter mit der Komponente "CAFedSearch"

Konfigurieren Sie die JAR-Datei für den neuen anwenderspezifischen Suchadapter mit der Komponente "CAFedSearch" für das Erstellen der CA SDM-Suchquellen.

Gehen Sie wie folgt vor:

1. Kopieren Sie die JAR-Datei vom Speicherort "dist\lib" (in "Kompilieren der JAR-Dateien des neuen anwenderspezifischen Adapters" erstellt) in das folgende CA SDM-Verzeichnis:

```
%NX_ROOT%\bopcfg\www\CATALINA_BASE_FS\webapps\cafedsearch\WEB-INF\lib
```

2. Navigieren Sie zum folgenden CA SDM-Verzeichnis:
\$NX_ROOT\sample\cafedsearch\
3. Erstellen Sie eine neue XML-Vorlagendatei für den anwenderspezifischen Suchadapter. Zum Beispiel die Datei "XYZ-tmpl.xml".
4. Die Vorlagendatei enthält Folgendes:

```
<?xml version="1.0" encoding="UTF-8"?>

<beans default-autowire="byName"
xsi:schemaLocation="http://www.springframework.org/schema/beans
http://www.springframework.org/schema/beans/spring-beans-2.5.xsd
http://cxf.apache.org/core
http://cxf.apache.org/schemas/core.xsd
http://cxf.apache.org/jaxrs
http://cxf.apache.org/schemas/jaxrs.xsd"
xmlns:cxf="http://cxf.apache.org/core"
xmlns:jaxrs="http://cxf.apache.org/jaxrs"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns="http://www.springframework.org/schema/beans">

    <bean autowire="autodetect"
        class=" com.abc.xyz.XYZAdapter "
        id="XYZAdapterConfiguration" scope="singleton">
        <property name="username" value="$(xyz_username)"/>
        <property name="password" value="$(xyz_password)"/>
    </bean>

    <bean autowire="autodetect" class="com.abc.xyz.XYZAdapter"
id="XYZSearchAdapter" init-method="init" destroy-method="destroy"
depends-on="XYZAdapterConfiguration">
```

```
        <property name="config"
ref="OpenSpaceAdapterConfiguration" />
    </bean>
</beans>
```

5. Sie können Eigenschaftswerte erstellen, die auf den Eingabewerten basieren, die für Suchadapter in Schritt 4 angegeben wurden.

Fügen Sie "xyz_username" und "xyz_password" in der Datei "adapters.properties" hinzu, und geben Sie Werte zur Eigenschaft an.

6. Führen Sie die Hilfsprogrammdatei aus, um die XML-Konfigurationsdatei für anwenderspezifische Suchadapter zu generieren:

```
fs_adapters_cli -i -k XYZ -b XYZSearchAdapter -t "XYZ-tmpl.xml " -o "xyz.xml"
```

7. Die Datei "xyz.xml" wird erstellt und in der Datei "adapters-config.xml" registriert.

8. Kopieren Sie die Dateien "xyz.xml" und "adapters-config.xml" in folgendes CA SDM-Verzeichnis:

```
$NX_ROOT\samples\cafedsearch\WEB-INF
```

9. Führen Sie den folgenden Befehl aus, um verbundene Tomcat-Dienste neu zu starten:

```
pdm_tomcat_nxd -c STOP -t FS
pdm_tomcat_nxd -c START -t FS
```

10. Erstellen Sie die föderierten Suchquellen für den XYZ-Adapter in der CA SDM-Benutzeroberfläche.

Weitere Informationen zu föderierten Suchquellen finden Sie unter [Föderierte Suchquellen in CA SDM erstellen](#) (siehe Seite 166).

11. Navigieren Sie in CA SDM zur Registerkarte Knowledge Management. Aktivieren Sie das Kontrollkästchen "XYZ", und führen Sie Suchvorgänge aus.

Der neue anwenderspezifische Suchadapter wird erfolgreich mit der CAFedSearch-Komponente konfiguriert.

Verifizieren des neuen anwenderspezifischen Suchadapters

Verifizieren Sie die Funktionalität Ihres neuen anwenderspezifischen Suchadapters durch die Verwendung des REST-Clients.

Gehen Sie wie folgt vor:

1. Laden Sie den REST-Client aus dem Internet herunter:

<https://code.google.com/p/rest-client/>

2. Starten Sie den Client mithilfe von Java (JRE ist erforderlich).
3. Geben Sie die folgende URL in die Benutzeroberfläche des REST-Clients ein:

```
http://sdmhostname:<FS_Tomcat_Port>/cafedsearch/sdm/search?q=search&userid=<sdmuserid>&source=<Adapter Name>
```

4. Schalten Sie den CA SDM-Sicherheits-Interceptor aus. Öffnen Sie die folgende Datei zum Bearbeiten, und kommentieren Sie den Abschnitt "<jaxrs:inInterceptors>" aus:

\$NX_ROOT\bopcfg\www\CATALINA_BASE_FS\webapps\cafedsearch\WEB-INF\beans.xml

Hinweis: Das Ausschalten des Sicherheitsfilters wird in der Produktionsumgebung nicht empfohlen. Schalten Sie den Sicherheitsfilter in einer Testumgebung aus, um die neue anwenderspezifische Suchadapterfunktionalität zu verifizieren.

5. Prüfen Sie, ob der neue anwenderspezifische Suchadapter ordnungsgemäß funktioniert. Wenn keine Suchergebnisse angezeigt werden, versuchen Sie, die Protokolle zu überprüfen, oder erhöhen Sie die Protokollebene auf "Debuggen".

Hinzufügen des Cross-Origin Resource Sharing-Filters (CORS)

Die Funktion der föderierten Suche wird auf der Webclient-Schnittstelle konfiguriert, wenn der Cross-Origin Resource Sharing-Filter (CORS) zur Webbenutzeroberfläche und zum Tomcat der Föderierten Suche (FS) hinzugefügt wird. Dieser Filter ermöglicht es Ihnen, eine Liste von ursprungsübergreifenden Requests hinzuzufügen. Standardmäßig wird die Webbenutzeroberflächeneinstellung auf "*" gesetzt, was bedeutet, dass alle ursprungsübergreifenden Requests zulässig sind, egal ob sie sich auf den gleichen oder auf einen anderen Ursprung beziehen. Es wird empfohlen, dass Sie diese Einstellung mit einer Liste von für Ihre Umgebung konfigurierte CA SDM-Weboberflächen-Server weiter einschränken.

Um die Einstellungen des Webbenutzeroberflächen-Clients zu bearbeiten und ursprungsübergreifende Requests zu erlauben, gehen Sie wie folgt vor:

Gehen Sie wie folgt vor::

1. Navigieren Sie zum folgenden CA SDM-Verzeichnis, um die Webbenutzeroberflächen-Einstellungen zu bearbeiten:

`$NX_ROOT\bopcfg\www\CATALINA_BASE_FS\webapps\cafedsearch\WEB-INF\web.xml`
2. Öffnen Sie die Datei "web.xml" und überprüfen Sie Folgendes:

`<web-app><filter><init-param><param-name>cors.allowOrigin</param-name>`
3. Aktualisieren Sie den `<param-value>`-Tag mit einer durch Leerzeichen getrennten Liste von Domänen. Zum Beispiel die Basis-URL-Adresse für die Webbenutzeroberfläche:

`<param-value>http://web01:8080 http://web02:8080
http://web03:8080</param-value>`
4. Speichern Sie die Datei "web.xml". Tomcat wird automatisch neu gestartet.
5. Testen und prüfen Sie die Konfiguration der föderierten Suche auf der Webclient-Schnittstelle. Stellen Sie sicher, dass sie funktioniert.
6. Nehmen Sie die gleichen Aktualisierungen an der Datei web.xml.tpl vor, damit die Aktualisierungen an der Webbenutzeroberfläche bestehen bleiben, nachdem die CA SDM-Konfiguration ausgeführt wurde.

Abrufen des Servlets "CAFedSearch" mithilfe von REST

Das Servlet "CAFedSearch" stellt eine RESTful-Schnittstelle bereit, an die anwenderspezifische Such-Clients, Programme und Benutzeroberflächen (UI) die Suchanfragen senden können.

Diese RESTful-Schnittstelle akzeptiert nur die "HTTP Collection GET"-Requests nach der "OpenSearch"-Spezifikation. Die Unterstützung für JSON- und XML-Antworten wird bereitgestellt. Jede Request muss ein BOPSID-Token von Service Desk enthalten, das über CA SDM RESTful- oder SOAP-Webservices abgerufen werden kann.

Gehen Sie wie folgt vor:

1. Rufen Sie ein BOPSID-Token mithilfe der CA SDM RESTful-Webservices ab.
2. Rufen Sie einen REST-Zugriffsschlüssel ab, indem Sie einen HTTP POST-Request auf der "rest_access"-Ressource zusammen mit den Anmeldeinformationen senden.

Sie können auch ein BOPSID-Token mithilfe des REST-Zugriffsschlüssels abrufen, indem Sie einen HTTP POST-Request auf der "bopsid"-Ressource senden.

3. Weitere Informationen über das Senden von Requests an CA SDM RESTful-Webservices finden Sie in den Beispieldateien im folgenden CA SDM-Verzeichnis:

`NX_ROOT\samples\sdk\rest\java`

4. Um die API der föderierten Suche für die Suche zu verwenden, senden Sie einen HTTP GET-Request auf der Suchressource, und übergeben Sie die Suchkriterien und das BOPSID-Token über die CA SDM-URL.
GET

`http://<sdmhostname>:<FS_TOMCAT_PORT>/cafedsearch/sdm/search?q=<searchTerms>&source=<adapterName>&BOPSID=<bopsidToken>&userid=<userId>`

searchTerms

Gibt eine durch Leerzeichen getrennte Liste von Schlüsselwörtern an. Muss URL-codiert sein.

adapterName

Gibt einen Suchmaschinennamen wie im Feld für den Datensatz der Suchquelle an, indem das Konfigurationshilfsprogramm des Adapters angegeben wird.

Andere unterstützte Argumente sind Folgende:

index

Gibt den ersten Index an, der in den Suchergebnissen erforderlich ist. Dies muss eine Ganzzahl ≥ 1 sein.

page

Gibt die erste Seite an, die in den Suchergebnissen erforderlich ist. Dies muss eine Ganzzahl ≥ 1 sein.

size

Gibt die Anzahl der Ergebnisse pro Seite an, die für den Such-Client erforderlich ist.

type

Zu den gültigen Werten gehören "JSON" oder "XML".

Kapitel 7: Richtlinie zur Implementierung:

Dieses Kapitel enthält folgende Themen:

[Implementieren von Richtlinien](#) (siehe Seite 199)

Implementieren von Richtlinien

Eine wesentliche Komponente für die Konfiguration Ihres Service Desk ist die Implementierung von Richtlinien in einer Weise, die Ihrem Geschäftsprozess am besten entspricht.

CA SDM stellt für eine vordefinierte Implementierung von Richtlinien zur Verfügung, die für einige Standorte geeignet ist und als gute Ausgangsbasis für andere dient. Überprüfen Sie die Standard-Implementierung in allen Bereichen der Richtliniendefinitionen, um festzustellen, welche Teile Ihre Bedürfnissen bereits entsprechen und welche Teile Sie anpassen müssen.

Benachrichtigungen

Mit CA Service Desk Manager können Sie Mitarbeiter in Schlüsselpositionen automatisch von Ticketaktivitäten (Nachforschen, Eskalieren) und Events (z. B. Öffnen eines Tickets) benachrichtigen. Sie können auch Schlüsselpersonal von Knowledge-Berichtskarte (KRC) und Support-Automatisierung-Unterstützungssitzungen benachrichtigen. Wenn eine wichtige Aktivität oder ein wichtiges Event auftritt, erzeugt CA Service Desk Manager eine Benachrichtigungsmeldung, die Folgendes ausführt:

- Identifizieren der Ticketaktivität oder des Events
- Verweisen auf das Ticket
- Einschließen weiterer optionaler Informationen
- Identifizieren potenzieller Kontakte

Sie können eine Benachrichtigungsmeldung für ein Ticket aufgrund einer Systemfunktion anzeigen. Eine Systemfunktion schließt das Öffnen, Schließen oder Ändern eines Tickets über seine Verlaufsinformationen ein.

Zum Einrichten von automatischen Benachrichtigungen gehören folgende Aufgaben:

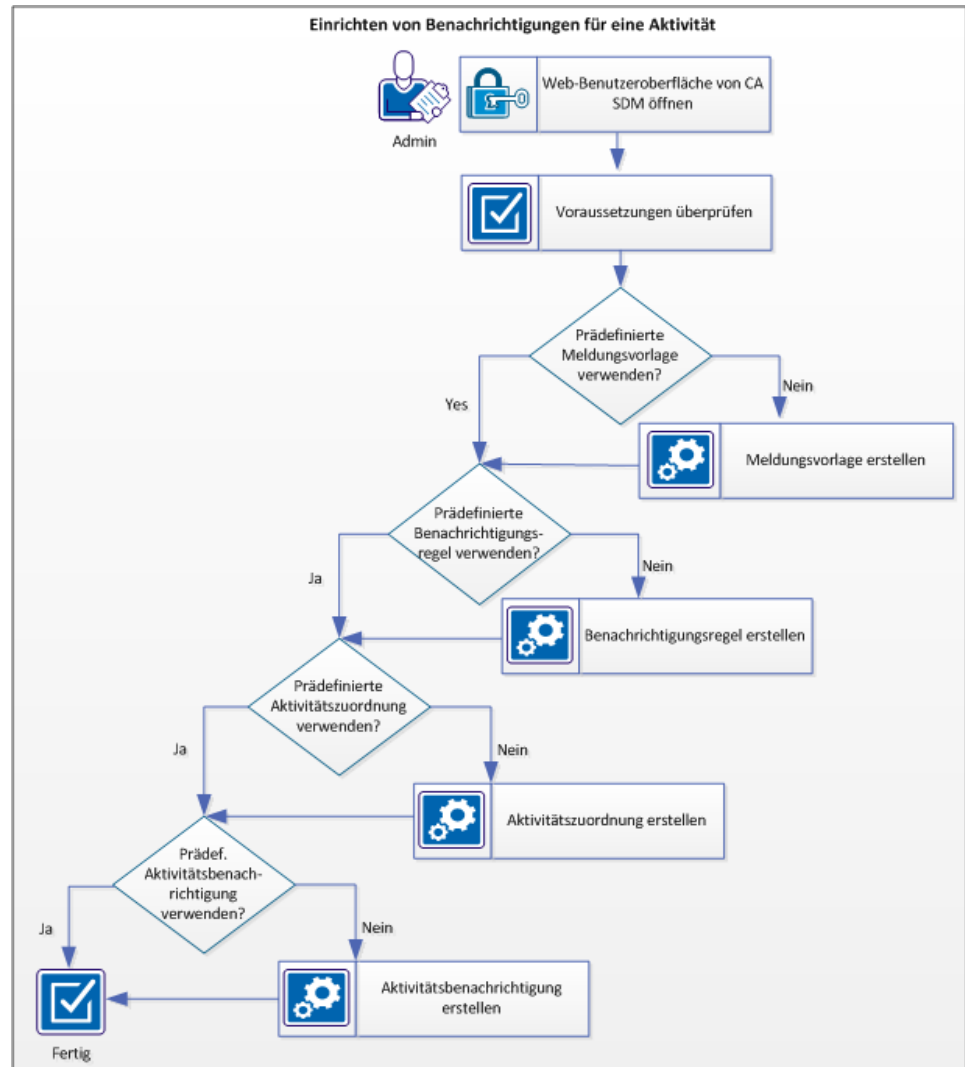
- Definieren von Aktivitätsbenachrichtigungen, die die Arten von Aktivitäten bestimmen, welche Benachrichtigungen erzeugen.

- Definieren von Objektkontaktbenachrichtigungen, die die Art von Objekten bestimmen, die zum Senden von Benachrichtigungen in einer Aktivitätsbenachrichtigung verwendet werden können.
- Identifizieren der zum Senden der Nachrichten verwendeten Methoden.

So richten Sie Benachrichtigungen für eine Aktivität ein

Sie können eine Benachrichtigung definieren, die für eine bestimmte Aktivität gesendet wird. Eine Aktivität ist eine von einer Person durchgeführte Aktion, z. B. das Lösen eines Tickets, das Senden einer verwalteten Umfrage, das Ausführen einer Knowledge-Berichtskarte usw. Sogar tägliche Aktivitäten wie z. B. ein Rückruf, Abrechnen oder Schließen eines Datensatzes, Erhöhen der Priorität oder Aktualisieren eines Status können dazu führen, dass eine Benachrichtigung gesendet wird.

Folgendes Diagramm zeigt, wie Sie Benachrichtigungen für eine Aktivität einrichten:



Gehen Sie wie folgt vor:

1. [Öffnen Sie die CA SDM-Web-Benutzeroberfläche](#) (siehe Seite 202).
2. [Überprüfen Sie die Voraussetzungen](#) (siehe Seite 202).
3. Wenn Sie keine vordefinierte Meldungsvorlage verwenden möchten, [erstellen Sie eine Meldungsvorlage](#) (siehe Seite 205).
4. Wenn Sie keine vordefinierte Benachrichtigungsvorlage verwenden möchten, [erstellen Sie eine Benachrichtigungsvorlage](#) (siehe Seite 208).

5. Wenn Sie keine vordefinierte Aktivitätszuordnung verwenden möchten, [erstellen Sie eine Aktivitätszuordnung](#) (siehe Seite 210).
6. Wenn Sie keine vordefinierte Aktivitätsbenachrichtigung verwenden möchten, [erstellen Sie eine Aktivitätsbenachrichtigung](#) (siehe Seite 210).

Öffnen der CA SDM-Web-Benutzeroberfläche

Melden Sie sich in der Web-Benutzeroberfläche aus folgenden Servern an, abhängig von Ihrer CA SDM-Konfiguration:

- Konventionell: Primärserver oder Sekundärserver
- Erweiterte Verfügbarkeit: Anwendungsserver oder Hintergrundserver

Überprüfen der Voraussetzungen

Überprüfen Sie folgende Voraussetzungen, bevor Sie das Setup durchführen:

- [Die Option zum Hinzufügen der URL in der Benachrichtigung ist installiert](#) (siehe Seite 202).
- [Die Benachrichtigungsmethode für den Empfänger ist bestätigt](#) (siehe Seite 203).
- Wenn Sie eine manuelle Benachrichtigung einer E-Mail-Adresse senden möchten, die mit keinem Kontakt verknüpft ist, dann [erlauben Sie temporäre E-Mail-Adressen](#) (siehe Seite 203)

Installieren der Option zum Hinzufügen der URL in der Benachrichtigung

Das Feld "web_url" in den Tabellen "Change_Request" und "Workflow_Task" enthält einen URL-Wert, der einem Anwender den Zugriff auf einen bestimmten Change oder eine bestimmte Workflow-Aufgabe über die Web-Schnittstelle erlaubt. Bei der Verwendung in E-Mail-Benachrichtigungen kann der Anwender einfach auf die URL klicken und ohne weitere Abfragen direkt zur Web-Schnittstelle gehen.

Bevor Sie die URL-Hyperlinks in Benachrichtigungen implementieren können, müssen Sie das System folgendermaßen konfigurieren:

1. Installieren Sie und konfigurieren Sie die CA SDM Web-Schnittstelle. Weitere Informationen zur Konfiguration der CA SDM-Web-Benutzeroberfläche finden Sie im *Implementierungshandbuch*.
2. Konfigurieren und installieren Sie die Option „web_cgi_url“ mit dem Optionsmanager, um den Speicherort der Web-Engine von CA SDM anzugeben. Zum Beispiel: `http://hostname/scripts/pdmcgi.exe`. Bei der Konfiguration für erweiterte Verfügbarkeit sollte der Hostname auf den Anwendungsserver oder auf den Lastenausgleich verweisen.

Bestätigen der Benachrichtigungsmethode für den Empfänger

Stellen Sie sicher, dass der Kontakt, dem Sie die Benachrichtigung senden möchten, zu dieser bestimmten Benachrichtigungsmethode zugewiesen ist.

Gehen Sie wie folgt vor:

1. Wählen Sie auf der Registerkarte "Administration" die Option "Sicherheit und Rollenverwaltung" > "Kontakte".
Die Seite "Kontakt - Suche" wird geöffnet.
2. Suchen Sie mithilfe des Filters nach dem Kontakt, und wählen Sie aus dem Suchergebnis den Kontakt aus, den Sie benachrichtigen möchten.
Die Seite der Kontaktdetails wird geöffnet.
3. Wählen Sie Benachrichtigung auf der Registerkarte Kontaktdetails aus.
4. Bestätigen Sie die Benachrichtigungsmethode. Wählen Sie basierend auf Ihrer Benachrichtigungspriorität die erforderliche Option aus. Zum Beispiel möchten Sie eine E-Mail-Benachrichtigung für Notfallbenachrichtigungen senden. Aktivieren Sie die Option E-Mail im Feld Notfall.
5. Um die Benachrichtigungsmethode zu ändern, klicken Sie auf Bearbeiten, ändern Sie die Option, und klicken Sie auf Speichern.
Die Benachrichtigungsmethode für den Kontakt wird überprüft.

Zulassen von temporären E-Mail-Adressen

Eine vorübergehende E-Mail-Adresse ist eine Adresse, die keinem Kontakt im System zugeordnet ist. Vorübergehende E-Mail-Adressen sind bei Umständen wie dem folgenden nützlich:

- Ein Endanwender ist nicht im Büro oder hat Schwierigkeiten, auf sein Standard-E-Mail-Konto zuzugreifen.
- Der Analyst möchte E-Mails verwenden, um Interaktionen mit dem Anwender nachzuverfolgen.

- Der Analyst sendet eine manuelle Benachrichtigung an eine *temporäre* E-Mail-Adresse für den Anwender.
- Der Analyst kann das Aktivitätsprotokoll anzeigen, das mit der manuellen Benachrichtigung aktualisiert wird.

Die Empfänger können nicht auf temporäre Adressen nicht antworten, wenn ihre E-Mail-Adresse keinem Kontaktdatensatz zugeordnet ist oder sie nicht über die Berechtigung verfügen, das Ticket zu aktualisieren.

Hinweis: Temporäre E-Mail-Adressen sind immer SMTP-E-Mail-Adressen. Sie werden nur unterstützt, nur wenn die bevorzugte Methode SMTP unterstützt. Informationen zum Einrichten von temporären E-Mail-Adressen finden Sie in der *Online-Hilfe*.

Gehen Sie wie folgt vor:

1. Wählen Sie auf der Registerkarte "Administration" die Option "Optionsmanager", "Benachrichtigungen".
Die Seite Optionen - Liste wird geöffnet.
2. Klicken Sie auf "notification_allow_temp_address".
Die Seite mit den Optionsdetails zu "notification_allow_temp_address" wird geöffnet.
3. Klicken Sie auf "Bearbeiten".
4. Klicken Sie auf "Installieren".
Die Seite mit den Optionsdetails zu "notification_allow_temp_address" wird geöffnet.
5. Klicken Sie auf "Fenster schließen".
6. Starten Sie die CA SDM-Server neu. Weitere Informationen darüber, wie Sie abhängig von Ihrer CA SDM-Konfiguration den CA SDM-Server starten, finden Sie im Szenario "*Neustart der CA SDM-Server*", oder suchen Sie die Informationen im *Administrationshandbuch*.
Temporäre E-Mail-Adressen werden jetzt für manuelle Benachrichtigungen erlaubt.

Erstellen von Meldungsvorlagen

Erstellen Sie eine Meldungsvorlage, die die Werte für die Verwendung der Benachrichtigung enthält. Wenn Sie mehrere Benachrichtigungen senden, können Sie mithilfe der Meldungsvorlagen Ihre Auslastung vereinfachen.

Hinweis: Wenn die Mandantenfähigkeit installiert ist, wählen Sie in der Dropdown-Liste den entsprechenden Mandanten aus. Mit der Option "öffentlich (freigegeben)" wird das Objekt für alle Mandanten erstellt.

Gehen Sie wie folgt vor:

1. Wählen Sie Benachrichtigungen, Meldungsvorlagen in der Registerkarte "Administration" aus.

Die Seite "Meldungsvorlagen - Liste" wird geöffnet.

2. Klicken Sie auf "Neu erstellen".

Die Seite "Neue Meldungsvorlage erstellen" wird angezeigt.

3. Füllen Sie die Felder nach Wunsch aus.

Symbol

Definiert ein eindeutiges Kennzeichen für diese Meldungsvorlage.

Objekttyp

Gibt den Objekttyp an, der mit dieser Vorlage verknüpft ist. Wählen Sie zum Beispiel Request/Incident/Problem für eine Benachrichtigung aus, die sich auf ein Ticket bezieht.

Datensatzstatus

Gibt den Status der Vorlage entweder als aktiv oder inaktiv an. Legen Sie den Status auf Aktiv fest, um die Meldungsvorlage zu verwenden.

Automatische Benachrichtigung

Gibt an, dass die Benachrichtigung, die mit dieser Vorlage verknüpft ist, automatisch gesendet wird, wenn die Aktivität auftritt. Angenommen, Sie richten eine Anfangsbenachrichtigung, die zu benachrichtigenden Objekte und die Meldungsvorlage ein, möchten aber noch nicht die Benachrichtigungen aktivieren. In diesem Fall aktivieren Sie nicht "Automatische Benachrichtigung". Wenn Sie zum Starten von automatischen Benachrichtigungen bereit sind, aktivieren Sie das Kontrollkästchen. Die Benachrichtigung wird aktiviert und erfolgt wie definiert.

Benachrichtigungsebene

Zeigt die relative Gewichtung dieser Benachrichtigung an. Wählen Sie zum Beispiel "Notfall" aus, wenn die E-Mail-Benachrichtigung sofort an den Kontakt gesendet werden soll, wenn die verknüpfte Aktivität auftritt.

Titel der Benachrichtigungsmeldung

Gibt den Zusammenfassungstitel der Meldung an. Sie können Variablen verwenden, um die Incident-Nummer im Meldungstitel einzufügen. Zum Beispiel: @{call_req_id.type.sym} @{call_req_id.ref_num} @{type.sym}.

Benachrichtigungstext

Gibt den Inhalt der Meldung an. Sie können Variablen verwenden, um den Analystnamen, den Namen des Endanwenders und die Beschreibung in die Meldung einzufügen. Beispiel:

@{call_req_id.type.sym} @{call_req_id.ref_num} @{type.sym}.

Zugewiesen zu: @{call_req_id.assignee.combo_name}

Kunde: @{call_req_id.customer.combo_name}

Beschreibung: @{call_req_id.description}

Klicken Sie zum Anzeigen auf die folgende URL:

@{call_req_id.web_url}

Sie können das ARTEFAKT-Schlüsselwort benutzen, um anzugeben, wie Artefakte in ausgehenden Meldungen, Meldungsvorlagen, Benachrichtigungen und automatischen Antworten gehandhabt werden. Das ARTEFAKT-Schlüsselwort benutzt die folgenden Werte:

- **NONE:** Gibt an, dass Artefakte nicht validiert werden. Dieser Wert ist der gleiche, als ob Sie kein Schlüsselwort benutzen.
- **PROTECTED:** Tickets werden zur Bestätigung auf das Vorhandensein der Raute validiert. Wenn die Bestätigung scheitert, wird das Artefakt als ungültig angesehen, und das Filtern schlägt fehl, wenn das Filter die Suche nach einem Artefakt ({{object_id}}) bedeutet.
- **SICHER** - Entschlüsselt die Ticketnummer. Wenn der Wert kein gültiges Kennwort ist, wird das Artefakt als ungültig angesehen, und das Filtern schlägt fehl, wenn das Filtern die Suche nach einem Artefakt ({{object_id}}) bedeutet.

HTML-Meldung

Gibt die HTML-Meldung an, die dem Empfänger angezeigt wird. Wenn der Empfänger die Meldung auf einem Mobilgerät, wie z. B. einem Handy oder PDA, erhält, wird sie im Nur-Text-Format angezeigt. Klicken Sie auf HTML-Meldung bearbeiten, um den HTML-Editor zu öffnen.

Schnellansicht

Zeigt die Meldung an, wie sie für den Empfänger angezeigt wird.

HTML-Quelle

Zeigt die Meldung im HTML-Quellcode an.

4. Klicken Sie auf "Speichern".

Die Meldungsvorlage wird erstellt.

Erstellen von Benachrichtigungsregeln

Erstellen Sie die Benachrichtigungsregel, um die Kontakte anzugeben, die unter bestimmten Umständen benachrichtigt werden sollen.

Hinweis: Wenn die Mandantenfähigkeit installiert ist, wählen Sie in der Dropdown-Liste den entsprechenden Mandanten aus. Mit der Option "öffentlich (freigegeben)" wird das Objekt für alle Mandanten erstellt.

Gehen Sie wie folgt vor:

1. Wählen Sie Benachrichtigungen, Benachrichtigungsregeln in der Registerkarte "Administration" aus.

Die Seite "Benachrichtigungsregeln - Liste" wird angezeigt.

2. Klicken Sie auf "Neu erstellen".

Die Seite "Neue Benachrichtigungsregel erstellen" wird geöffnet.

3. Füllen Sie die folgenden Felder aus:

Symbol

Definiert eine eindeutige Kennung für diese Benachrichtigungsregel. Geben Sie zum Beispiel "Aktualisierung der Ticket-Beschreibung" ein.

Objekttyp

Definiert das Objekt, für das die Regel gilt. Wählen Sie zum Beispiel Request/Incident/Problem für eine Aktivität aus, die sich auf ein Ticket bezieht.

4. Klicken Sie auf "Speichern und Fortfahren".
5. Klicken Sie auf "Bedingung", um das Makro auszuwählen, das Sie verwenden können, um eine Bedingung für diese Regel zu definieren. Führen Sie eine der folgenden Aktionen aus, um die Bedingung zu definieren:

Hinweis: Bei einer Benachrichtigungsregel ohne Bedingungen werden bei jedem Auftreten der Aktivität alle Kontakte benachrichtigt.

- Suchen Sie in der Liste nach dem Makro, und wählen Sie es aus.
- Klicken Sie auf "Neu erstellen", um ein Makro zu erstellen.

6. Klicken Sie auf "Meldungsvorlage", um eine Meldungsvorlage hinzuzufügen, die Sie für diese Regel erstellt haben. Führen Sie einen der folgenden Schritte aus:

- Suchen Sie in der Liste nach der Vorlage, und wählen Sie sie aus.
- Klicken Sie auf "Neu erstellen", um eine Meldungsvorlage zu erstellen.

7. Wählen Sie die zu benachrichtigenden Kontakte auf den folgenden Registerkarten aus:

Hinweis: Mit der Schaltfläche "Kontakte aktualisieren" auf jeder Registerkarte können Sie weitere Kontakte für die Benachrichtigung suchen und auswählen.

Objektkontakte

Zeigt die verfügbaren Organisationen, Anbieter und Configuration Items für den ausgewählten Objekttyp an, die eine Benachrichtigung zu Tickets erhalten. Zum Beispiel können Sie Betroffener Endanwender oder Admin. Org. des betroffenen Endanwenders für die Benachrichtigung auswählen.

Kontakte

Zeigt die Personen an, die der Benachrichtigungsregel hinzugefügt sind, unabhängig von ihrer Zuordnung zum Ticket.

Kontakttypen

Zeigt die Anwender an, die innerhalb der Benachrichtigungsregel mit der gleichen Klassifizierung definiert sind, z. B. Analysten oder Kunden.

8. Klicken Sie auf "Speichern".

Die Benachrichtigungsregel wird erstellt.

Erstellen von Aktivitätszuordnungen

Ordnen Sie dem Objektattribut eine Aktivität zu, um die Änderungen am zugehörigen Objektattribut zu verfolgen. Ordnen Sie zum Beispiel die Aktivität "Feldaktualisierung" dem Objektattribut des Felds "Beschreibung" eines Incident-Datensatzes zu. Dies ermöglicht es Ihnen, eine Benachrichtigung zu senden, sobald die Beschreibung des Incidents aktualisiert ist. Ein Objektattribut kann nur eine Aktivitätsbenachrichtigung erhalten.

Hinweis: Wenn die Mandantenfähigkeit installiert ist, wählen Sie in der Dropdown-Liste den entsprechenden Mandanten aus. Mit der Option "öffentlich (freigegeben)" wird das Objekt für alle Mandanten erstellt.

Gehen Sie wie folgt vor:

1. Wählen Sie auf der Registerkarte "Administration" die Option "Benachrichtigungen", "Aktivitätszuordnungen".
Die Seite Aktivitätszuordnungen - Liste wird geöffnet.
2. Klicken Sie auf "Neu erstellen".
Die Seite "Neuen Aktivitätszuordnungstyp erstellen" wird geöffnet.
3. Füllen Sie die folgenden Felder aus:

Symbol

Definiert ein eindeutiges Kennzeichen für diese Zuordnung.

Code

Definiert einen internen Code für die Aktivitätszuordnung.

Objekttyp

Legt den Namen des Objekts fest, für das das Attribut gilt. Wählen Sie zum Beispiel Request/ Incident/ Problem aus.

Objekttyp-Attribut

Definiert das Objektattribut, mit dem der Aktivitätstyp verknüpft ist. Geben Sie zum Beispiel das Objektattribut des Felds "Beschreibung" eines Incident-Datensatzes ein.

Aktivitätstyp

Gibt den Typ der Aktivität an. Wählen Sie zum Beispiel Feldaktualisierung aus, um zu überprüfen, wann das ausgewählte Objektattribut aktualisiert wird.

Protokoll aufzeichnen

Gibt an, ob diese Aktivitätszuordnung einen Eintrag im Audit-Protokoll anlegt.

4. Klicken Sie auf "Speichern".
Die Seite "Aktivitätszuordnungstyp - Detail" wird geöffnet.
5. Klicken Sie auf "Fenster schließen".

Die Aktivitätszuordnung wird erstellt.

Erstellen von Aktivitätsbenachrichtigungen

Ordnen Sie die Aktivität zu einer Benachrichtigung zu. Wenn die Aktivität stattfindet, dann wird die verknüpfte Benachrichtigung an die ausgewählten Kontakte gesendet.

Hinweis: Wenn die Mandantenfähigkeit installiert ist, wählen Sie in der Dropdown-Liste den entsprechenden Mandanten aus. Mit der Option "öffentlich (freigegeben)" wird das Objekt für alle Mandanten erstellt. Es ist nicht möglich, unterschiedliche manuelle Aktivitätsbenachrichtigungen pro Mandant zu verwalten oder eine manuelle Aktivitätsbenachrichtigung zu kopieren.

Gehen Sie wie folgt vor:

1. Wählen Sie Benachrichtigungen, Aktivitätsbenachrichtigungen in der Registerkarte "Administration" aus.

Die Seite Aktivitätsbenachrichtigungen - Liste wird geöffnet.

2. Klicken Sie auf "Neu erstellen".

Die Seite "Neue Aktivitätsbenachrichtigung erstellen" wird geöffnet.

3. Füllen Sie die folgenden Felder aus:

Symbol

Definiert ein eindeutiges Kennzeichen für diese Aktivitätsbenachrichtigung.

Code

Definiert einen internen Code für die Aktivitätsbenachrichtigung.

Aktivität gültig für

Gibt das Objekt an, für das diese Aktivität gilt.

4. Klicken Sie auf "Speichern und Fortfahren".

Die Seite "Aktivitätsbenachrichtigung aktualisieren" wird geöffnet.

5. Füllen Sie die folgenden Felder aus:

Intern

Gibt an, ob die Aktivitätsbenachrichtigung nur für interne Mitarbeiter verfügbar oder auch für Endanwender sichtbar ist.

Datensatzstatus

Gibt an, ob die Aktivitätsbenachrichtigung aktiv oder inaktiv ist. Legen Sie den Status auf "Aktiv" fest, um die Aktivitätszuordnung zu verwenden.

Aktivität der zugehörigen Tickets

Gibt an, ob das Aktivitätsprotokoll auf einem Ticket auf alle zugehörigen Tickets übertragen wird. Die Propagierung des Aktivitätsprotokolls ist nur für zugehörige Incidents, Probleme und Changes gültig.

Hinweis: Wenn Sie die Mandantenfähigkeit verwenden, gehen Sie folgendermaßen vor:

- Geben Sie in der Drop-down-Liste "Aktivität der zugehörigen Tickets" den entsprechenden Mandantentyp an.
- Geben Sie im Mandantenfeld den Namen des Mandanten ein, oder klicken Sie auf das Suchsymbol, um einen Mandanten zu suchen.

Objektyp

Legt den Namen des Objekts fest, für das die Aktivität gilt.

6. Klicken Sie auf der Registerkarte "Benachrichtigungsregeln" auf "Benachrichtigungsregeln aktualisieren". Führen Sie eine der folgenden Aktionen aus:
 - Geben Sie die Suchkriterien ein, klicken Sie auf "Suchen", und wählen Sie die Benachrichtigungsregel aus dem Suchergebnis aus.
 - Klicken Sie auf "Neu erstellen", um eine Benachrichtigungsregel zu erstellen.

7. (Wenn Sie dem Empfänger der Benachrichtigung eine Umfrage senden möchten) Wählen Sie die Registerkarte Umfrage aus, und [definieren Sie eine Umfragebenachrichtigung](#) (siehe Seite 214). Mit Umfragen können Sie Kunden-Feedback erfassen und analysieren. Ein Aktivitätsprotokoll wird generiert, zum einen, wenn eine Umfragebenachrichtigung gesendet wird, und zum anderen, wenn eine Umfrage von einem Kunden empfangen wird.

Hinweis: Die Registerkarte "Umfrage" gilt für alle Objekttypen mit Ausnahme von Knowledge-Dokumenten, Knowledge-Dokumentkommentaren und Knowledge-Berichtskarten. Falls in der Liste der Objekttypen angegeben, wird die Registerkarte "E-Mails" anstelle der Registerkarte "Umfrage" auf der Seite "Aktivitätsbenachrichtigung aktualisieren" angezeigt. Auf der Registerkarte "E-Mails" können Sie nach einer oder mehreren E-Mail-Nachrichten suchen, die mit dieser Benachrichtigung verknüpft werden sollen, oder eine neue Nachricht definieren.

8. (Wenn Sie ein Event auslösen möchten, nachdem die Benachrichtigung gesendet wurde) Wählen Sie die Registerkarte "Events" aus. Ereignisse sind Prozeduren, die nach Ablauf einer bestimmten Zeitspanne durch die Issue-Verwaltung abgearbeitet werden. Wenn die Aktivitätsbenachrichtigung ausgelöst wird, dann treten die ausgewählten Events auf. Aktualisieren Sie zum Beispiel den Status des Incidents auf "Schließen". Suchen Sie nach dem Event, und klicken Sie auf die Schaltfläche Events aktualisieren, um das Event zu einer Aktivitätsbenachrichtigung hinzuzufügen.

9. Klicken Sie auf "Speichern".

Die Seite "Aktivitätsbenachrichtigung - Detail" wird geöffnet.

10. Klicken Sie auf "Fenster schließen".

Der Aktivitätsbenachrichtigung wird erstellt. Wenn ein Fehler auf dem ausgehenden Mail-Server auftritt, werden keine E-Mail-Benachrichtigungen gesendet und in das Warteschlangenverzeichnis "\$NX_ROOT/site/mail_queue" gestellt. Wenn der Mail-Server wieder aktiv wird, verarbeitet und sendet er nach einem gewissen Zeitabstand E-Mails. Sie können die [Variable für das Wiederholungsintervall der E-Mail](#) (siehe Seite 214) festlegen, um die E-Mail wiederzuverwerten, die während der Belegung des Mail-Servers in die Warteschlange gestellt worden war.

E-Mail-Benachrichtigungen, die der ausgehende Mail-Server nicht gesendet hat, werden solange erneut gesendet, bis Sie Folgendes tun:

- Halten Sie den Mail Daemon (pdm_mail_nxd) an, der ausgehende E-Mail-Benachrichtigungen verarbeitet.
- Löschen Sie manuell die Nachrichten aus dem Verzeichnis "\$NX_ROOT/site/mail_queue".

Definieren von Umfragebenachrichtigungen

Füllen Sie die folgenden Felder nach Wunsch aus:

Umfrage senden

Gibt an, ob die Umfrage aktiviert oder deaktiviert werden soll. Wenn Sie dieses Kontrollkästchen aktivieren, wird die Umfrage an den Kontakt gesendet, sobald die markierte Aktivitätsbenachrichtigung ausgelöst wird.

Standardumfrage

Legen Sie eine Standardumfrage über das Suchsymbol fest, oder geben Sie eine eigene Umfrage im Textfeld an.

Titel der Umfragemeldung

Geben Sie den Titel für die Umfrage ein.

Text der Umfragemeldung

Geben Sie eine Nachricht für den Kontakt ein. Wenn ein Anwender die Benachrichtigung von einer Umfrage empfängt, enthält der Meldungstext automatisch eine URL, auf die der Anwender über seinen Webbrowser zugreifen kann, um das Umfrageformular aufzurufen und auszufüllen.

Festlegen der Variablen zu Wiederholungsintervallen für E-Mails

Sie können den Zeitabschnitt (in Sekunden) festlegen, in dem Fehlversuche bei der Übermittlung der E-Mail-Nachricht an den Mail-Server wiederholt werden.

Hinweis: CA SDM versucht nicht, E-Mail-Nachrichten erneut zu senden, wenn der ausgehende Mail-Server die Nachricht erhalten hat, diese jedoch nicht vom Anwender abgerufen werden kann. In diesem Fall werden die Regeln und Richtlinien zur Wiederholung bei Übertragungsfehlern des ausgehenden Mail-Servers angewendet, falls eingerichtet.

Wiederholungen werden jeweils für einzelne Nachrichten durchgeführt. Wenn der Mail-Server für einen Zeitraum nicht verfügbar ist, wird jede Nachricht solange erneut übertragen, wie für sie festgelegt ist. Es wird nicht versucht, alle Nachrichten des Übertragungsvorgangs erneut zu senden. Wenn der Daemon für ausgehende E-Mails wieder verfügbar ist, werden alle noch nicht gesendeten Nachrichten auf einmal übertragen. Schlägt dieser Übertragungsversuch fehl, werden die Zeitgeber für alle Nachrichten auf dieselbe Zeit zurückgesetzt.

Die Einstellung "NX_EMAIL_RETRY_INTERVAL" in der Datei "NX.env" steuert das Wiederholungsintervall. Sie können das Standardwiederholungsintervall auf einem oder mehreren Servern anpassen.

Gehen Sie wie folgt vor:

1. Melden Sie sich abhängig von Ihrer CA SDM-Konfiguration bei folgendem Server an:
 - Konventionell: Primärserver
 - Erweiterte Verfügbarkeit: Hintergrundserver.
2. Wechseln Sie in das Verzeichnis "\$NX_ROOT"
3. Öffnen Sie die Datei "NX.env" in einen Texteditor wie WordPad.
4. Ändern Sie den Wert des Intervalls in "NX_EMAIL_RETRY_INTERVAL" wie folgt:

`NX_EMAIL_RETRY_INTERVAL=number_of_seconds`

NX_EMAIL_RETRY_INTERVAL

Legt den Zeitabschnitt (in Sekunden) fest, in dem Fehlübertragungen von E-Mail-Nachrichten wiederholt werden.

number_of_seconds

Gibt die Anzahl von Sekunden für jedes E-Mail-Wiederholungsintervall an. Der Standardwert ist 600 Sekunden (10 Minuten). Der Minimalwert, den Sie verwenden können, beträgt 20 Sekunden. Wenn Sie einen Wert festlegen, der das Minimum (20 Sekunden) unter- oder 2000000 Sekunden überschreitet, wird der Standardwert von 10 Minuten verwendet.

5. Speichern und schließen Sie die Datei.
6. Starten Sie die CA SDM-Server neu. Weitere Informationen darüber, wie Sie abhängig von Ihrer CA SDM-Konfiguration den CA SDM-Server starten, finden Sie im Szenario "Neustart der CA SDM-Server", oder suchen Sie die Informationen im *Administrationshandbuch*.

Die Änderung wird übernommen.

So erstellen Sie Objektkontaktbenachrichtigungen

Damit können Sie Empfänger anhand des aktuellen Werts in einem Feld im Ticket benachrichtigen. Anstatt eine Person festzulegen, die benachrichtigt werden soll (wie bei einer Benachrichtigungsmethode), geben Sie ein Objekt an. Verwenden Sie beispielsweise das Feld "An", um sicherzustellen, dass diese Benachrichtigung an die Person gesendet wird, die derzeit im Feld "An" festgelegt ist, selbst wenn sich dieser Wert seit der Definition des Tickets geändert hat.

Gehen Sie wie folgt vor:

1. Wählen Sie auf der Registerkarte "Administration" die Optionen "Benachrichtigungen", "Objektkontaktbenachrichtigungen" aus.

Die Seite "Objektkontaktbenachrichtigung - Liste" wird geöffnet.
2. Klicken Sie auf "Neu erstellen".

Die Seite "Neue Objektkontaktbenachrichtigung erstellen" wird angezeigt.

3. Füllen Sie die folgenden Felder aus:

Symbol

Definiert ein eindeutiges Kennzeichen für die Objektkontaktbenachrichtigung.

Status

Gibt an, ob die Objektkontaktbenachrichtigung derzeit aktiv oder inaktiv ist.

Objektyp

Zeigt den Namen des Objekts an, für das Attribut gilt.

Objektattributname

Gibt den Namen der Objektkontaktbenachrichtigung (im Feld "Symbol") in Majic an, der ein interner CA-Code ist. Der Attributname hängt von der Auswahl des Objekttypen ab:

- Beim Objekttyp "Issue" oder "Workflow-Aufgabe" lautet der Attributname "Zuständiger", "Angefordert von" oder "Gruppe". Dies sind die Attributnamen in den chg-Objekten, und sie sind Feldern in den "Change_Request"-Tabellen zugeordnet.
- Ist der Objekttyp ein Issue-Aktivitätsprotokoll, muss der Attributname mit dem Attributnamen in dem Aktivitätsprotokollobjekt beginnen, das ihn mit einer bestimmten Instanzierung des chg-Objekts verknüpft. Der Attributname kann "change_id.group" lauten.

Beschreibung

Beschreibt die Objektkontaktbenachrichtigung.

4. Klicken Sie auf "Speichern".

Die neue Objektkontaktbenachrichtigung wird in "Objektkontaktbenachrichtigungen - Liste" angezeigt.

Hinweis: Weitere Informationen zum Konfigurieren von Objektkontaktbenachrichtigungen finden Sie in der *Online-Hilfe*.

Liste der Empfänger von manuellen Benachrichtigungen

Sie können einen Standardsatz verfügbarer Empfänger einrichten, der die Verfassungsseite für manuelle Benachrichtigungen für Anfragen, Incidents und Probleme aufweist. Verfügbare Empfänger rationalisieren den manuellen Benachrichtigungsprozess für Analysten, da Sie eine Liste mit Kontaktobjekten (zum Beispiel Betroffener Endbenutzer) oder individuelle Kontaktnamen für die einfache Verwendung als Empfänger von manuellen Benachrichtigungen einrichten können.

Durch Hinzufügen eines Objektkontaktempfängers werden die individuellen Kontaktnamen hinzugefügt, die der Objektkontakt für die Empfängerliste darstellt (wodurch doppelte Einträge zusammengeführt werden). Der gleiche Kontakt kann mehrmals für unterschiedliche Kontaktobjekte wie zum Beispiel "Zuständiger" und "Betroffener Endbenutzer" referenziert werden. Einige Einträge wie z. B. das Kontaktobjekt "Beteiligtenliste" können mehrere Einträge zur Empfängerliste hinzufügen.

Kontakte und Kontaktobjekte bleiben in der Liste der verfügbaren Empfänger, nachdem Sie sie zur Liste hinzugefügt haben. Mit diesem Verhalten können Sie Empfänger entfernen, ohne dass die ursprüngliche Liste der verfügbaren Empfänger betroffen ist.

Beispiel: Funktionsweise der Liste der verfügbaren Empfänger

Die folgenden Beispiele zeigen, wie Standardempfänger den manuellen Benachrichtigungsprozess rationalisieren.

"Objektkontaktempfänger" schließt die folgenden Einträge ein:

- UserA gehört zu den Kontaktobjekten "Zuständiger" und "Betroffener Endbenutzer".
- "Beteiligtenliste" schließt mehrere Kontaktnamen ein. Zum Beispiel UserB und UserC.

Sie haben folgende Möglichkeiten:

- Beide Kontaktobjekte hinzufügen, die UserA auf die Empfängerliste verweisen.
Nur ein UserA-Eintrag wird in der Empfängerliste aufgelistet.
- Versehentlich UserA von der Empfängerliste entfernen.

Sie müssen sich nicht auf das Ticket beziehen, um den UserA-Namen zu erhalten, und suchen, um es wieder zurückzuholen. Sie können UserA schnell zur Empfängerliste hinzufügen, da UserA in der Liste der verfügbaren Empfänger aufgelistet wird.

- Versehentlich einen Kontaktnamen, wie z. B. UserC, von der Empfängerliste entfernen, die aus der Beteiligtenliste kam.

Sie können die Beteiligtenliste von Objektkontaktempfängern hinzufügen, um den Kontaktnamen wieder hinzuzufügen. Da doppelte Einträge zusammengefasst werden, sind andere Kontakte in der Beteiligtenliste, die nicht aus der Empfängerliste gelöscht wurden, nicht betroffen.

Benachrichtigungen an vorherige Zuständige

Sie können die Werte "Vorheriger Zuständiger" oder Gruppe" für eine Aktivitätsbenachrichtigung definieren, die Änderungen in Schlüsselfeldern erkennt, wenn ein Ticket gespeichert wird. Mit vorherigen Werten können Sie einen vorherigen Zuständigen benachrichtigen, wenn ein Ticket übertragen wird, oder sowohl die aktuelle als auch die vorherige Gruppe benachrichtigen, wenn die Priorität eines Tickets eskaliert wird.

Die Felder mit vorherigen Werten eines Tickets sind lokale Felder, die nur im Speicher und nicht in der Datenbank existieren. Die Felder werden während des Speichervorgangs eines Tickets aufgefüllt und bei Beendigung des Benachrichtigungsprozesses gelöscht. Ein Feld mit vorherigem Wert ist über eine Aktivitätszuordnung einem bestimmten Aktivitätstyp zugeordnet.

Sie können bisherige Werte definieren, die Änderungen an den folgenden Schlüsselfeldern eines Tickets erkennen:

Feld	Requests, Incidents, Probleme	Changes	Issues
Status	Ja	Ja	Ja
Aktiv	Ja	Ja	Ja
Verantwortlicher	Ja	Ja	Ja
Request-Bereich/Kategorie	Ja	Ja	Ja
Gruppe	Ja	Ja	Ja
Impact	Ja	Ja	Ja
Priorität	Ja	Ja	Ja
Urgency	Ja	No	No
Relevanz	Ja	No	No

Es gibt mehrere Kontakte, die Sie für jeden Objekttyp angeben können (Request, Incident, Problem, Change oder Issue), die die aktuellen und vorherigen Kontakte benachrichtigen, wenn eine Aktivität stattfindet.

- **Zuständiger** - Person, die der Verarbeitung des Tickets zugewiesen ist
- **Vorheriger Zuständiger** - Person, die vorher der Verarbeitung des Tickets zugewiesen war
- **Gruppe** - Gruppe, die der Verarbeitung des Tickets zugewiesen ist
- **Vorherige Gruppe** - Gruppe, die vorher der Verarbeitung des Tickets zugewiesen war

Wenn die Benachrichtigungsregel gespeichert ist, werden die Felder "Vorheriger Zuständiger" und "Vorherige Gruppe" auf der Seite mit der Liste der Benachrichtigungsregeln angezeigt.

Beispiel: Konfiguration von aktuellen und vorherigen Werten für Schlüsselfelder

Das folgende Verwendungsbeispiel beschreibt, wie ein Administrator aktuelle und ältere Werte für Schlüsselfelder konfiguriert, um dabei zu helfen, sicherzustellen, dass der vorherige Support-Mitarbeiter benachrichtigt wird, wenn ein Request durch eine Weiterleitung von Ihnen entfernt wird.

1. **Situation** - Ein Support-Mitarbeiter ist frustriert, da ein Ticket von ihm weg übermittelt wurde und er nicht darüber benachrichtigt wurde.
2. **Aufgabe** - Der Administrator fügt die Objektkontakte "Zuständiger" und "Vorheriger Zuständiger" der Benachrichtigungsregel zur Benachrichtigung über Übertragungsaktivitäten hinzu. Sie hängen eine Meldungsvorlage an und geben auf dem Request-Formular den aktuellen und den vorherigen Zuständigen an, die benachrichtigt werden sollen.
3. **Aktion** - Wenn der Request abgespeichert wird, werden die Felder "Zuständiger" und "Vorheriger Zuständiger" des Request aufgefüllt. Wenn die Aktivität stattfindet (Ticket wird übermittelt), wird die Bedingung für die Regel ausgewertet.
4. **Ergebnis** - Wenn die Bedingung erfüllt wird, wird eine Benachrichtigungsmeldung, die die Ticketaktivität beschreibt, an den aktuellen und den vorherigen Zuständigen geschickt.

Benachrichtigen von Kontakten, wenn ein Ticket übertragen wird (Beispiel)

Sie können sowohl die aktuellen als auch die vorherigen Kontakte benachrichtigen, wenn ein CA SDM-Ticket übertragen wird.

Beispiel: Benachrichtigen der aktuellen und vorherigen Kontakte, wenn ein Ticket übertragen wird

1. Wählen Sie auf der Registerkarte "Administration" die Option "Benachrichtigungen" > "Aktivitätsbenachrichtigungen" aus.
Die Seite "Aktivitätsbenachrichtigungen - Liste" wird angezeigt.
2. Wählen Sie die Aktivitätsbenachrichtigung "Übertragen".
Die Seite "Übertragungsaktivitätsbenachrichtigung - Detail" wird angezeigt.
3. Wählen Sie im Feld "Objekttyp" die Option "Anfragen/Incidents/Probleme".
4. Wählen Sie auf der Registerkarte "Benachrichtigungsregeln" unter "Symbol" die Standardbenachrichtigungsregel aus.
Die Seite "Standardbenachrichtigungsregel" wird geöffnet.
5. Klicken Sie auf der Registerkarte "Objektkontakte" auf "Objektkontakte aktualisieren".
6. Klicken Sie auf "Suche".
Die Seite "Notification Rule Update Recipients" wird angezeigt.
7. Wählen Sie unter "Objektkontakte" in der linken Liste die Einträge "Zuständiger" und "Vorheriger Zuständiger", und klicken Sie auf die Auswahl Schaltfläche (≥>).
Das markierte Element wird in die rechte Liste aufgenommen.
Hinweis: Um mehrere Objektkontakte zu markieren, halten Sie die STRG-Taste oder die Umschalttaste gedrückt, während Sie mit der linken Maustaste klicken.
8. Klicken Sie auf "OK".
9. Speichern Sie die Benachrichtigungsregel.
Die Liste "Objektkontakte" zeigt den markierten Objektkontakt an.
10. Klicken Sie auf der Seite "Standardbenachrichtigungsregel" auf die Option "Meldungsvorlage". Wählen Sie eine Vorlage aus und stellen Sie sicher, dass die Option "Automatische Benachrichtigung" aktiviert ist.
11. Erstellen Sie eine neue Anfrage, geben Sie einen Verantwortlichen an, und klicken Sie auf "Speichern".

12. Wählen Sie auf der Seite "Anfrage - Detail" die Option "Aktivitäten", und wählen Sie dann im Menü "Datei" den Befehl "Übertragen".
13. Geben Sie einen neuen Verantwortlichen an, und klicken Sie auf "Speichern".
Die Benachrichtigung wird an den aktuellen und den vorherigen Zuständigen gesendet, wenn die Übertragung stattfindet.

Benachrichtigungen für Configuration Items

Mit einer Benachrichtigung für Configuration Items (CI) können Sie eine Aktivitätsbenachrichtigung definieren, die einem spezifischen CI zugeordnet ist, welches wiederum einem spezifischen CA SDM-Ticket zugeordnet ist. Diese Funktion ermöglicht Ihnen, Informationen über die Benutzer, Organisationen und Anbieter eines CI nachzuverfolgen.

Sie können die CI-Objektkontakte auf der Seite Benachrichtigungsregeln-Aktualisierungs-Empfängern angeben, wie z. B. Wartungsorganisation des CI, Hauptkontakt des CI usw.

Beispiel für das Benachrichtigen des Hauptkontakts eines Configuration Items über ein Problem

Sie können eine Aktivitätsbenachrichtigung für einen Hauptkontakt definieren, die an ein bestimmtes CI für ein bestimmtes CA SDM-Ticket gesendet wird.

Beispiel: Benachrichtigen des Hauptkontakts eines Configuration Items über ein Issue

1. Wählen Sie auf der Registerkarte "Administration" die Option "Benachrichtigungen" > "Aktivitätsbenachrichtigungen" aus.
Die Seite "Aktivitätsbenachrichtigungen - Liste" wird angezeigt.
2. Wählen Sie aus der Liste die erste Aktivitätsbenachrichtigung aus.
Die Seite "Initial Activity Notification Detail" wird angezeigt.
3. Wählen Sie den Objekttyp aus, den Sie verwenden möchten.
4. Wählen Sie auf der Registerkarte "Benachrichtigungsregeln" die Verknüpfung zur Standardbenachrichtigungsregel aus.
Die Seite "Standardbenachrichtigungsregel" wird geöffnet.
5. Wählen Sie die Verknüpfung zur Standardmeldungsvorlage und stellen Sie sicher, dass die Option "Automatische Benachrichtigung" aktiviert ist.
6. Klicken Sie auf die Registerkarte "Objektkontakte" und dann auf "Objektkontakte aktualisieren".
Die Seite "Objektkontaktbenachrichtigung - Suche" wird geöffnet.
7. Klicken Sie auf "Suche". Es wird eine Liste der Objektkontakte angezeigt.

8. Wählen Sie aus der Liste im linken Bereich den Hauptkontakt des CI aus, und klicken Sie auf die Schaltfläche zur Kontaktauswahl (≥>).

Das markierte Element wird in die rechte Liste aufgenommen.

Um mehrere Objektkontakte zu markieren, halten Sie die STRG-Taste oder die Umschalttaste gedrückt, während Sie mit der linken Maustaste klicken. Sie können ein Objekt für eine Anfrage und mehrere Objekte für einen Change oder ein Issue hinzufügen.

Der Objektkontakt wird in der rechten Liste aufgeführt.

9. Klicken Sie auf "OK".
10. Speichern Sie die Benachrichtigungsregel.

Die Liste "Objektkontakte" zeigt den markierten Objektkontakt an.

11. Führen Sie die folgenden Schritte aus:

- Erstellen CI auf der Registerkarte "Service Desk" oder aktualisieren Sie ein vorhandenes.
- Fügen Sie den primären Kontakt hinzu, der auf der Registerkarte "Objektkontakte" aufgeführt wird. Der markierte Objektkontakt wird auf der Seite "Configuration Items - Detail" angezeigt.
- Fügen Sie dem Issue das CI hinzu.

Wenn ein Aktivitätsereignis auftritt, wird die Regel implementiert und die Bedingung wird ausgewertet. Wenn das Kriterium für die Bedingung erfüllt ist, wird eine Benachrichtigung mit einer Beschreibung der Ticket-Aktivität an alle Kontakte des CI gesendet, das mit der Benachrichtigungsregel verknüpft ist.

Reader für Benachrichtigungsprotokoll

Der Reader für Benachrichtigungsprotokoll zeigt die Benachrichtigungen, die für den angemeldeten Benutzer empfangen wurden, nach Datum, Dringlichkeit und Status an. Mit dem Reader für Benachrichtigungsprotokoll können Sie Folgendes tun:

- Die Sortierreihenfolge ändern und Menüoptionen einstellen, um den Reader für Benachrichtigungsprotokoll automatisch anzuzeigen, wenn neue Nachrichten empfangen werden.
- Auf eine Benachrichtigungsmeldung doppelklicken, um anzufordern, dass CA SDM die Detailseite für das mit der Benachrichtigung verknüpfte Ticket anzeigt.
- Benachrichtigungsmeldungen überwachen, indem Sie bestimmte Auswahlkriterien eingeben, um die Datenbank für die Analyse oder die Auswahl von Benachrichtigungsmeldungen auf der Basis der in den Feldern eingegebenen Daten abzufragen. Zum Beispiel können Sie nur die nicht gelöschten Benachrichtigungsmeldungen auflisten, indem Sie das Feld „Meldungsstatus“ in „Nicht gelöscht“ ändern.

- Benachrichtigungsmeldungen löschen, um Ihre Liste mit Benachrichtigungen auf eine überschaubare Größe zu begrenzen. Wenn Sie den Reader für Benachrichtigungsprotokoll zum ersten Mal aufrufen, werden gelöschte Benachrichtigungen nicht angezeigt. Sie haben aber die Möglichkeit, gelöschte Benachrichtigungen anzuzeigen, wenn dies nötig ist.

Einstellen der Optionen für den Reader für Benachrichtigungsprotokolle

Sie können Optionen für den Reader für Benachrichtigungsprotokolle einstellen um festzulegen, wie Sie beim Eingang neuer Nachrichten benachrichtigt werden.

So stellen Sie die Optionen für den Reader für Benachrichtigungsprotokolle ein:

1. Navigieren Sie auf der Registerkarte "Service Desk" zu "Ansicht" und dann zu "Protokoll-Reader".

Die Seite des Readers für Benachrichtigungsprotokolle wird angezeigt.

2. Aktivieren Sie das Kontrollkästchen links von jeder Benachrichtigung, um die weiter unten aufgeführten Optionen einzustellen. Sie können Elemente auswählen, um Vorgänge durchzuführen, z. B. "Auswahl löschen" oder "Auswahl löschen".

Kopf

Zeigt die Kopfzeile der Meldung. Sie enthält üblicherweise die Nummer des Tickets und den Aktivitätstyp.

Startdatum

Zeigt das Datum und die Uhrzeit an, zu der die Benachrichtigung an Ihr Protokoll-Reader-Fenster gesendet wurde.

Status

Zeigt den Status der Benachrichtigung an.

Urgency

Legt die Dringlichkeitsstufe für die Benachrichtigung (niedrig, normal, hoch oder Notfall) fest, welche die relative Wichtigkeit von verschiedenen Aktivitäten angibt. Dringlichkeitsstufen sind vordefiniert; der Systemadministrator ist jedoch verantwortlich für die Einstellung anderer Aspekte der Benachrichtigung wie z. B. der Benachrichtigungsmethode und der Aktivitätszuweisung. Der Systemadministrator legt auch die Benachrichtigungsmethode fest, die für Kontakte und Gruppen auf jeder Dringlichkeitsstufe verwendet wird.

Benachrichtigungstext

Der volle Benachrichtigungstext für die Benachrichtigung.

Der Protokoll-Reader zeigt eventuelle Änderungen an.

3. Klicken Sie auf "Schließen".

Die Seite des Readers für Benachrichtigungsprotokolle wird geschlossen und die Optionen sind eingestellt.

Personalisierte Antworten

Diese personalisierten Antworten können beim Hinzufügen von Aktivitäten zum Datensatz erstellt und an die Datensätze für Anfragen, Issues und Changes angehängt werden. Zum Beispiel können Sie in den Fenstern "Statusänderung" oder "Protokollkommentar", die aus dem Menü "Aktivitäten" aufgerufen werden können, personalisierte Antworten ergänzen.

Erstellen einer personalisierten Antwort

Sie können eine personalisierte Antwort erstellen, die Anfragen, Issues und Change-Datensätzen hinzugefügt wird.

So erstellen Sie eine personalisierte Antwort:

1. Wählen Sie auf der Registerkarte "Administration" die Option "Service Desk" > "Persönliche Antworten" aus.

Die Listenseite "Personalisierte Antwort" wird angezeigt.

2. Klicken Sie auf "Neu erstellen".

Die Seite "Neue personalisierte Antwort erstellen" wird angezeigt.

3. Füllen Sie die Felder auf der Seite aus:

Antwortbesitzer

Der Kontakt, der der Eigentümer der Antwort ist. Wenn dieses Feld leer ist, steht die Antwort allen Analysten zur Verfügung.

Antwort

Text, den alle Empfänger der Antwort erhalten. Dieses Feld kann bis zu 1000 Zeichen enthalten.

In diesem Feld können Sie Variablen verwenden. Beispiel:

```
Ticket ref_num: @{call_req_id.ref_num}  
Zuständiger: @{call_req_id.assignee.combo_name}  
Kunde: @{call_req_id.customer.combo_name}  
Beschreibung: @{call_req_id.description}
```

4. Markieren Sie die Arten von Datensätzen, für die diese Antwort verfügbar sein soll. Klicken Sie auf "Speichern".

Eine personalisierte Antwort wird erstellt.

Ersetzung von personalisierten Antwortvariablen

Variablen können im Text einer persönlichen Antwort eingebettet werden. Mit diesen Variablen können Informationen aus der entsprechenden Anforderung, dem Änderungsauftrag, der Problemanfrage, dem Problem oder dem Vorfall einsetzen. Die Syntax der Variablen ist die gleiche Syntax, die in anderen Bereichen der CA SDM-Anwendung, z. B. in den Meldungsvorlagen für Aktivitätsbenachrichtigungen und dem Meldungstext für manuelle Benachrichtigungen verwendet wird. Die Informationen können nur aus der entsprechenden Anforderung, dem Change, dem Issue, dem Problem oder dem Incident eingesetzt werden. In Meldungsvorlagen für die Aktivitätsbenachrichtigung und den Meldungstext für die manuelle Benachrichtigung können zusätzlich Informationen aus dem Aktivitätsprotokolldatensatz verwendet werden.

Kontrollkästchen für jeden Objekttyp (Anforderungen, Changes, Issues, Incidents und Probleme) ermöglichen das Filtern von Antworten während der Auswahl. Bei nicht aktiviertem Objekttyp steht die Antwort für dieses Objekt nicht zur Verfügung. Ist zum Beispiel nur das Kontrollkästchen "Anforderung" aktiviert, erscheint die Antwort nur in Aktivitäten für eine Anforderung.

Eine einzige Antwort kann für alle Objekttypen (Anforderungen, Änderungsaufträge, Problemanfragen, Probleme und Vorfälle) verwendet werden. Da jedes Objekt unterschiedliche Attribute besitzt, werden Informationen, die sich nicht auf das Objekt beziehen, nicht ersetzt (zum Beispiel beim Versuch, die Anforderungsnummer in einer Antwort für einen Issue zu ersetzen).

Im Folgenden finden Sie ein Antwort-Textbeispiel und die unterschiedlichen Ersetzungen, die für jeden Objekttyp auftreten:

```
Dies ist Anforderung Nr. '{@call_req_id.ref_num}'  
Dies ist Änderungsauftrag Nr. '{@change_id.chg_ref_num}'  
Dies ist Problemanfrage Nr. '{@issue_id.ref_num}'
```

In einer *Anfrage* wird das Folgende eingesetzt:

```
Dies ist Anforderung Nr. 'cr_demo:11'  
Dies ist der Änderungsauftrag Nr.  
Dies ist die Problemanfrage Nr.
```

In einem *Change* wird das Folgende eingesetzt:

```
Dies ist die Anforderung Nr.  
Dies ist Änderungsauftrag Nr. 'chg_demo:3'  
Dies ist die Problemanfrage Nr.
```

In einem *Issue* wird das Folgende eingesetzt:

Dies ist die Anforderung Nr.
Dies ist der Änderungsauftrag Nr.
Dies ist Problemanfrage Nr. 'iss_demo:6'

Durch Verwendung der Kontrollkästchen "Diese Antwort zeigen für" können verschiedene Versionen einer Antwort mit den passenden Ersetzungsvariablen für das entsprechende Objekt (Anforderungen, Changes, Issues, Probleme oder Incidents) erstellt werden.

Für Variablen in den verschiedenen Objekten gilt das folgende Format.

Objekt	Variablenformat
Anforderung / Vorfall / Problem	@{call_req_id.attr}
Change	@{change_id.attr}
Issue	@{issue_id.attr}

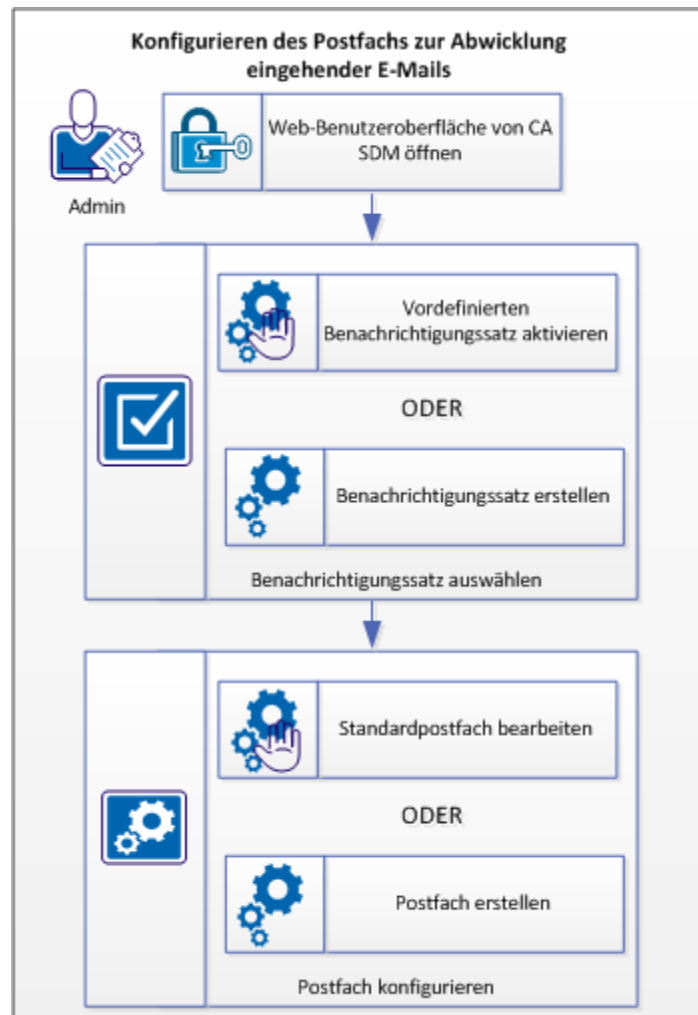
Die Werte werden eingesetzt, wenn die Antwort aus dem Feld "Anwenderbeschreibung" kopiert wird. Die Antwort wird kopiert, nachdem sie in der Dropdown-Liste "Persönliche Antwort" ausgewählt wurde und die Dropdown-Liste nicht mehr im Fokus ist.

So konfigurieren Sie das Postfach zur Bearbeitung der eingehenden E-Mails

Mit Hilfe von E-Mail können Sie mit Endanwendern, wie Mitarbeitern oder Kunden, kommunizieren. Das Postfach in CA SDM bearbeitet eingehende E-Mails von Anwendern und gibt entsprechend der E-Mail eine Aktion an. Zum Beispiel sendet der Anwender eine E-Mail an CA SDM, um einen Incident zu erstellen. Das Postfach überprüft die E-Mail, erstellt einen Incident, und schickt eine Benachrichtigung an den Anwender, der darüber informiert wird, dass der Incident erfolgreich erstellt wurde.

CA SDM bietet ein Standardpostfach ("Standard" genannt), das aktiv ist und von Ihnen in Ihrer Organisation verwendet werden kann. Sie können das Standardpostfach ändern und zusätzliche Postfächer erstellen. Nachdem Sie ein Postfach erstellt oder das standardmäßige Postfach geändert haben, definieren Sie die Postfachregeln. Mit Postfachregeln können Sie Aktionen, Antworten oder beides konfigurieren, die für Meldungen auftreten müssen, welche aus einem Postfach abgerufen wurden.

Folgendes Diagramm zeigt, wie das Postfach konfiguriert sein muss, um eingehende E-Mails zu bearbeiten:



Gehen Sie wie folgt vor:

1. [Öffnen Sie die CA SDM-Web-Benutzeroberfläche](#) (siehe Seite 202).
2. [Erstellen Sie eine Benachrichtigungswortfolge](#) (siehe Seite 228).
 - [Aktivieren Sie eine vordefinierte Benachrichtigungswortfolge](#) (siehe Seite 229).
 - [Erstellen Sie eine Benachrichtigungswortfolge](#) (siehe Seite 230).
3. [Konfigurieren Sie das Postfach](#) (siehe Seite 236).
 - [Bearbeiten Sie das Standardpostfach](#) (siehe Seite 236).
 - [Erstellen Sie ein Postfach](#) (siehe Seite 241).

Öffnen der CA SDM-Web-Benutzeroberfläche

Melden Sie sich in der Web-Benutzeroberfläche aus folgenden Servern an, abhängig von Ihrer CA SDM-Konfiguration:

- Konventionell: Primärserver oder Sekundärserver
- Erweiterte Verfügbarkeit: Anwendungsserver oder Hintergrundserver

Erstellen einer Benachrichtigungswortfolge

Die Benachrichtigungswortfolge wird an den Absender der E-Mail gesendet. Um zum Beispiel zu bestätigen, dass ein Incident erfolgreich erstellt wurde. CA SDM gibt vordefinierte Benachrichtigungswortfolgen an, die standardmäßig auf "Inaktiv" festgelegt sind. Sie können die Wortfolgen aktivieren und bearbeiten. Sie können auch Benachrichtigungswortfolgen erstellen, um sie den Anforderungen Ihrer Organisation optimal anzupassen.

Wählen Sie eine der folgenden Optionen:

- [Aktivieren einer vordefinierten Benachrichtigungswortfolge](#) (siehe Seite 229).
- [Erstellen von Benachrichtigungswortfolgen](#) (siehe Seite 230)

Aktivieren einer vordefinierte Benachrichtigungswortfolge

Standardmäßig sind vordefinierte Benachrichtigungszeichenfolgen auf "Inaktiv" festgelegt. Wenn Sie die Benachrichtigungszeichenfolge aktivieren, kann sie in Benachrichtigungen eingesetzt werden.

Hinweis: Wenn die Mandantenfähigkeit installiert ist, wählen Sie in der Dropdown-Liste den entsprechenden Mandanten aus. Mit der Option "öffentlich (freigegeben)" wird das Objekt für alle Mandanten erstellt.

Gehen Sie wie folgt vor:

1. Wählen Sie auf der Registerkarte "Administration" die Optionen "Benachrichtigungen", "Benachrichtigungswortfolgen" aus.
Die Seite "Benachrichtigungswortfolge - Liste" wird geöffnet.
2. Suchen Sie nach der Benachrichtigungswortfolge.
3. Klicken Sie auf die Wortfolge, die Sie aktivieren möchten. Wählen Sie zum Beispiel "Benachrichtigungsverlauf - Change".
Die Seite "Benachrichtigungswortfolge - Detail" wird geöffnet.
4. Klicken Sie auf "Bearbeiten".
Die Seite "Benachrichtigungswortfolge aktualisieren" wird geöffnet.
5. Wählen Sie "Aktiv" in der Drop-down-Liste "Aktiv" aus.
6. (Optional) Ändern Sie im Bedarfsfall die anderen [Felder](#) (siehe Seite 230). Ändern Sie zum Beispiel die Wortfolge.
7. Klicken Sie auf "Speichern".
Die Seite "Benachrichtigungswortfolge - Detail" wird geöffnet.
8. Klicken Sie auf "Fenster schließen".
Die Benachrichtigungszeichenfolge ist aktiv.

Erstellen von Benachrichtigungswortfolgen

Sie können eine Benachrichtigungswortfolge erstellen, die standardisierte Texte und Makros enthält. Diese Benachrichtigungswortfolge wird als Antwort der E-Mails von Anwendern gesendet.

Hinweis: Wenn die Mandantenfähigkeit installiert ist, wählen Sie in der Dropdown-Liste den entsprechenden Mandanten aus. Mit der Option "öffentlich (freigegeben)" wird das Objekt für alle Mandanten erstellt.

Gehen Sie wie folgt vor:

1. Wählen Sie auf der Registerkarte "Administration" die Optionen "Benachrichtigungen", "Benachrichtigungswortfolgen" aus.
Die Seite "Benachrichtigungswortfolge - Liste" wird geöffnet.
2. Klicken Sie auf "Neu erstellen".
Die Seite Neue Benachrichtigungswortfolge erstellen wird geöffnet.
3. Füllen Sie die [Felder für die Benachrichtigungswortfolge](#) (siehe Seite 230) entsprechend aus.
4. Klicken Sie auf "Speichern".
Die Benachrichtigungswortfolge wird erstellt.

Benachrichtigungswortfolgen-Felder

Füllen Sie folgende Felder aus, um eine Benachrichtigungswortfolge zu bearbeiten oder zu erstellen:

Symbol

Definiert ein eindeutiges Kennzeichen für diesen Datensatz.

Code

Gibt einen eindeutigen Wert an, der in der Tabelle "usp_notification_phrase" für die Benachrichtigungswortfolge verwendet werden soll. In der Tabelle "usp_notification_phrase" werden allgemeine Wortfolgen aufgelistet, die von Benachrichtigungsvorlagen verwendet werden können. Informationen zur Tabelle "usp_notification_phrase" finden Sie im *Technischen Referenzhandbuch*.

Wortfolge

Gibt die Wortfolge für die Benachrichtigung an. Sie können sowohl Nur-Text-Versionen als auch HTML-Versionen angeben. Da HTML die meisten Leerzeichen in einzelne Leerschritte konsolidiert, müssen Sie Zeilenumbrüche oder Absatzmarken mit Tags angeben.

Zum Beispiel wird folgende Nur-Text-Wortfolge in der Benachrichtigungswortfolge "Vertrauliche Notiz" verwendet:

Diese E-Mail und sämtliche darin übertragenen Dateien sind ausschließlich für den/die vorgesehenen Empfänger gedacht. Sie enthalten möglicherweise mit Privilegien verbundene und vertrauliche Informationen. Jede unbefugte Rezension, Verwendung, Offenlegung oder Verbreitung ist verboten. Wenn Sie nicht der beabsichtigte Empfänger dieser E-Mail sind, löschen Sie die E-Mail und alle darin übertragenen Dateien, und verständigen Sie umgehend den Absender.

Folgende HTML-Wortfolge kann verwendet werden, um den Anwender darum zu bitten, die Benachrichtigungsliste anzuzeigen:

Klicken Sie auf folgende URL, um die Benachrichtigungsliste anzuzeigen:
`@{call_req_id.web_url}+HTML=cr_lr.html+INSTANCE=@{id}`

Weitere Informationen zu Wortfolgen finden Sie unter dem Thema [Benachrichtigungs-codes und -zeichenfolgen](#). (siehe Seite 231)

Benachrichtigungs-codes und -zeichenfolgen

Mit Benachrichtigungszeichenfolgen können Sie standardisierte Informationen oder standardisierten Text zu einer Anzahl unterschiedlicher Benachrichtigungsmeldungen hinzufügen, ohne Text oder Formeln in jeder Benachrichtigungsvorlage eingeben und pflegen zu müssen. Beispiel:

Auf diese Benachrichtigung antworten, um dem Ticket weitere Informationen hinzuzufügen

Zeichenfolgen standardisieren Text zur Verwendung in mehreren Meldungsvorlagen. Zum Beispiel können Sie eine übliche Zeichenfolge wie eine vertrauliche Notiz in einem einzelnen Datensatz pflegen und diese in mehreren Meldungsvorlagen verwenden. Benachrichtigungszeichenfolgen sind auch für Nachrichtenantworten wie z. B. eine Antwort-Notiz oder eine Web-URL-Verknüpfung nützlich. CA SDM stellt Zeichenfolgen bereit; Sie können aber auch eigene Zeichenfolgen erstellen. Sie können eine Zeichenfolge für die globale Verwendung in einer Meldungsvorlage als aktiv oder inaktiv festlegen. (Benachrichtigungszeichenfolgen sind standardmäßig inaktiv.) Wenn eine Zeichenfolge inaktiv ist, wird sie in allen Meldungsvorlagen ausgeblendet, die die Zeichenfolge verwenden.

Benachrichtigungszeichenfolgen können auch in den automatischen Antworten auf eingehende E-Mail-Nachrichten verwendet werden. Der Verarbeitungskontext für diese Art von Meldung ist unterschiedlich; lassen Sie das Präfix (change_id., issue_id., call_req_id.) weg, das in gewissen Makros wie ref_num und web_url für Zeichenfolgen verwendet wird, welche die Meldung benutzen. Dadurch können Benachrichtigungszeichenfolgen nicht in Benachrichtigungsvorlagen und automatischen E-Mail-Antworten gemeinsam verwendet werden.

Zum Beispiel stellt CA SDM folgende Zeichenfolgen bereit:

Symbol	Code	Wortfolge
Benachrichtigungsverlauf - Change	notify_history_chg	Klicken Sie auf die folgende URL, um die Benachrichtigungsliste anzuzeigen: <code>@{change_id.web_url}+HTMPL=chg_lr.html+INSTANCE=@{id}</code>
Benachrichtigungsverlauf - Issue	notify_history_iss	Klicken Sie auf die folgende URL, um die Benachrichtigungsliste anzuzeigen: <code>@{issue_id.web_url}+HTMPL=iss_lr.html+INSTANCE=@{id}</code>
Benachrichtigungsverlauf - Anfrage/Incident/Problem	notify_history_cr	Klicken Sie auf die folgende URL, um die Benachrichtigungsliste anzuzeigen: <code>@{call_req_id.web_url}+HTMPL=cr_lr.html+INSTANCE=@{id}</code>

Beispiel: Neue Zeichenfolgen

Im Folgenden finden Sie Beispielzeichenfolgen, die Sie erstellen können:

Symbol	Code	Wortfolge
Benachrichtigung - Vertraulich	ConfidentialNotice	Diese E-Mail und sämtliche darin übertragenen Dateien sind ausschließlich für den/die vorgesehenen Empfänger gedacht. Sie enthalten möglicherweise mit Privilegien verbundene und vertrauliche Informationen. Jede unbefugte Rezension, Verwendung, Offenlegung oder Verbreitung ist verboten. Wenn Sie nicht der beabsichtigte Empfänger dieser E-Mail sind, löschen Sie die E-Mail und alle darin übertragenen Dateien, und verständigen Sie umgehend den Absender.
Benachrichtigung - Incident-Antwort	IncidentReply	Um dem Incident einen Kommentar hinzuzufügen, antworten Sie einfach auf diese E-Mail oder fügen die Zeile unten ein (in einer separaten Zeile). %incident_id=@{call_req_id.ref_num}
Benachrichtigung - Incident-URL	IncidentURL	Zum Anzeigen klicken Sie auf die folgende URL: @{call_req_id.web_url}

Hinweis: Benutzen Sie separate Zeichenfolgen für Klartext- und HTML-Versionen von Meldungsvorlagen oder automatischen E-Mail-Antworten. HTML fasst die meisten Leerzeichen zu einzelnen Leerzeichen zusammen. Zeilen- oder Absatzumbrüche müssen daher mit Tags angegeben werden. HTML-Tags, die in Klartextversionen von Meldungen enthalten sind, werden angezeigt, aber nicht verarbeitet.

Syntax von Benachrichtigungszeichenfolgen

Fügen Sie Benachrichtigungszeichenfolgen mit der folgenden Makrosyntax in Meldungsvorlagen und E-Mail-Antwort-Nachrichten ein:

@{notification_phrase[code].phrase}

code

Gibt den eindeutigen Codewert der Tabelle der Benachrichtigungszeichenfolgen (usp_notification_phrase) an, beispielsweise "ConfidentialNotice".

Hinweis: In der Tabelle "usp_notification_phrase" werden häufig verwendete Zeichenfolgen aufgelistet, die in Vorlagen für Benachrichtigungsmeldungen verwendet werden können. Informationen zur Tabelle "usp_notification_phrase" finden Sie im *Technischen Referenzhandbuch*.

Beispiel:

```
@{notification_phrase[IncidentURL1].phrase}
```

```
@{notification_phrase[RequestReply].phrase}
```

Wenn CA SDM das Makro verarbeitet, wird die Makro-Zeichenfolge durch den Phrasentext aus der Tabelle "usp_notification_phrase" ersetzt. Wenn kein übereinstimmender Code gefunden werden kann (oder der Code inaktiv ist), wird das Makro durch eine leere Zeichenfolge ersetzt. Es werden keine Fehler in das Standardprotokoll (STDLOG) geschrieben, es wird jedoch eine Warnmeldung eingetragen, die Ihnen dabei helfen können, potenzielle Probleme zu lösen.

Hinweis: Das Einbetten von Zeichenfolgen in andere Zeichenfolgen ist auf einen Maximalwert für die Rekursionstiefe beschränkt, den Sie durch Festlegen der [Umgebungsvariable](#) (siehe Seite 498) "NX_MAX_EXPAND_DEPTH" konfigurieren können. Diese Beschränkung verhindert Probleme bei der Verarbeitung von Zeichenfolgen, direkt oder indirekt über eine dritte Zeichenfolge auf sich selbst verweisen.

Beispiel: Benachrichtigungszeichenfolgen in einer Benachrichtigung

Dieses Beispiel zeigt, wie Benachrichtigungszeichenfolgen in einer Benachrichtigung erscheinen. Im Beispiel werden die folgenden Codes und Wortfolgen verwendet:

Code	Wortfolge
ConfidentialNotice	Diese E-Mail und sämtliche darin übertragenen Dateien sind ausschließlich für den/die vorgesehenen Empfänger gedacht. Sie enthalten möglicherweise mit Privilegien verbundene und vertrauliche Informationen. Jede unbefugte Rezension, Verwendung, Offenlegung oder Verbreitung ist verboten. Wenn Sie nicht der beabsichtigte Empfänger dieser E-Mail sind, löschen Sie die E-Mail und alle darin übertragenen Dateien, und verständigen Sie umgehend den Absender.
IncidentReply	Um dem Incident einen Kommentar hinzuzufügen, antworten Sie einfach auf diese E-Mail oder fügen die Zeile unten ein (in einer separaten Zeile). %incident_id=@{call_req_id.ref_num}
IncidentURL	Zum Anzeigen klicken Sie auf die folgende URL: @{call_req_id.web_url}

Die folgende Meldungsvorlage enthält die Benachrichtigungszeichenfolgen:

```
@{call_req_id.type.sym} @{call_req_id.ref_num} Geschlossen.  
Zugewiesen zu: @{call_req_id.assignee.combo_name}  
Kunde: @{call_req_id.customer.combo_name}  
Beschreibung: @{call_req_id.description}  
  
@{notification_phrase[IncidentURL].phrase}  
@{notification_phrase[IncidentReply].phrase}  
  
@{notification_phrase[ConfidentialNotice].phrase}
```

Die Wortfolgen werden in einer Nachricht wie folgt angezeigt:

```
Incident 1234 Geschlossen.  
Zugewiesen zu: Analyst, Joe  
Kunde: Doe, John  
Beschreibung: Dies ist eine Beschreibung meines Problems
```

Klicken Sie zum Anzeigen auf die folgende URL:

```
http://helpdesk/CAisd/pdmweb.exe?OP=SEARCH+FACTORY=chg+SKIPLIST=1+QBE.EQ.id=40072  
3
```

Um dem Incident einen Kommentar hinzuzufügen, antworten Sie einfach auf diese E-Mail oder fügen die Zeile unten ein (in einer separaten Zeile).

```
%incident_id=1234
```

Diese E-Mail und sämtliche darin übertragenen Dateien sind ausschließlich für den/die vorgesehenen Empfänger gedacht. Sie enthalten möglicherweise mit Privilegien verbundene und vertrauliche Informationen. Jede unbefugte Rezension, Verwendung, Offenlegung oder Verbreitung ist verboten. Wenn Sie nicht der beabsichtigte Empfänger dieser E-Mail sind, löschen Sie die E-Mail und alle darin übertragenen Dateien, und verständigen Sie umgehend den Absender.

Konfigurieren des Postfachs

CA SDM gibt ein Standardpostfach an, das mit dem Mail-Server verbunden werden soll. Sie können dieses Standardpostfach konfigurieren, um das Kennwort, den Användernamen, den Hostnamen usw. zu ändern. Sie können auch zusätzliche Postfächer erstellen, um sie den Anforderungen Ihrer Organisation optimal anzupassen. Jedes Postfach kann seine eigene Definition haben, anstatt eines einzigen globalen Satzes von Definitionen zu verwenden. Sie können mehrere Postfächer definieren und unterschiedliche Vorlagen oder Standardwerte für jedes Postfach verwenden. Mit mehreren Definitionen können Mandanten separate Postfächer verwenden; ebenso kann ein einzelner Mandant oder eine einzelne Organisation damit unterschiedliche Postfächer verwenden und unterschiedliche Verhaltensweisen für jedes Postfach konfigurieren.

Wählen Sie eine oder beide der folgenden Möglichkeiten aus:

Wichtig! Es wird empfohlen, das zugeordnete Postfach auf "Inaktiv" festzulegen, bevor Sie eine Postfachregel aktualisieren. Andernfalls werden alle Nachrichten, die der Mail-Server zwischen der ersten und der letzten Änderung abrufen, mit den Regeln verarbeitet, die beim Abrufen der Nachricht gültig sind.

- [Bearbeiten Sie das Standardpostfach](#) (siehe Seite 236).
- [Erstellen Sie ein Postfach](#) (siehe Seite 241).

Bearbeiten des Standardpostfachs

CA SDM stellt ein aktives Standardpostfach bereit, das Sie bearbeiten können, um es an die eingehenden Mail-Übermittlungsanforderungen in Ihrer Organisation anzupassen.

Gehen Sie wie folgt vor:

1. Wählen Sie auf der Registerkarte "Administration" die Optionen E-Mail, Postfächer aus.
Die Seite Postfachliste wird geöffnet.
2. Klicken Sie auf "Standard" in der Spalte "Name".
Die Seite "Standardpostfach-Detail" wird geöffnet.
3. Klicken Sie auf "Bearbeiten".

4. Füllen Sie die anderen Felder nach Bedarf aus bzw. aktualisieren Sie sie:

CheckInterval

Gibt das Intervall an, in dem der Mail-Server nach neuen E-Mails abgefragt wird.

Aktiv

Zeigt den Postfachstatus an.

EmailType

Gibt das Protokoll an, das der Mail-Server verwendet. CA SDM unterstützt sowohl POP3 als auch IMAP4. Wenn Sie IMAP4 wählen, fragt CA SDM nur den Posteingangsordner des Postfachs ab.

Hostname

Gibt den Hostnamen des E-Mail-Servers an.

Port-Überschreibung

Gibt die Portnummer an, wenn die standardmäßige Portnummer überschrieben wird.

Anwendername

Gibt die Anwender-ID auf dem Mail-Server an.

Kennwort

Gibt das Kennwort auf dem Mail-Server an.

Sicherheitsstufe

Gibt die SMTP-Sicherheitsstufe an.

AttachmentRepository

Gibt das Repository an, wo E-Mail-Anhänge gespeichert werden.

AttachEntireEmail

Gibt an, ob eine ganze E-Mail als Anhang erlaubt ist.

ForceAttachmentSplitout

Gibt an, ob alle Anhänge in der E-Mail geteilt werden sollen, wenn eine ganze E-Mail als Anhang hinzugefügt wird. Die E-Mail und die zugehörigen Anhänge werden in separate Dateien geteilt und an die Tickets angehängt. Nur anwendbar, wenn die Option "Ganze E-Mail anhängen" ausgewählt ist.

AllowAnonymous

Gibt an, ob Tickets von anonymen Mails erstellt werden können.

SaveUnknownEmails

Gibt an, ob die E-Mails gespeichert werden sollen, die die Regeln, die im Postfach angegebenen sind, nicht verarbeitet. Diese E-Mails werden unter "\$NX_ROOT/site/mail_unknown" gespeichert.

Antwortadresse verwenden

Gibt an, ob die alternative E-Mail-Adresse für Antworten verwendet werden soll.

Use TLS

Gibt an, ob TLS-Support (Transport Layer Security) in E-Mails verwendet werden soll.

CA-Zertifikat Pfad

Gibt den Pfad an, wo das vertrauenswürdige Zertifikat bereitgestellt wurde.

Hinweis: Bei der Konfiguration für erweiterte Verfügbarkeit müssen Sie das vertrauenswürdige Zertifikat auf der gleichen Lokation sowohl für den Hintergrundserver als auch für den Standby-Server bereitstellen. CA SDM unterstützt nur Base-64-verschlüsseltes Format (PEM) für CA-Zertifikate.

5. (Optional) Erstellen oder aktualisieren Sie die [Postfachregeln](#) (siehe Seite 247) und [Richtlinien](#) (siehe Seite 245) nach Bedarf.

Hinweis: Die Regeln, die für ein Postfach anwendbar sind, können nicht mit einem anderen Postfach verknüpft werden. Um die gleichen Regeln für ein anderes Postfach wiederzuverwenden, stellen Sie die Regeln für das andere Postfach wieder her. Sie können auch das vorhandene Postfach kopieren.

Wichtig! Es wird empfohlen, das verknüpfte Postfach auf "Inaktiv" festzulegen, bevor Sie eine Postfachregel aktualisieren. Andernfalls werden alle Nachrichten, die der Mail-Server zwischen der ersten und der letzten Änderung abrufen, mit den Regeln verarbeitet, die gültig sind.

6. Klicken Sie auf "Speichern".

Die Änderungen am Standardpostfach werden gespeichert und angewendet. Die erste Abfrage findet nach einer Sekunde statt.

Mehrere Postfächer

CA SDM kann mehrere Postfächer verarbeiten und verwalten. Jedes Postfach kann seine eigene Definition haben, anstatt eines einzigen globalen Satzes von Definitionen zu verwenden. Sie können mehrere Postfächer definieren und unterschiedliche Vorlagen oder Standardwerte für jedes Postfach verwenden. Mit mehreren Definitionen können Mandanten separate Postfächer verwenden; ebenso kann ein einzelner Mandant oder eine einzelne Organisation damit unterschiedliche Postfächer verwenden und unterschiedliche Verhaltensweisen für jedes Postfach konfigurieren. Sie können mehrere Postfächer einrichten, indem Sie die Administrationsschnittstelle verwenden. Jedes Postfach verwendet folgende Tabellen:

- usp_mailbox - Definiert das Postfach.

- **usp_mailbox_rule** - Gibt einen Regelsatz für jedes Postfach an.

Da Postfachregeln Text-API-Vorgaben liefern, können Sie E-Mail-Schnittstellen mit anderer Software und Parametern (wie Kategorie, Zuständiger usw.) erstellen, die speziell für die Schnittstelle konfiguriert werden.

Hinweis: IMAP-Server unterstützen mehrere Postfächer für ein einzelnes Konto, alternative Postfächer werden jedoch nicht unterstützt; nur der Standard-Posteingang wird unterstützt.

Mehrere Postfächer und Regeln

Die Komponente "Mail Eater" (pdm_maileater_nxd) auf dem Primärserver verwendet Postfachverbindungen und Regeln, um Nachrichten von einem oder mehreren Konten auf einem oder mehreren Mail-Servern zu lesen und zu verarbeiten. Mail Eater verarbeitet Postfächer seriell (es wird jeweils nur ein Postfach verarbeitet) und Regeln in Sequenznummerreihenfolge.

Bei mehreren Postfächern werden folgende Regeln verwendet:

1. Beim Starten des Primärservers liest die Komponente "Mail Eater" die folgenden Tabellen:

usp_mailbox

Stellt eine Verbindung zu einem Mail-Server dar.

usp_mailbox_rules

Stellt die Regeln dar, die sich auf die Verbindung beziehen (usp_mailbox).

Contact_Method

Stellt die für automatische Antworten benutzten Kontaktmethoden dar.

Document_Repository

Stellt die Dokument-Repositorys zum Speichern von Anhängen dar.

Die Komponente "Mail Eater" erkennt automatisch Änderungen an den Objekten in irgendeiner dieser Tabellen, einschließlich der Hinzufügung weiterer Objekte. Wenn eine Änderung an usp_mailbox oder usp_mailbox_rule vorgenommen wird, wird das Abfrageintervall für das betroffene Postfach für eine Sekunde nach der Anwendung der Änderung neu geplant.

2. Bei dem durch das einzelne Postfach definierten Intervall lädt die Komponente "Mail Eater" jede E-Mail in den Posteingang für das zugehörige Konto und verarbeitet die E-Mail wie folgt:
 - a. Prüft die E-Mail-Adresse auf Richtlinienverletzungen. Wenn die Komponente "Mail Eater" eine Verletzung findet, wird die Verarbeitung beendet, und die Auswirkungen auf das Standardprotokoll entsprechen der Postfachdefinition.
 - b. Vergleicht die E-Mail mit jeder Regel (mailbox_rule), die zu diesem Postfach gehört.

- c. Wenn eine übereinstimmende Regel gefunden wird, gibt die Komponente die Meldung zum Versenden an die Text-API weiter und antwortet dem Benutzer entsprechend der festgelegten Aktion für die Regel.

Bei Antwort-E-Mails identifiziert die Filterzeichenfolge das Objekt und verwendet die Text-API für die Verarbeitung. Nach der Verarbeitung wird die Antwort an die Antwortadresse oder die Adresse "Von" weitergeleitet.

- d. Nachdem die Komponente "Mail Eater" eine übereinstimmende Regel gefunden hat, werden keine anderen Regeln überprüft, und Mail Eater verarbeitet die nächste E-Mail im Posteingang.
 - e. Wenn keine übereinstimmende Regel gefunden wird, wird die Nachricht verworfen.
- 3. Nachdem die Komponente "Mail Eater" alle E-Mails für einen Posteingang verarbeitet hat, werden die verarbeiteten und verworfenen Nachrichten aus dem Mail-Server entfernt und das nächste Verarbeitungsintervall wird geplant.

Erstellen von Postfächern

Sie können ein Postfach erstellen, das mit dem Mail-Server verbunden wird und dessen Einstellungen für Host, Anwender, Kennwort usw. Sie festlegen können.

Gehen Sie wie folgt vor:

1. Wählen Sie auf der Registerkarte "Administration" die Optionen E-Mail, Postfächer aus.

Die Seite mit der Liste der Postfächer wird geöffnet.

2. Klicken Sie auf "Neu erstellen".

Die Seite "Postfach-Detail" wird geöffnet.

3. Füllen Sie die Felder nach Bedarf aus:

CheckInterval

Gibt das Intervall an, in dem der Mail-Server nach neuen E-Mails abgefragt wird.

Aktiv

Zeigt den Postfachstatus an.

EmailType

Gibt das Protokoll an, das der Mail-Server verwendet. CA SDM unterstützt sowohl POP3 als auch IMAP4. Wenn Sie IMAP4 wählen, fragt CA SDM nur den Posteingangsordner des Postfachs ab.

Hostname

Gibt den Hostnamen des E-Mail-Servers an.

Port-Überschreibung

Gibt die Portnummer an, wenn die standardmäßige Portnummer überschrieben wird.

Anwendername

Gibt die Anwender-ID auf dem Mail-Server an.

Kennwort

Gibt das Kennwort auf dem Mail-Server an.

Sicherheitsstufe

Gibt die SMTP-Sicherheitsstufe an.

AttachmentRepository

Gibt das Repository an, wo E-Mail-Anhänge gespeichert werden.

AttachEntireEmail

Gibt an, ob eine ganze E-Mail als Anhang erlaubt ist.

ForceAttachmentSplitout

Gibt an, ob alle Anhänge in der E-Mail geteilt werden sollen, wenn eine ganze E-Mail als Anhang hinzugefügt wird. Die E-Mail und die zugehörigen Anhänge werden in separate Dateien geteilt und an die Tickets angehängt. Nur anwendbar, wenn die Option "Ganze E-Mail anhängen" ausgewählt ist.

AllowAnonymous

Gibt an, ob Tickets von anonymen Mails erstellt werden können.

SaveUnknownEmails

Gibt an, ob die E-Mails gespeichert werden sollen, die die Regeln, die im Postfach angegebenen sind, nicht verarbeitet. Diese E-Mails werden unter "\$NX_ROOT/site/mail_unknown" gespeichert.

Antwortadresse verwenden

Gibt an, ob die alternative E-Mail-Adresse für Antworten verwendet werden soll.

Use TLS

Gibt an, ob TLS-Support (Transport Layer Security) in E-Mails verwendet werden soll.

CA-Zertifikat Pfad

Gibt den Pfad an, wo das vertrauenswürdige Zertifikat bereitgestellt wurde.

Hinweis: Bei der Konfiguration für erweiterte Verfügbarkeit müssen Sie das vertrauenswürdige Zertifikat auf der gleichen Lokation sowohl für den Hintergrundserver als auch für den Standby-Server bereitstellen. CA SDM unterstützt nur Base-64-verschlüsseltes Format (PEM) für CA-Zertifikate.

4. Klicken Sie auf der Registerkarte "Regeln" auf "Neu erstellen", um eine Postfachregel zu erstellen.

Die Seite "Neue Postfachregel erstellen" wird geöffnet.

Hinweis: Die Regeln, die für ein Postfach anwendbar sind, können nicht mit einem anderen Postfach verknüpft werden. Um die gleichen Regeln für ein anderes Postfach wiederzuverwenden, stellen Sie die Regeln für das andere Postfach wieder her. Sie können auch das vorhandene Postfach kopieren.

Wichtig! Es wird empfohlen, das verknüpfte Postfach auf "Inaktiv" festzulegen, bevor Sie eine Postfachregel aktualisieren. Andernfalls werden alle Nachrichten, die der Mail-Server zwischen der ersten und der letzten Änderung abrufen, mit den Regeln verarbeitet, die gültig sind.

5. Füllen Sie die [Felder der Postfachregel](#) (siehe Seite 247) aus, und klicken Sie auf "Speichern".
6. Wählen Sie die Registerkarte "Richtlinie" aus, um die Postfachrichtlinien zu definieren, um Ihre Organisation vor gewissen Arten des E-Mail-Missbrauchs zu schützen. Füllen Sie die [Felder der Postfachrichtlinie](#) (siehe Seite 245) aus, und klicken Sie auf "Speichern".

Das Postfach wird erstellt.

Wenn Sie mehrere Postfächer verwenden, dann verwendet die Komponente "Mail Eater" (pdm_maileater_nxd) Postfachverbindungen und Regeln, um Nachrichten von einem oder mehreren Konten auf einem oder mehreren Mail-Servern zu lesen und zu verarbeiten. Der "Mail Eater" wird abhängig von Ihrer CA SDM-Konfiguration auf folgenden Servern ausgeführt:

- Konventionell: Primärserver
- Erweiterte Verfügbarkeit: Hintergrundserver

"Mail Eater" fragt die Postfächer seriell (es wird jeweils nur ein Postfach verarbeitet) und Regeln in der Reihenfolge der Sequenznummern ab:

- a. Beim Start eines Primärservers oder eines Hintergrundservers liest "Mail Eater" folgende Tabellen in der Datenbank:

usp_mailbox

Stellt eine Verbindung zu einem Mail-Server dar.

usp_mailbox_rules

Stellt die Regeln dar, die sich auf die Verbindung beziehen (usp_mailbox).

Contact_Method

Stellt die für automatische Antworten verwendeten Kontaktmethoden dar.

Document_Repository

Stellt die Dokument-Repositorys zum Speichern von Anhängen dar.

Die Komponente "Mail Eater" erkennt automatisch Änderungen an den Objekten in irgendeiner dieser Tabellen, einschließlich der Hinzufügung weiterer Objekte. Wenn eine Änderung an usp_mailbox oder usp_mailbox_rule vorgenommen wird, wird das Abfrageintervall für das betroffene Postfach für eine Sekunde nach der Anwendung der Änderung neu geplant.

- b. Bei dem durch das einzelne Postfach definierten Intervall lädt die Komponente "Mail Eater" jede E-Mail in den Posteingang für das zugehörige Konto und verarbeitet die E-Mail wie folgt:
- c. Prüft die E-Mail-Adresse auf Richtlinienverletzungen. Wenn die Komponente "Mail Eater" eine Verletzung findet, wird die Verarbeitung beendet, und die Auswirkungen auf das Standardprotokoll entsprechen der Postfachdefinition.
- d. Vergleicht die E-Mail mit jeder Regel (mailbox_rule), die zu diesem Postfach gehört.

- e. Wenn eine übereinstimmende Regel gefunden wird, gibt die Komponente die Meldung zum Versenden an die Text-API weiter und antwortet dem Anwender entsprechend der festgelegten Aktion für die Regel.

Bei Antwort-E-Mails identifiziert die Filterzeichenfolge das Objekt und verwendet die Text-API für die Verarbeitung. Nach der Verarbeitung wird die Antwort an die Antwortadresse oder die Adresse "Von" weitergeleitet.

- f. Nachdem die Komponente "Mail Eater" eine übereinstimmende Regel gefunden hat, werden keine anderen Regeln überprüft, und Mail Eater verarbeitet die nächste E-Mail im Posteingang.

- g. Wenn keine übereinstimmende Regel gefunden wird, wird die Nachricht verworfen.

Nachdem die Komponente "Mail Eater" alle E-Mails für einen Posteingang verarbeitet hat, werden die verarbeiteten und verworfenen Nachrichten aus dem Mail-Server entfernt und das nächste Verarbeitungsintervall wird geplant.

Erstellen von Postfachrichtlinien

Sie können Richtlinien erstellen, die sich auf Aktionen, Antworten (oder beides) beziehen, die ausgeführt werden müssen, damit die E-Mail in den Posteingang zugestellt wird.

So erstellen Sie eine Postfachregel:

1. Wählen Sie auf der Registerkarte "Administration" die Option "E-Mail" > "Postfächer" aus.

Die Seite "Postfachliste" wird angezeigt, auf der Attribute aufgelistet werden.

2. Klicken Sie auf den Namen des Postfachs, für das Sie Richtlinien konfigurieren möchten.

Die Seite "Postfach-Detail" wird angezeigt.

3. Klicken Sie auf die Registerkarte "Richtlinie".

Dem Postfach zugeordnete Richtliniendetails werden angezeigt.

4. Klicken Sie auf "Bearbeiten".

Sie können die Felder bearbeiten.

5. Füllen Sie die [Felder](#) (siehe Seite 245) nach Bedarf aus.

6. Klicken Sie auf "Speichern".

Die Postfachrichtlinie wird festgelegt und tritt sofort in Kraft.

E-Mail-Adresse/Stunde

Gibt die maximale Anzahl von E-Mails pro E-Mail-Adresse pro Stunde an. Sie können die folgenden Werte angeben:

- -1 = Keine Begrenzung (Standardeinstellung)
- 0 = Keine E-Mails zulässig.
- 1 = Maximal zulässige Anzahl von E-Mails.

LogViolation

Protokolliert die Verletzung im Standardprotokoll. Sie können die folgenden Werte angeben:

- Nicht protokollieren
- Nur erste Verletzung (Standardeinstellung)
- Alle Verletzungen

Hinweis: Die Option "Nur erste Verletzung" speichert eine Liste der E-Mail-Adressen, die mit Nachrichten verknüpft sind, welche die Postfachrichtlinien verletzen, und verwendet die Liste für das Protokoll, um doppelte Protokolleinträge zu vermeiden. Die Liste wird gelöscht, wenn der Mail Eater-Daemon neu gestartet wird. Wenn Sie jedoch die Einstellung von "Nur erste Verletzung" in eine der anderen Optionen und zurück ändern, wird die Liste der E-Mail-Adresse, die im Rahmen dieser Einstellung protokolliert wurde, nicht gelöscht. Wenn ein Postfach während der Verwendung dieser Einstellung zahlreiche Verletzungen protokolliert, empfehlen wir, den Mail Eater-Daemon regelmäßig neu zu starten, um die Liste zu löschen, oder die Option "Nicht protokollieren" zu verwenden.

Aufnahmeliste

Gibt E-Mail-Adresse oder -Domänen an, die E-Mails verarbeiten dürfen. Es sind nur E-Mails zulässig, die mit der Liste übereinstimmen. Sie können mehrere Adressen oder Domänen angeben, indem Sie sie durch ein Komma, ein Semikolon, ein Leerzeichen oder einen Zeilenumbruch trennen. Die Eingabe nur eines Sternchens (*) entspricht der Weltdomäne selbst und stimmt mit allen Domänen überein, die nicht in der Ausschlussliste enthalten sind.

Ausschlussliste

Gibt E-Mail-Adresse oder -Domänen an, die keine E-Mails verarbeiten dürfen. Sie können mehrere Adressen oder Domänen angeben, indem Sie sie durch ein Komma, ein Semikolon, ein Leerzeichen oder einen Zeilenumbruch trennen.

Hinweis: Adressen in der Ausschlussliste setzen alle Werte in der Einschlussliste außer Kraft. Adressen in der Einschlussliste setzen Domänen in der Ausschlussliste außer Kraft und können bestimmte Ausnahmen für bestimmte Absender in einer sonst verbotenen Domäne bereitstellen. Domänen in der Ausschlussliste setzen die Weltdomäne in der Einschlussliste außer Kraft. Die Weltdomäne ist in der Ausschlussliste nicht gültig.

Felder der Postfachrichtlinie

Sie können folgende Felder verwenden, um die Richtlinie zu implementieren:

E-Mail-Adresse/Stunde

Gibt die Anzahl der E-Mails pro Stunde an, die von einer E-Mail-Adresse an dieses Postfach gesendet werden können. Wenn eine E-Mail-Adresse die Grenze überschreitet, wird die E-Mail-Adresse der Ausschlussliste hinzugefügt. Es werden dann keine Meldungen von dieser Absender-E-Mail-Adresse mehr für dieses Postfach verarbeitet, bis Sie die E-Mail-Adresse aus der Ausschlussliste entfernen.

LogViolation

Gibt an, ob die E-Mail-Adressen protokolliert werden soll, die die Richtlinie in der Datei "stdlog" verletzen.

Aufnahmeliste

Gibt die E-Mail-Adressen (zum Beispiel "user@company.com") oder die E-Mail-Domänen (zum Beispiel "company.com") an, die E-Mails senden dürfen.

Die Standard-Einschlussliste für jedes Postfach ist ein Sternchen (*). Ein Sternchen allein als ganzer Name in der Liste gibt die Welt-Domäne an und bezieht sich auf alle E-Mail-Domänen, die nicht in der Ausschlussliste enthalten sind. Diese Angabe verhindert Unklarheiten bezüglich der Frage, ob die Ausschlussliste die vollständige Liste der erlaubten Domänen oder die Ausnahmen für Domänen in der Ausschlussliste ist. Dies geschieht auf folgende Art und Weise:

- Eine Einschlussliste, die die Welt-Domäne einschließt, gibt an, dass alle anderen Einträge in der Einschlussliste Ausnahmen für die Ausschlussliste sind und nur Domänen oder Adressen in der Ausschlussliste (mit Aufnahme von bestimmten Adressen in der Einschlussliste) blockiert werden.
- Eine Einschlussliste, die die Welt-Domäne nicht enthält, gibt an, dass nur die in der Einschlussliste aufgeführten Adressen und Domänen senden dürfen, und das nur, falls die Absenderdomäne (falls die bestimmte Adresse nicht in der Einschlussliste steht) oder die Adresse nicht in der Ausschlussliste steht.

Ausschlussliste

Gibt die E-Mail-Adressen (zum Beispiel "user@company.com") oder die E-Mail-Domänen (zum Beispiel "company.com") an, die keine E-Mails senden dürfen.

Hinweis: Postfachrichtlinien gehören nur zum einzelnen verknüpften Postfach. Eine Adresse, die wegen der Verletzung der Beschränkung der maximalen Anzahl an E-Mails automatisch zu einer Postfach-Ausschlussliste hinzugefügt wird, wird weder automatisch zur Ausschlussliste für andere Postfächer hinzugefügt noch wird die E-Mail-Anzahl für andere Postfächer verwendet.

Postfachregelfelder

Füllen Sie die folgenden Postfachregelfelder nach Bedarf aus:

Sequenz

Gibt die Sequenznummer der Regel an. Meldungen werden gegen Regeln in Sequenznummerreihenfolge überprüft, von unten nach oben.

Postfach

Gibt das Postfach an, zu dem diese Regel gehört.

Aktiv

Setzt die Regel auf aktiv oder inaktiv.

Filter

Gibt an, welcher Teil der E-Mail nach dem Filtermuster durchsucht werden soll, z. B. nach Einschränkungen in der Betreffzeile. Weitere Informationen finden Sie unter dem Thema [Musterabgleich in Postfachregeln](#). (siehe Seite 252)

FilterString

Gibt eine Zeichenfolge für reguläre Ausdrücke an, die mit dem E-Mail-Inhalt abgeglichen werden soll. Zum Beispiel: [\t\r\n]request[\t\r\n]. Mit dem Platzhalter {{object_id}} können Sie den Artefaktwert für die Text-API angeben, um somit die Meldung mit einem bestimmten Ticket zu verbinden. Weitere Informationen finden Sie unter den Themen [Objektkennungsbeschränkungen in Filterzeichenfolgen](#) (siehe Seite 254) und [Sonderzeichen in regulären Ausdrücken](#). (siehe Seite 255)

IgnoreCase

Gibt an, ob bei der Übereinstimmung von Mustern die Groß- und Kleinschreibung berücksichtigt werden soll.

Aktion

Gibt die auszuführende Aktion an, wenn das Filterkriterium z. B. mit "Objekt erstellen/aktualisieren" übereinstimmt.

Hinweis: Informationen zu Regelaktionen finden Sie im *Administrationshandbuch*.

ActionObject

Zeigt die Art von Ticket-Objekt an, auf die sich Meldungsaktionen beziehen, zum Beispiel, "Request".

Minimaler Artefakttyp

Gibt den gewünschten Mindestwert für das Überprüfen von Artefakten an:

KEINE

Gibt an, dass Artefakte nicht validiert werden. Dieser Wert bedeutet, dass der Eingabedatei keine Schlüsselwörter hinzugefügt werden. Akzeptiert auch Befehle für Text-API-Ticket-IDs.

GESCHÜTZT

Tickets werden zur Bestätigung auf das Vorhandensein der Raute validiert. Wenn die Bestätigung scheitert, wird das Artefakt als ungültig eingestuft, und dort wo der Filter nach einem Artefakt ({{object_id}}) sucht, kann die E-mail das Filterergebnis nicht anzeigen.

SICHER

Validiert die Ticketnummer eines verschlüsselten Datenblocks. Wenn der Wert keine gültige verschlüsselte Ticketnummer ist, wird das Artefakt für ungültig eingestuft, und dort wo der Filter nach einem Artefakt ({{object_id}}) sucht, kann die E-mail das Filterergebnis nicht anzeigen.

Hinweis: Typen mit einem höheren Sicherheitsniveau sind erlaubt. Das heißt, wenn Sie den Mindestwert auf GESCHÜTZT setzen, dann sind sowohl GESCHÜTZT und SICHER erlaubt, jedoch nicht KEINE. Hinzu kommt, dass wenn GESCHÜTZT oder SICHER ausgewählt sind, keine Befehle für Text-API-Ticket-IDs erlaubt sind. Weitere Informationen über Artefakte finden Sie im Thema [Hinweise zur Verwendung von Artefakten](#). (siehe Seite 257)

Antwort

Gibt eine Benachrichtigungsmethode an, um eine automatische Antwort zu senden. Zum Beispiel: E-Mail. Wenn Sie diese Option nicht auswählen, wird keine Antwort gesendet. Die Antwort zeigt an, ob die meldungsbezogenen Aktionen erfolgreich waren oder nicht. Die Antwort erfolgt getrennt von anderen Benachrichtigungen. Wenn Sie mehrere Postfächer verwenden, dann empfehlen wir Ihnen, die Benachrichtigungsmethode zu verwenden, um [E-Mail-Antworten zu konfigurieren](#) (siehe Seite 263).

Betreff der Antwort

Gibt eine Betreffzeile für die Antwort an, z. B. Service Desk-Antwort.

In stdlog schreiben

Schreibt E-Mail-Text in das Standardprotokoll (stdlog), wenn der Filter übereinstimmt.

LogEntryPrefix

Gibt ein Präfix an, das anzufügen ist, wenn man den E-Mail-Text den Standardprotokolleinträgen hinzufügt. Verwenden Sie diese Option, um zu ermöglichen, dass Protokolleinträge Regeln zugeordnet werden können.

AddSubjectLine

Fügt vor dem Verarbeiten die Betreffzeile der ursprünglichen Meldung dem Meldungstext hinzu. Sie können eine Betreffzeile anhängen, voranstellen oder keine Betreffzeile hinzufügen. Die Betreffzeile wird entweder der Ticket-Beschreibung oder dem Protokollkommentar hinzugefügt, je nach den Aktionen für die Meldung.

Standardeinstellungen für die Text-API

Gibt zusätzliche Standardbefehle für die Text-API bei Übereinstimmung des Filters an. Wird mit dem Inhalt des Abschnitts [EMAIL_DEFAULTS] der Datei "text_api.cfg" kombiniert. Das Feld "Standard-TextAPI" enthält Befehle für TextAPI-Schlüsselwörter, die auf ein Ticket angewendet werden, wenn das Ticket aus einer E-mail erstellt wird, das mit einer Postfachregel übereinstimmt. Der Befehl wird nicht angewandt, wenn die Meldung zu einem vorhandenen Ticket gehört.

Um Standard-TextAPI-Befehle anzugeben, platzieren Sie im Feld "Standard-TextAPI" jeden Befehl auf eine separate Zeile. Formatieren Sie die Befehle wie folgt:

`OBJECT.FIELD=value`

Hinweis: Vor dem Befehl darf kein Prozentzeichen (%) stehen. Das Prozentzeichen ist nur dann erforderlich, wenn ein entsprechender Befehl in den Text der E-mail eingebettet ist.

Formatieren Sie den Befehl z. B. wie folgt:

`REQUEST.PRIORITY=3`

`PROBLEM.CATEGORY=Einrichtungen`

`INCIDENT.GROUP=Heizungs- und sanitäre Installationen`

Text-API – bei Eingang ignorieren

Gibt zusätzliche zu ignorierende Details für die Text-API bei Übereinstimmung des Filters an. Wird mit dem Inhalt des Abschnitts [EMAIL_IGNORE_INCOMING] der Datei "text_api.cfg" kombiniert.

Das Feld "Eingehende API-Texte ignorieren" führt Befehle für TextAPI-Schlüsselwörter auf, die im Text der eingehenden E-mail nicht verwendet werden dürfen. Alle in diesem Feld aufgeführten Befehle werden ignoriert, wenn sie sich in einer eingehenden E-mail befinden.

So definieren Sie Befehle vom Typ "Eingehende API-Texte ignorieren":

- a. Platzieren Sie jeden Befehl im Feld "Eingehende API-Texte ignorieren" in eine separate Zeile.
- b. Formatieren Sie die Befehle wie folgt:

`OBJECT.FIELD`

Hinweis: Vor dem Befehl darf kein Prozentzeichen (%) stehen. Das Prozentzeichen ist nur dann erforderlich, wenn ein entsprechender Befehl in den Text der E-mail eingebettet ist.

Formatieren Sie den Befehl z. B. wie folgt:

CHANGE.ASSIGNEE

PROBLEM.GROUP

REQUEST.EFFORT

- c. Definieren Sie alle, für jedes Feld verwendete Befehle im Abschnitt [KEYWORDS] der Datei "text_api.cfg". Diese Datei befindet sich im Unterverzeichnis "site" des CA SDM-Installationsverzeichnis.

Details

Gibt Informationen über die Regel an.

Erfolgstext

Gibt die Nur-Text-Inhalte einer Antwortmeldung an, wenn die Meldung erfolgreich verarbeitet wird. Beispiel:

Vielen Dank für die Aktualisierung Ihres Request. Ein Support-Techniker wird sich innerhalb der nächsten 24 Stunden mit Ihnen in Verbindung setzen.

Sie können auch eine Benachrichtigungswortfolge eingeben, wenn bereits erstellt. Zum Beispiel können Sie eine Benachrichtigungswortfolge für automatische E-Mail-Antworten verwenden.

Vielen Dank für Ihre Anfrage.

@{notification_phrase[Code der Benachrichtigungswortfolge].phrase}

Erfolg (HTML)

Gibt HTML-Inhalte einer Antwortmeldung an, wenn die Meldung erfolgreich verarbeitet wird. Mit den folgenden Optionen können Sie HTML-Text in der Vorschau anzeigen und bearbeiten:

Erfolgs-HTML bearbeiten

Öffnet den HTML-Editor, mit dem Sie die HTML-Datei bearbeiten können.

Schnellansicht

Erstellt eine Vorschau der HTML.

HTML-Quelle

Zeigt die HTML-Quelle an.

Sie können zum Beispiel auch eine Benachrichtigungswortfolge verwenden.

Vielen Dank für Ihre Anfrage.</p>

@{notification_phrase[Code der Benachrichtigungswortfolge].phrase}</p>

Fehlertext

Gibt die Nur-Text-Inhalte einer Antwortmeldung an, wenn die Verarbeitung der Meldung fehlschlägt. Sie können auch eine Benachrichtigungswortfolge eingeben, wenn bereits erstellt. Sie können zum Beispiel den folgenden Text verwenden:

Vielen Dank für Ihre Anfrage.

@{notification_phrase[Code der Benachrichtigungswortfolge].phrase}

Fehler (HTML)

Gibt HTML-Inhalte einer Antwortmeldung an, wenn die Verarbeitung der Meldung fehlschlägt.

Erstellen von Postfachregeln

Sie können Regeln erstellen, die bestimmte Schlüsselwörter oder Elemente in den eingehenden Nachrichten erkennen und die entsprechenden festgelegten Aktionen bzw. Antworten (oder beides) ausführen.

Hinweis: Die Regeln, die für ein Postfach anwendbar sind, können nicht mit einem anderen Postfach verknüpft werden. Um die gleichen Regeln für ein anderes Postfach wiederzuverwenden, stellen Sie die Regeln für das andere Postfach wieder her. Sie können auch das vorhandene Postfach kopieren.

Wichtig! Es wird empfohlen, das verknüpfte Postfach auf "Inaktiv" festzulegen, bevor Sie eine Postfachregel aktualisieren. Andernfalls werden alle Nachrichten, die der Mail-Server zwischen der ersten und der letzten Änderung abrufen, mit den Regeln verarbeitet, die gültig sind.

So erstellen Sie eine Postfachregel:

1. Wählen Sie auf der Registerkarte "Administration" die Option "E-Mail" > "Postfachregeln" aus.

Die Seite "Benachrichtigungsregeln - Liste" wird angezeigt, auf der Regeln aufgelistet werden.

2. Klicken Sie auf "Neu erstellen".

Die Seite "Postfachregeldetail" wird angezeigt.

3. Füllen Sie die [Felder](#) (siehe Seite 247) nach Bedarf aus.

4. Klicken Sie auf "Speichern".

Die Postfachregel wurde erstellt und ist aktiv.

Aktionen für Postfachregeln

Mit Hilfe von Postfachregeln können Sie die folgenden E-Mail-Aktionen durchführen:

- E-Mail ignorieren – die E-Mail wird nicht verarbeitet und nicht beantwortet.

Diese Aktion ist nützlich für systemerstellte Nachrichten, wie bei Abwesenheit oder fehlgeschlagener Mailzustellung.

- E-Mail ignorieren und antworten – die E-Mail wird nicht verarbeitet und der Absender erhält eine Antwort. Antwort-E-Mails verwenden die Antworterfolgsmeldungen und die Nachrichten über fehlgeschlagene Antworten werden ignoriert.
- Objekt aktualisieren – verwendet die Filterzeichenfolge, um die Objektkennung zu bestimmen (z. B. %Incident:{{object_id}}% in der E-Mail) und sendet eine Aktualisierungsanfrage an die Text-API. Wenn die Objektkennung nicht gefunden wird, führt die Text-API keinen Vorgang aus.

Diese Aktion verarbeitet normalerweise E-Mail-Antworten, wo die Objektkennung in die E-Mail eingebettet wird. Wenn keine Objektkennung vorhanden ist, wird normalerweise die Nachricht einer fehlgeschlagenen Antwort gesendet.

- Objekt erstellen/aktualisieren – Verwendet die Filterzeichenfolge, um die Objektkennung zu bestimmen (z. B. %Incident:{{object_id}}% in der E-Mail) und sendet eine Aktualisierungsanfrage an die Text-API. Wenn die Objektkennung gefunden wird, aktualisiert die Text-API ein Ticket. Wenn die Objektkennung gefunden wird, erstellt die Text-API ein Ticket.

Diese Aktion ist das standardmäßige Verhalten der Programmroutine Mail Daemon (Mail Eater), wo die E-Mail Text-API-Schlüsselwörter enthält oder nicht enthält.

Hinweis: Informationen zum Konfigurieren von Postfachregeln finden Sie in der *Online-Hilfe*.

Musterabgleich in Postfachregeln

Postfachregeln verwenden reguläre Ausdrücke für den Musterabgleich. Achten Sie auf die folgenden Leerzeichen, die für reguläre Ausdrücke in Postfachregeln gelten:

\t

Gibt eine horizontale Registerkarte an.

\r

Gibt ein Wagenrücklaufzeichen an.

\n

Gibt ein Zeichen für Zeilenvorschub oder eine neue Zeile an.

Die Zeichen, die Zeilenumbrüche im Text darstellen, können je nach Betriebssystem, Mail-Server und Mail-Client variieren. Einige Beispiele:

- UNIX verwendet "\n".
- Microsoft verwendet "\r\n".
- Macintosh verwendet "\r".
- MacOS-X verwendet "\n".

Unter gewissen Umständen tauschen die Mail-Verarbeitungselemente von CA SDM einen dieser Zeilenumbruchzeichen gegen ein anderes, um eine Unterscheidung zwischen unterschiedlichen Textelementen wie Nachrichtentext und angehängte Parameter festzulegen oder aufrecht zu erhalten. Wenn Sie einen Zeilen- oder Paragraphenumbruch verwenden möchten, erstellen Sie Ihre Filter so, dass entweder \r oder \n abgeglichen werden können, je nachdem, welches gefunden wird. Wenn Sie einen Zeilenumbruch zwischen zwei Schlüsselwörtern angeben möchten, erstellen Sie Ihre Filter so, dass Sequenz von einem oder mehreren \r- und \n-Zeichen abgeglichen werden kann.

Zeilenumbrüche durch den Mail-Client, der eine Meldung sendet, können unerwartete Zeilenumbrüche inmitten des Textes hervorrufen, was eigentlich mit Ihrer Filterzeichenfolge übereinstimmen soll, wenn die Filterzeichenfolge den Meldungstext durchsucht. Ein Leerzeichen kann zu einem Wagenrücklauf, Zeilenvorschub oder beidem werden, oder der Wagenrücklauf, der Zeilenvorschub oder beide können nach einem Leerzeichen eingefügt werden. Wenn eine Meldung in HTML verfasst wird, und Aufzählungen oder Nummerierungen oder aber eingerückte Absätze enthält, können Tabulatoren auch vorhanden sein, nachdem der Mail-Client die Meldung konvertiert und gesendet hat. Wenn Sie Leerzeichen mitten in eine Filterzeichenfolge setzen, verwenden Sie einen Block mit regulären Ausdrücken, der Leerzeichen veränderbarer Größe darstellt. Dieser Block lautet [\t\r\n]+ (eckige Klammer auf, Leerzeichen, Rückwärtsschrägstrich, t, Rückwärtsschrägstrich, r, Rückwärtsschrägstrich, n, eckige Klammer zu, Pluszeichen), und stellt eine beliebige Sequenz von einem oder mehreren Leerzeichen, Tabulatoren, Wagenrückläufen und Zeilenvorschüben dar.

Beispiel: Verwendung von [\t\r\n] zum exakten Abgleich eines Schlüsselworts

Dieses Beispiel zeigt, wie Sie Leerzeichen verwenden können, um das Schlüsselwort "forder" abzugleichen und andere mögliche Schlüsselwörter wie folgende nicht abzugleichen:

Angefordert von
Anfordern
Angefordert
orequesta

Um nur das Schlüsselwort "forder" zu erreichen, stellen Sie dem Schlüsselwort "forder" ein oder mehrere Leerzeichen wie folgt voran oder nach:

```
[ \t\r\n]forder[ \t\r\n]
```

Der Mail Eater gleicht nur das Wort "forder" oder das Wort als Teil eines Satzes ab und nicht als Teil eines anderen Wortes wie "Angefordert von".

Objektkennungsbeschränkungen in Filterzeichenfolgen

Die Beschränkungen beziehen sich auf die Postfachregel-Filterzeichenfolgen, die die Objektkennung (z. B. %Incident:{{object_id}}%) in einer E-Mail bestimmen. Der Text, der eine Objektkennung ({{object_id}}) umgibt, muss sowohl hinsichtlich seines Inhalts als auch hinsichtlich seiner Länge eindeutig sein. Der Text muss deutlich Anfang und Ende des zwischen dem Text befindlichen Ticket-ID-Artefaktwerts definieren.

Die folgenden Beschränkungen beziehen sich darauf, wie der Mail Eater den *Anfang* des Ticket-ID-Artefaktwerts definiert:

- Der Platzhalter {{object_id}} muss nicht das erste Element in der Filterzeichenfolge sein. Es ist mindestens ein Zeichen und im Allgemeinen ein unverwechselbares Schlüsselwort erforderlich, oder vor dem Objekt-ID-Schlüsselwort muss eine Folge von Buchstaben, Ziffern und Symbolen stehen.
- Das unmittelbar dem Platzhalter {{object_id}} vorangehende Zeichen darf kein wiederholbares oder optionales Zeichen sein (also ein Zeichen, dem ein Pluszeichen (+), ein Sternchen (*), oder ein Fragezeichen (?) folgt), das Bestandteil eines Ticket-ID-Artefaktwerts sein kann. Wiederholbare oder optionale Zeichen können hinsichtlich des Anfangs des Ticket-ID-Artefaktwerts mehrdeutig sein, es sei denn, es handelt sich um Leerzeichen. Der Artefaktwert einer Ticket-ID darf keine nichtdruckbaren Zeichen (Leerzeichen, Tabulator, Zeilenumbruch, Zeilenvorschub) enthalten.
- Das unmittelbar dem Platzhalter {{object_id}} vorangehende Zeichen darf kein wiederholbarer oder optionaler, eingeklammerter Zeichensatz sein, der Zeichen beinhaltet, die Bestandteil des Ticket-ID-Artefaktwerts sein können.

Die folgenden Beschränkungen beziehen sich darauf, wie der Mail Eater die *Länge* des Ticket-ID-Artefaktwerts definiert:

- Der Platzhalter {{object_id}} darf nicht das letzte Element in der Filterzeichenfolge sein. Dem Platzhalter {{object_id}} müssen ein oder mehrere Zeichen folgen.
- Das unmittelbar dem Platzhalter {{object_id}} folgende Zeichen darf kein wiederholbares oder optionales Zeichen sein (also ein Zeichen, dem ein Pluszeichen (+), ein Sternchen (*), oder ein Fragezeichen (?) folgt), das Bestandteil eines Ticket-ID-Artefaktwerts sein kann. Wiederholbare oder optionale Zeichen können hinsichtlich des Endes des Ticket-ID-Artefaktwerts mehrdeutig sein, es sei denn, es handelt sich um Leerzeichen. Der Artefaktwert einer Ticket-ID darf keine nichtdruckbaren Zeichen (Leerzeichen, Tabulator, Zeilenumbruch, Zeilenvorschub) enthalten.

- Das erste Zeichen nach dem Platzhalter {{object_id}} darf kein Zeichen sein, das Bestandteil eines Ticket-ID-Artefaktwerts sein kann.
- Vermeiden Sie die folgenden Zeichen unmittelbar vor und nach dem Platzhalter {{object_id}}:
 - Alle Groß- oder Kleinbuchstaben
 - Zahlzeichen
 - Pluszeichen (+)
 - Schrägstrich (/)
 - Komma (,)
 - Punkt (.), denn er kann für jedes Zeichen außer einem Zeilenumbruch stehen und daher eines der in dieser Liste aufgeführten Zeichen sein.

Alle diese Zeichen können innerhalb eines Ticket-ID-Artefaktwerts vorkommen. Wenn ein eingeklammerter Zeichensatz (mehrere von einer Klammer eingefasste Zeichen, die alle mit einem angewendeten Filter übereinstimmen können) direkt vor oder hinter dem Platzhalter {{object_id}} steht, dann darf dieser keines dieser Zeichen enthalten.

Sonderzeichen in regulären Ausdrücken

Die Musterübereinstimmung für die Filter in Postfachregeln erfolgt gemäß den Regeln für reguläre ASCII-Ausdrücke mit Sonderzeichen im C-Stil.

Wichtig! Es ist empfehlenswert, dass Sie mit Regex-Syntax vertraut sind, um Sonderzeichen in regulären Ausdrücken zu benutzen.

Beachten Sie beispielsweise die folgenden Sonderzeichen für Regex-Muster, die für reguläre Ausdrücke in Postfachregeln gelten:

\t

Gibt eine horizontale Registerkarte an. In Filterzeichenfolgen für Postfachregeln stimmt \t mit dem Anfang und Ende von Text (und Tabulatoren) überein und ist kennzeichnend für den Mail Eater.

\r

Gibt einen Wagenrücklauf an (zurück zum Anfang der Zeile).

Hinweis: Benutzen Sie \r nicht für die Suche nach Nachrichtenbetriffs oder Absenderadressen.

\n

Gibt einen Zeilentrenner an (Kombination aus Zeilenvorschub und Wagenrücklauf).

Hinweis: Benutzen Sie \r nicht für die Suche nach Nachrichtenbetriffs oder Absenderadressen.

\t, \r, und \n sind die Sonderzeichen, die am häufigsten in regulären Ausdrücken für Postfachregeln auftreten.

Beispiel: Verwendung von \t, \r und \n.

[\t]Anfrage[\t]

Sucht nach Text mit dem Wort "Anfrage". Die Klammern stimmen mit jedem Zeichen des Zeichensatzes überein, einschließlich des Leerzeichens. Daher stimmt [\t mit einem Leerzeichen oder einem Tabulator überein.

[\r \n]+wichtig[\t \r \n]

Sucht nach Text mit dem Wort "wichtig" am Beginn einer Zeile, einer Nachricht oder als der gesamte Text einer Zeile. Die Klammern stimmen mit jedem Zeichen des Zeichensatzes überein. Das + (Pluszeichen) stimmt mit einem oder mehr als einem der vorangehenden Zeichen überein, daher stimmt [\r \n]+ mit einem oder mehreren Wagenrückläufen und Zeilentrennern überein.

Beispieltext für Benachrichtigungszeichenfolgen in einer Postfachregel

Dieses Beispiel zeigt, dass Mustertext an, den Sie verwenden können, um Benachrichtigungszeichenfolgen in eine Postfachregel einzuschließen. Sie definieren separate Versionen einer Benachrichtigungszeichenfolge für Klartext und für HTML, wenn die Zeichenfolge Zeilenumbrüche oder andere Formatierungen enthält.

Verwenden Sie den folgenden Text in "Erfolgstext", "Erfolgs-HTML" oder beiden Feldern auf der Registerkarte "Erfolgreiche Antwort" der Seite "Postfachregel aktualisieren":

■ Erfolgstext

Vielen Dank für Ihre Anfrage.
{notification_phrase[IncidentURL1]}.phrase}

■ Erfolg (HTML)

Vielen Dank für Ihre Anfrage.</p>
{notification_phrase[IncidentURL1H]}.phrase}</p>

Hinweis: Weitere Informationen zu Benachrichtigungstexten, die auf der Registerkarte "Administration" unter "Benachrichtigungen", "Benachrichtigungswortfolgen" definiert werden, finden Sie in der *Online-Hilfe*.

Weitere Informationen:

[Benachrichtigungs-codes und -zeichenfolgen](#) (siehe Seite 231)

[Syntax von Benachrichtigungszeichenfolgen](#) (siehe Seite 233)

Hinweise zur Verwendung von Artefakten

Ein E-Mail *Artefakt* verweist auf etwas, das aus dem Mail-Prozess entsteht, zum Beispiel eine E-Mail-Adresse, die in einer weitergeleiteten E-Mail enthalten ist. Die Text-API verwendet Artefakte, die eine Ticket-ID (wie z. B. eine Referenznummer) für den Antwort-Support enthalten. Wenn die Ticket-ID gefunden wird, wird ein existierendes Text-API-Schlüsselwort (wie z. B. %INCIDENT_ID) gesetzt und der Eingabe für die Text-API hinzugefügt. Der Mail Eater erkennt, dass eine Antwort einem besonderen Ticket zugeordnet ist, indem das Artefakt in der Meldung gesucht wird.

Mit Postfachregeln können Sie das Artefakt und den Wert angeben, die die Text-API verwendet. Sie können zum Beispiel eine Regel für Incidents als Incident:{{object_id}}% definieren. Wenn eine Regel Incident:1234 findet, verwendet die Text-API %INCIDENT_ID=1234 (1234 ist die ref_num für den Incident). Da das Artefakt in einer E-Mail einmalig und leicht zu finden sein muss, können Sie das Artefakt unverwechselbarer machen, wie z. B. %Incident:{{object_id}}%. Ein Prozentzeichen (%), Leerzeichen oder ein anderes Zeichen, der nicht in einem Artefaktwert erscheinen darf, muss nach {{object_id}} stehen. Groß- und Kleinbuchstaben, Zahlen, Schrägstriche, Kommas und Pluszeichen sind potenziell Teil eines Wertes. Die sicheren Artefakte werden nach der Verschlüsselung Base64-verschlüsselt. Wenn Sie keine sicheren Artefakte verwenden, dürfen die Zeichen, die nach dem Artefakt stehen, gegebenenfalls nicht im Tickets-Suffix, das für diesen Tickettyp konfiguriert wurde, enthalten sein.

Bei Verwendung der Filterzeichenfolge der Postfachregeln zur Identifizierung des Ticket-ID-Artefakts stellt das Schlüsselwort {{object_id}} die Position in der Filterzeichenfolge dar, an der das Ticket-ID-Artefakt erwartet wird. Dieses Schlüsselwort unterscheidet zwischen Groß- und Kleinschreibung, auch wenn die Postfachregel dies nicht tut.

Beispiel: Verwendung des E-Mail-Artefakts

Das folgende Beispiel zeigt ein ARTEFAKT-Format für die Verwendung in einer Postfachregel für ein Change-Ticket.

Nutzung: %REQUEST=@{call_req_id.ref_num}%

Beispiel: %REQUEST=1234%

Wenn Sie die Filterzeichenfolge der Postfachregel erstellen, beachten Sie folgende Bedingungen:

- Zwischen dem vorangehenden Ticket-ID-Artefakt und den folgenden Schlüsselwörtern muss es eine klare Grenze geben. Wir empfehlen eingehend, in diesem abgrenzend Text Leerzeichentext aufzunehmen.

- Beenden Sie den Teil der Filterzeichenfolge, die dem Schlüsselwort `{{object_id}}` vorangeht, nicht in einem wiederholbaren oder optionalen Muster, das mit dem Anfang des Ticket-ID-Artefakts übereinstimmen kann, und beenden Sie kein Muster, dessen Länge mehrdeutig ist. Zum Beispiel darf die Filterzeichenfolge kein `request(er|ed|ing)?{{object_id}}` enthalten, da diese Konstruktion eine Mehrdeutigkeit verursacht, ob ein nachgestelltes "er", "ed" oder "ing" das Ende des vorangehenden Texts oder Teil des Präfixes einer ungeschützten Ticket-ID ist.
- Der Teil der Filterzeichenfolge, die den Schlüsselwort `{{object_id}}` folgt, darf in keinem wiederholbaren oder optionalen Muster beginnen, das mit dem Ende des Ticket-ID-Artefakts übereinstimmen könnte, darf mit keinem Muster beginnen, dessen Länge mehrdeutig ist, und muss mindestens ein Leerzeichen-Element enthalten. Beispiel:
 - Die Filterzeichenfolge darf kein `{{object_id}}[A-Z]?` enthalten, da `[A-Z]?` mit dem letzten Zeichen des Ticket-ID-Artefakts übereinstimmen könnte.
 - Die Filterzeichenfolge darf nicht mit `{{object_id}}Item` enden, da es möglich ist, dass Item im Ticket-ID-Artefakt entweder als Suffix einer Ticket-ID in einem Klartext- oder geschütztem Artefakt oder als Zeichen innerhalb eines sicheren Artefakts erscheint.
 - `{{object_id}}` Item ist annehmbar, da das Leerzeichen nicht Teil eines Ticket-ID-Artefakts sein kann, und nicht Teil eines geschützten oder klaren Ticket-ID-Artefakts ist. Allerdings ist `{{object_id}}[ \t\r\n]+Item` (eckige Klammer auf, Leerzeichen, Rückwärtsschrägstrich, t, Rückwärtsschrägstrich, r, Rückwärtsschrägstrich, n, eckige Klammer zu, Pluszeichen, +Item) besser, da das `[ \t\r\n]+` einen Ausgleich schafft, wenn das Mailprogramm einen Zeilenumbruch nach dem `{{object_id}}` einfügt.
- Wenn Sie die Filterzeichenfolgen für unterschiedliche Postfachregeln erstellen, vermeiden Sie, eine Filterzeichenfolge zu benutzen, die eine andere Filterzeichenfolge für Postfachregeln vollkommen einschließt oder in dem der Teil vor oder nach einem Schlüsselwort `{{object_id}}` diesen Teil einer anderen Filterzeichenfolge für Postfachregeln vollkommen einschließt. Je nach der Reihenfolge, in der diese Filter geprüft werden, kann eine Meldungsübereinstimmung für einen Filter mit einem anderen übereinstimmen, wobei ein Teil des Ticket-ID-Artefakts mit dem zusätzlichen Text, der zwischen den beiden Filterzeichenfolgen unterscheidet, übereinstimmt.

Administrationshandbuch: Erstellen einer Postfachregel, die jede eingehende Meldung erfasst

Dieser neue Abschnitt gilt für das *Administrationshandbuch*, Kapitel "Richtlinie zur Implementierung", Abschnitt "E-mail-Verwaltung, Postfachregeln".

Sie können eine Postfachregel erstellen, die jede eingehende Meldung erfasst, die von einer anderen Postfachregel nicht gefiltert wird.

Setzen Sie dazu den Filter auf "Betreff enthält" und geben Sie für die Filterzeichenfolge einen Punkt und ein Sternchen an (".*").

- Ein Punkt erfasst alle Zeichen, mit Ausnahme von Zeilenumbrüchen.
- Ein Sternchen erfasst null oder mehrere der Zeichen, die direkt vor dem Sternchen stehen.

Demzufolge gibt diese Regel null oder mehrere Zeichen an, die keine Zeilenumbrüche sind.

Beispiel: Eine "Alles erfassen"-Postfachregel

Diese Beispiel veranschaulicht, wie man mit einer Regel vom Typ ".*" alle eingehenden Meldungen erfassen kann.

Filter = "Betreff enthält"
Filterzeichenfolge = ".*"

Verwenden der TextAPI-Voreinstellungen und Ignorieren der eingehenden TextAPI-Einstellungen für Postfachregeln

Mit Hilfe der Felder "Standard-TextAPI" und "Eingehende API-Texte ignorieren" können Sie bestimmte Voreinstellungen für den Posteingang festlegen und TextAPI-Befehle angeben, die bei eingehenden E-mails nicht angenommen werden dürfen. Diese Felder greifen auf die Voreinstellungen im Abschnitt [EMAIL_DEFAULTS] zurück, sowie auf die Liste mit unzulässigen Befehlen im Abschnitt [EMAIL_IGNORE_INCOMING] der Datei "text_api.cfg". Wenn es zu einem Konflikt zwischen der Definition einer Postfachregel und der Definition in der Datei "text_api.cfg" kommt, gilt der in der Postfachregel festgelegte Wert.

Das Feld "Standard-TextAPI" enthält Befehle für TextAPI-Schlüsselwörter, die auf ein Ticket angewendet werden, wenn das Ticket aus einer E-mail erstellt wird, das mit einer Postfachregel übereinstimmt. Der Befehl wird nicht angewandt, wenn die Meldung zu einem vorhandenen Ticket gehört.

So definieren Sie Befehle vom Typ "Standard-TextAPI":

1. Platzieren Sie jeden Befehl im Feld "Standard-TextAPI" in eine separate Zeile.
2. Formatieren Sie die Befehle wie folgt:

OBJECT.FIELD=value

Hinweis: Vor dem Befehl darf kein Prozentzeichen (%) stehen. Das Prozentzeichen ist nur dann erforderlich, wenn ein entsprechender Befehl in den Text der E-mail eingebettet ist.

Formatieren Sie den Befehl z. B. wie folgt:

REQUEST.PRIORITY=3
PROBLEM.CATEGORY=Einrichtungen
INCIDENT.GROUP=Heizungs- und sanitäre Installationen

Das Feld "Eingehende API-Texte ignorieren" führt Befehle für TextAPI-Schlüsselwörter auf, die im Text der eingehenden E-mail nicht verwendet werden dürfen. Alle in diesem Feld aufgeführten Befehle werden ignoriert, wenn sie sich in einer eingehenden E-mail befinden.

So definieren Sie Befehle vom Typ "Eingehende API-Texte ignorieren":

1. Platzieren Sie jeden Befehl im Feld "Eingehende API-Texte ignorieren" in eine separate Zeile.
2. Formatieren Sie die Befehle wie folgt:

`OBJECT.FIELD`

Hinweis: Vor dem Befehl darf kein Prozentzeichen (%) stehen. Das Prozentzeichen ist nur dann erforderlich, wenn ein entsprechender Befehl in den Text der E-mail eingebettet ist.

Formatieren Sie den Befehl z. B. wie folgt:

`CHANGE.ASSIGNEE`

`PROBLEM.GROUP`

`REQUEST.EFFORT`

3. Definieren Sie alle, für jedes Feld verwendete Befehle im Abschnitt [KEYWORDS] der Datei "text_api.cfg". Diese Datei befindet sich im Unterverzeichnis "site" des CA SDM-Installationsverzeichnis.

So konfigurieren Sie die E-Mail-Antworten

Die E-Mail-Benachrichtigungen, die Sie in Postfächern verwenden, sind spezifisch für Antworten, die einem Kontakt als Antwort auf dessen E-Mails geschickt werden. Sie können beispielsweise E-Mails so konfigurieren, dass wenn ein Kontakt auf eine Antwortverknüpfung in einer E-Mail-Benachrichtigung klickt, die Antwort-E-Mail zu einem Postfach geleitet wird.

Hinweis: Diese Einrichtung unterscheidet sich von den regulären E-Mail-Benachrichtigungen.

Gehen Sie wie folgt vor:

1. [Öffnen Sie die CA SDM-Web-Benutzeroberfläche](#) (siehe Seite 202).
2. Stellen Sie sicher, dass Sie das [Postfach für eingehende E-Mail konfiguriert haben](#) (siehe Seite 226).
3. [Konfigurieren Sie den Mail-Server](#) (siehe Seite 261).
4. (Optional) Geben Sie eine Benachrichtigungs-E-Mail-Adresse in der Kontaktdefinition an.

Hinweis: Wählen Sie auf der Registerkarte "Administration" die Option Sicherheits- und Rollenmanagement, Kontakte aus, und wählen Sie den zu bearbeitenden Kontakt aus.

5. [Ändern Sie die E-Mail-Benachrichtigungsmethode](#) (siehe Seite 263).

Öffnen der CA SDM-Web-Benutzeroberfläche

Melden Sie sich in der Web-Benutzeroberfläche aus folgenden Servern an, abhängig von Ihrer CA SDM-Konfiguration:

- Konventionell: Primärserver oder Sekundärserver
- Erweiterte Verfügbarkeit: Anwendungsserver oder Hintergrundserver

Konfigurieren des Mail-Servers

Benachrichtigungen zu einem Ereignis (sowohl automatische wie manuelle) werden unter Verwendung eines zentral festgelegten Mail-Servers versendet.

Gehen Sie wie folgt vor:

1. Wählen Sie auf der Registerkarte "Administration" die Option "Optionsmanager", "E-Mail".
Die Seite Optionen - Liste wird geöffnet.
2. Klicken Sie auf die [E-Mail-Option](#) (siehe Seite 262), die Sie installieren möchten.
Die Seite mit den Optionsdetails wird geöffnet.

3. Klicken Sie auf "Bearbeiten", geben Sie die erforderlichen Werte in die Felder ein, und klicken Sie dann auf "Installieren".

Der Mail-Server ist fertig konfiguriert, um Nachrichtigen zu senden (ausgehende Nachrichtigen).

4. Wiederholen Sie diese Schritte bei Bedarf, um alle erforderlichen Optionen der Optionsliste zu konfigurieren.

E-Mail-Optionen

Die E-Mail-Schnittstelle sendet E-Mail-Benachrichtigungen und ermöglicht Anwendern die Erstellung von Tickets per E-Mail.

mail_from_address

Gibt bei der Postbenachrichtigung das Feld "Von:" an. Die Adresse hat das Format Displayname<anwender@unternehmen.com>.

mail_login_password

Gibt das Login-Kennwort für den SMTP-Server an.

mail_login_userid

Gibt die Anwender-ID für die Anmeldung am SMTP-Server an.

mail_max_threads

Gibt die größtmögliche Anzahl von gleichzeitigen SMTP-Verbindungen an, die versuchen können, mit dem SMTP-Server zu kommunizieren.

mail_reply_to_address

Definiert die Antwortadresse für E-Mail-Benachrichtigungen. Diese Option ist nützlich, wenn E-Mails von einem Anwenderkonto geschickt werden, Antworten jedoch an eine andere E-Mail-Adresse geschickt werden sollen. Der Standardwert ist identisch mit der Absenderadresse ("Von").

mail_smtp_domain_name

Definiert den Domänennamen des SMTP-Servers an. Sie können den Domänennamen löschen, indem Sie den Wert auf NONE setzen.

mail_smtp_hosts

Gibt eine Leerstellen-getrennte Liste von Hostnamen des SMTP-Servers für E-Mail-Benachrichtigungen an.

mail_smtp_host_port

Gibt einen SMTP-Port an, um den Standard-SMTP-Port zu überschreiben.

mail_smtp_security_level

Gibt die SMTP-Sicherheitsstufe an. Gültige Einstellungen sind: 0=keine Sicherheit, 1=grundlegende Authentifizierung, 2=NTLM, 3=MD5 und 4=LOGIN. Wenn Sie diese Option auf 1 setzen, konfigurieren Sie Optionen für "mail_login_password" und "mail_login_userid". Die meisten SMTP-Server erfordern keine Authentifizierung.

mail_smtp_use_tls

Gibt den TLS-Verwendung (Transport Layer Security) in der E-Mail an. Die gültigen Einstellungen sind "Yes" = TLS verwenden, "No" = TLS nicht verwenden.

mail_ca_cert_path

Gibt den Pfad an, wo das vertrauenswürdige Zertifikat bereitgestellt wurde.

Hinweis: Bei der Konfiguration für erweiterte Verfügbarkeit müssen Sie das vertrauenswürdige Zertifikat auf allen CA SDM-Servern am gleichen Speicherort bereitstellen. CA SDM unterstützt nur Base-64-verschlüsseltes Format (PEM) für CA-Zertifikate.

Ändern der E-Mail-Benachrichtigungsmethode

Ändern Sie die E-Mail-Benachrichtigungsmethode, um die E-Mail-Antworten zu konfigurieren.

Gehen Sie wie folgt vor:

1. Wählen Sie auf der Registerkarte Administration die Optionen Benachrichtigungen, Benachrichtigungsmethoden, E-Mail aus. Klicken Sie dann auf Bearbeiten.
2. Aktivieren Sie auf der Seite E-Mail-Aktualisierungsbenachrichtigung - Methode das Kontrollkästchen unterstützt SMTP, um SMTP zu aktivieren.
3. Geben Sie **pdm_mail [-F from_email_address] [-T reply_to_email_address]** als Benachrichtigungsmethode ein.

E-Mail-Adresse "Von"

Gibt die Adresse an, die als "Von"-Adresse der Nachricht verwendet wird. Diese Adresse setzt die Absenderadresse in der Server-Konfiguration für ausgehende Post außer Kraft.

Antwort-E-Mail-Adresse

Gibt die Adresse an, an die Antworten geschickt werden. Diese Adresse setzt die Antwortadresse in der Server-Konfiguration für ausgehende Post außer Kraft.

Wenn eine Antwortadresse in der Server-Konfiguration für ausgehende Post festgelegt wird und keine Antwortadresse in der Benachrichtigungsmethode angegeben wird, wird die Antwortadresse in der Server-Konfiguration für ausgehende Post mit dieser Benachrichtigungsmethode verwendet.

Hinweis: Wenn das Schlüsselwort "\$(REPLY_FROM)" als Adresse angegeben wird, setzt sich diese Adresse aus dem Anwendernamen und Mail-Server-Hostnamen für das Postfach zusammen. Dieses Schlüsselwort ist nur gültig, wenn eine Postfachregel die Benachrichtigungsmethode verwendet.

Benachrichtigungsmethoden, die es verwenden, dürfen für keinen anderen Zweck benutzt werden. Beispiel: Anwendername=dev, Servername=mail32.ca.com, \$(REPLY_FROM)=dev@mail32.ca.com. Verwenden Sie dieses Schlüsselwort nur, wenn Ihr Mail-Server so konfiguriert ist, dass er den Mail-Servernamen als äquivalent zum E-Mail-Domännennamen akzeptiert. Verwenden Sie dieses Schlüsselwort mit Vorsicht: Wenn der Hostname in der Postfachkonfiguration keine vollständige Domänenerweiterung aufweist (zum Beispiel mailserver1 an Stelle von mailserver1.customer7.com), wird er nicht automatisch vom Feldübersetzungsprogramm erweitert.

Hinweis: Die E-Mail-Adresse "Von" und die Antwort-E-Mail-Adresse sind die Adressen, die in den Kopfzeilen "Von" und "Antwort an" der Nachricht angezeigt werden, wenn der Anwender sie liest. Wenn die Adressen identisch sind, können Sie nur die "Von"-Adresse angeben.

4. Klicken Sie auf "Speichern".

Die E-Mail-Benachrichtigungsmethode wurde geändert. Wenn der Kontakt auf die E-Mail-Benachrichtigung antwortet, wird die Antwort standardmäßig an das angegebene Postfach adressiert.

Weitere Informationen:

[Dienstprogramm "pdm mail" - Senden von E-Mail-Informationen](#) (siehe Seite 1209)

Identifizieren alternativer Absenderadressen

Sie können den Parameter "-n" im Betreff der Meldung verwenden, so dass CA SDM den Absender der Meldung identifiziert, der eine andere E-Mail-Adresse verwendet als diejenige, von der sie ursprünglich gesendet wurde. Das Schlüsselwort "-m" mit einem nachfolgenden Leerzeichen und der E-Mail-Adresse, die CA SDM erkennt, müssen die letzten Elemente der Betreffzeile sein. Beachten Sie Folgendes, wenn Sie den Parameter "-m" im Betreff verwenden:

- Sowohl die tatsächliche Absendeadresse als auch die alternative Adresse, die mit "-m" angegeben ist, werden in den Einschluss- und Ausschlusslisten überprüft.
- Die E-Mail-Adresse, die als die alternative Adresse angegeben ist, darf nur die Adresse und nicht den begleitenden Anzeigenamen enthalten.
- Wenn in der Betreffzeile mehr als ein Wort auf den Parameter "-m" folgt, wird die alternative Adresse nicht erkannt.

Postfachabfrage

Wenn ein Fehler auf dem ausgehenden Mail-Server auftritt, werden keine E-Mail-Benachrichtigungen gesendet und in das Warteschlangenverzeichnis `%NX_ROOT%\site\mail_queue` gestellt. Wenn der Mail-Server wieder aktiv wird, verarbeitet und sendet er nach einem gewissen Zeitabstand E-Mails. Sie können den Zeitabstand ändern, um die E-Mail wiederzuverwerten, die während der Belegung des Mail-Servers in die Warteschlange gestellt worden war.

E-Mail-Benachrichtigungen, die der ausgehende Mail-Server nicht gesendet hat, werden solange erneut gesendet, bis Sie Folgendes tun:

- Halten Sie den Mail Daemon (`pdm_mail_nxd`) an, der ausgehende E-Mail-Benachrichtigungen verarbeitet.
- Löschen Sie manuell die Nachrichten aus dem Verzeichnis `%NX_ROOT%\site\mail_queue`.

Festlegen der Variablen zu Wiederholungsintervallen für E-Mails

Sie können den Zeitabschnitt (in Sekunden) festlegen, in dem Fehlversuche bei der Übermittlung der E-Mail-Nachricht an den Mail-Server wiederholt werden.

Hinweis: CA SDM versucht nicht, E-Mail-Nachrichten erneut zu senden, wenn der ausgehende Mail-Server die Nachricht erhalten hat, diese jedoch nicht vom Anwender abgerufen werden kann. In diesem Fall werden die Regeln und Richtlinien zur Wiederholung bei Übertragungsfehlern des ausgehenden Mail-Servers angewendet, falls eingerichtet.

Wiederholungen werden jeweils für einzelne Nachrichten durchgeführt. Wenn der Mail-Server für einen Zeitraum nicht verfügbar ist, wird jede Nachricht solange erneut übertragen, wie für sie festgelegt ist. Es wird nicht versucht, alle Nachrichten des Übertragungsvorgangs erneut zu senden. Wenn der Daemon für ausgehende E-Mails wieder verfügbar ist, werden alle noch nicht gesendeten Nachrichten auf einmal übertragen. Schlägt dieser Übertragungsversuch fehl, werden die Zeitgeber für alle Nachrichten auf dieselbe Zeit zurückgesetzt.

Die Einstellung `"NX_EMAIL_RETRY_INTERVAL"` in der Datei `"NX.env"` steuert das Wiederholungsintervall. Sie können das Standardwiederholungsintervall auf einem oder mehreren Servern anpassen.

Gehen Sie wie folgt vor:

1. Melden Sie sich abhängig von Ihrer CA SDM-Konfiguration bei folgendem Server an:
 - Konventionell: Primärserver
 - Erweiterte Verfügbarkeit: Hintergrundserver.
2. Wechseln Sie in das Verzeichnis "\$NX_ROOT"
3. Öffnen Sie die Datei "NX.env" in einen Texteditor wie WordPad.
4. Ändern Sie den Wert des Intervalls in "NX_EMAIL_RETRY_INTERVAL" wie folgt:

`NX_EMAIL_RETRY_INTERVAL=number_of_seconds`

NX_EMAIL_RETRY_INTERVAL

Legt den Zeitabschnitt (in Sekunden) fest, in dem Fehlübertragungen von E-Mail-Nachrichten wiederholt werden.

number_of_seconds

Gibt die Anzahl von Sekunden für jedes E-Mail-Wiederholungsintervall an. Der Standardwert ist 600 Sekunden (10 Minuten). Der Minimalwert, den Sie verwenden können, beträgt 20 Sekunden. Wenn Sie einen Wert festlegen, der das Minimum (20 Sekunden) unter- oder 2000000 Sekunden überschreitet, wird der Standardwert von 10 Minuten verwendet.

5. Speichern und schließen Sie die Datei.
6. Starten Sie die CA SDM-Server neu. Weitere Informationen darüber, wie Sie abhängig von Ihrer CA SDM-Konfiguration den CA SDM-Server starten, finden Sie im Szenario "Neustart der CA SDM-Server", oder suchen Sie die Informationen im *Administrationshandbuch*.

Die Änderung wird übernommen.

Service Level Agreements (Dienstverträge)

Ein Service Level Agreement (SLA) oder Servicetyp ist eine Vereinbarung zwischen einem Service Desk und seinen Kunden und beschreibt gewöhnlich die Serviceebene, die durch den Service Desk geboten wird. Wenn diese Dienstebene nicht geboten wird, kann der Service Desk einer Strafe unterliegen. Ein Service Desk zum Beispiel, der auf der Basis „Zahlung pro Dienst“ arbeitet, erhält unter Umständen nicht die vollständige Zahlung für einen Dienst, der die vereinbarte Dienstebene nicht erfüllt. Folglich nehmen die meisten Service Desks Service Level Agreements sehr ernst und unternehmen jede Anstrengung, die in diesen Vereinbarungen festgelegte Art von Dienst zu erfüllen.

Des Weiteren führen die meisten Service Desks sorgfältige Aufzeichnungen (Datensätze) darüber, wann Service Level Agreements erfüllt oder verletzt werden. Die mit CA SDM definierten Diensttypen sollen den Service Desk-Mitarbeitern bei der Erfüllung ihrer Service Level Agreements helfen und sie bei der Führung der Aufzeichnungen unterstützen, anhand derer sie prüfen müssen, ob die Service Level Agreements erfüllt wurden.

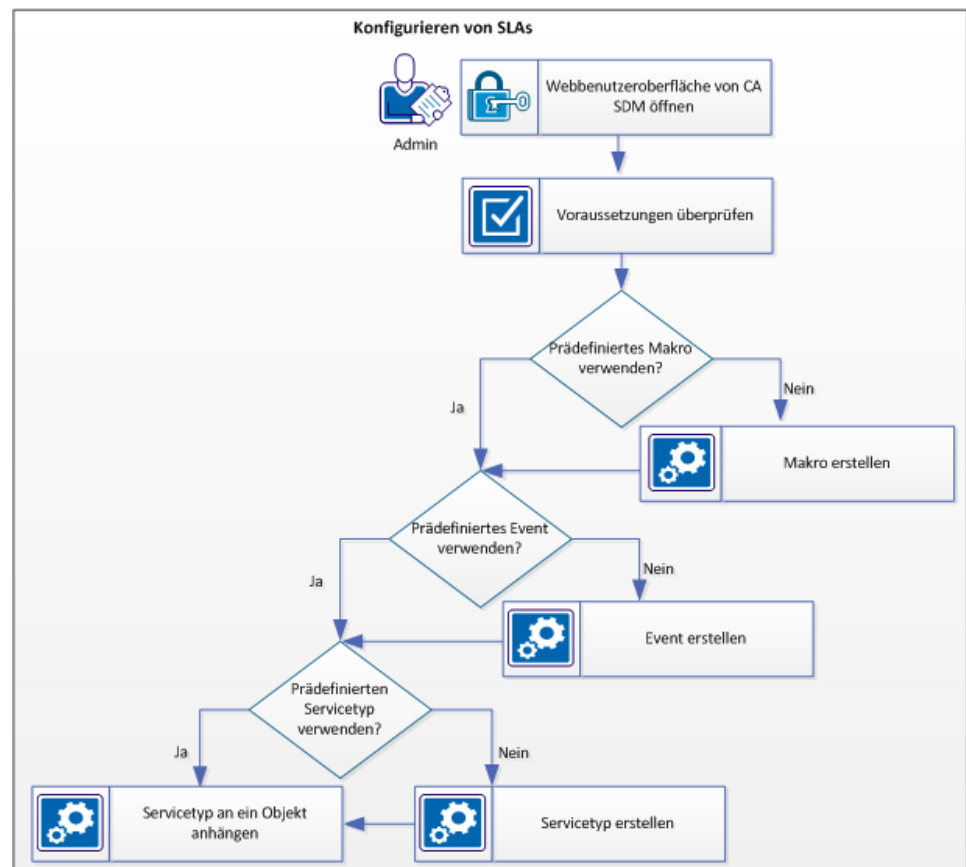
So konfigurieren Sie SLAs

In CA SDM beschreibt das SLA oder der Servicetyp die Service-Ebene, die der Service Desk-Analyst dem Kunden angibt. Um Ihre Unternehmensverpflichtungen und Ablaufpläne (die sich auf spezifische Tickets beziehen) zu verfolgen, werden Events an Servicetypen angehängt. Events werden verwendet, um die Bedingung, unter der der Servicetyp verletzt wird, und die Aktionen, die nach der Verletzung ausgeführt werden sollen, zu definieren. Jedes Event hat drei generische Verhaltensmerkmale: Bedingungen, Aktionen bei Wahr und Aktionen bei Falsch.

- Die Bedingung identifiziert den messbaren Status eines Tickets.
- Eine Aktion identifiziert die Prozesse, die automatisch ausgeführt werden, wenn die Bedingung nach einer bestimmten Zeitspanne wahr oder falsch ist.

Beispiel: Als Systemadministrator möchten Sie ein SLA von 24-Stunden für einen Hardware-Request festlegen. Anderenfalls wird eine E-Mail-Benachrichtigung an den Kunden-Support-Manager und an den Analysten gesendet. Dieses Beispiel wird im gesamten Szenario verwendet, um zu erklären, wie die E-Mail-Benachrichtigung für ein SLA konfiguriert wird.

Folgendes Diagramm zeigt, wie die 24 Stunden konfiguriert werden. Das SLA, das bei einer Verletzung eine E-Mail-Benachrichtigung sendet:



Gehen Sie wie folgt vor:

1. [Öffnen Sie die CA SDM-Web-Benutzeroberfläche](#) (siehe Seite 202).
2. [Überprüfen Sie die Voraussetzungen](#) (siehe Seite 268).
3. Wenn Sie kein vordefiniertes Makro verwenden möchten, [erstellen Sie ein Makro](#) (siehe Seite 274).
4. Wenn Sie kein vordefiniertes Event verwenden möchten, [erstellen Sie ein Event](#) (siehe Seite 276).
5. Wenn Sie keinen vordefinierten Servicetyp verwenden möchten, [erstellen Sie einen Servicetyp](#) (siehe Seite 280).
6. [Hängen Sie den Servicetyp an ein Objekt an](#) (siehe Seite 282).

Öffnen der CA SDM-Web-Benutzeroberfläche

Melden Sie sich in der Web-Benutzeroberfläche aus folgenden Servern an, abhängig von Ihrer CA SDM-Konfiguration:

- Konventionell: Primärserver oder Sekundärserver
- Erweiterte Verfügbarkeit: Anwendungsserver oder Hintergrundserver

Überprüfen der Voraussetzungen

Bevor Sie das Service Level Agreement konfigurieren, stellen Sie sicher, dass Sie folgende Schritte durchgeführt haben:

- Installation der [SLA-Optionen](#), (siehe Seite 268) die für die Anforderungen Ihrer Organisation erforderlich sind.
- [Die Benachrichtigungsmethode für den Empfänger ist bestätigt](#) (siehe Seite 203)
- [Eine Meldungsvorlage sollte erstellt sein](#) (siehe Seite 205), wenn Sie bei einer SLA-Verletzung eine E-Mail-Benachrichtigung senden möchten, und wenn Sie keine vordefinierte Meldung verwenden möchten.

Optionen für SLA

Installieren Sie je nach Anforderungen Ihrer Organisation die SLA-Optionen, die für die Einrichtung der SLA erforderlich sind.

Zum Beispiel kann in der "klassischen" SLA-Behandlung (aktiviert, falls die Option "classic_sla_processing" im Optionsmanager installiert wurde) nur ein Servicetyp gleichzeitig auf ein Ticket angewendet werden. Wenn verschiedenen Attributen in einem Ticket verschiedene Diensttypen zugewiesen sind, wird der Diensttyp mit der höheren Einstufung verwendet. Die Einstufung eines Diensttyps wird bei seiner Erstellung definiert. Die höchste Einstufung ist 1, die nächste 2 usw. Angenommen, dem Issue, der den Servicetyp einer Lösung in 12 Stunden (Einstufung 2) hat, wurde der Prioritätscode 1 zugewiesen. Dieser hat den Servicetyp einer Lösung in 4 Stunden (Einstufung 1). Der höher eingestufte Servicetyp bestimmt das Dienstverhalten für den zugehörigen Issue. In diesem Beispiel ist die Lösung in 4 Stunden höher als die Lösung in 12-Stunden eingestuft. Somit wird der Servicetyp einer Lösung in 4 Stunden für den Issue verwendet.

Folgende Optionen können über den Optionsmanager installiert werden:

Hinweis: Weitere Informationen zur Installation und zur Deinstallation einer Option finden Sie in der *Online-Hilfe*.

Option	Beschreibung
change_allow_sla_downgrade	Verändert das Verhalten der Option "chg_sla", so dass das System den Diensttyp eines Change automatisch herunterstufen kann. Die Option "chg_sla" wählt aus mehreren Change-Attributen den besten Servicetyp aus, kann jedoch den aktuellen Servicetyp nicht durch einen mit niedrigerem Rang ersetzen. Bei installierter Option wird der Diensttyp für alle betroffenen Attribute bewertet, wenn sich ein Attribut ändert. Der Diensttyp des Change wird auf den höchsten gefundenen Typ festgelegt, selbst wenn der neue Diensttyp einen niedrigeren Rang aufweist als der aktuelle Diensttyp des Change. Der beste Service ist der Diensttyp mit dem niedrigsten Rangwert. Bei gleichem Rang aller Diensttypen (einschließlich der Diensttypen ohne Rangwert) wird der zuerst in der Datenbank angelegte Diensttyp markiert. Damit diese Option ordnungsgemäß funktioniert, muss die Option "chg_sla" installiert werden. Sie können ähnliche Optionen für Issues und Requests installieren.
ttv_enabled	Startet den Verletzungszeitpunkt-Daemon, der die SLA für alle offenen Tickets und Aufgaben überwacht. Dieser Prozess legt nicht die SLA-Verletzung fest, sondern registriert den Zeitpunkt, an dem das Ticket oder die Aufgabe im jeweils aktuellen Status verletzt wird. Diese Erwartung wird bei Aktualisierung des Tickets oder der Aufgabe aktualisiert. Diese Option muss installiert werden, damit die anderen Optionen für den Verletzungszeitpunkt ordnungsgemäß funktionieren. Wichtig! Für diese Option ist es nicht erforderlich, die Option "classic_sla_processing" zu installieren.

set_sla_evt_open_date	Verwendet den Wert für das Datum und die Uhrzeit beim Öffnen eines Change, Issue oder Request als Startdatum und Startzeit für angehängte Events. Die angehängten Events werden ausgelöst, sobald das Ticket gespeichert wird.

Bestätigen der Benachrichtigungsmethode für den Empfänger

Stellen Sie sicher, dass der Kontakt, dem Sie die Benachrichtigung senden möchten, zu dieser bestimmten Benachrichtigungsmethode zugewiesen ist.

Gehen Sie wie folgt vor:

1. Wählen Sie auf der Registerkarte "Administration" die Option "Sicherheit und Rollenverwaltung" > "Kontakte".
Die Seite "Kontakt - Suche" wird geöffnet.
2. Suchen Sie mithilfe des Filters nach dem Kontakt, und wählen Sie aus dem Suchergebnis den Kontakt aus, den Sie benachrichtigen möchten.
Die Seite der Kontaktdetails wird geöffnet.
3. Wählen Sie Benachrichtigung auf der Registerkarte Kontaktdetails aus.
4. Bestätigen Sie die Benachrichtigungsmethode. Wählen Sie basierend auf Ihrer Benachrichtigungspriorität die erforderliche Option aus. Zum Beispiel möchten Sie eine E-Mail-Benachrichtigung für Notfallbenachrichtigungen senden. Aktivieren Sie die Option E-Mail im Feld Notfall.
5. Um die Benachrichtigungsmethode zu ändern, klicken Sie auf Bearbeiten, ändern Sie die Option, und klicken Sie auf Speichern.

Die Benachrichtigungsmethode für den Kontakt wird überprüft.

Erstellen von Meldungsvorlagen

Erstellen Sie eine Meldungsvorlage, die die Werte für die Verwendung der Benachrichtigung enthält. Wenn Sie mehrere Benachrichtigungen senden, können Sie mithilfe der Meldungsvorlagen Ihre Auslastung vereinfachen.

Hinweis: Wenn die Mandantenfähigkeit installiert ist, wählen Sie in der Dropdown-Liste den entsprechenden Mandanten aus. Mit der Option "öffentlich (freigegeben)" wird das Objekt für alle Mandanten erstellt.

Gehen Sie wie folgt vor:

1. Wählen Sie Benachrichtigungen, Meldungsvorlagen in der Registerkarte "Administration" aus.

Die Seite "Meldungsvorlagen - Liste" wird geöffnet.

2. Klicken Sie auf "Neu erstellen".

Die Seite "Neue Meldungsvorlage erstellen" wird angezeigt.

3. Füllen Sie die Felder nach Wunsch aus.

Symbol

Definiert ein eindeutiges Kennzeichen für diese Meldungsvorlage.

Objekttyp

Gibt den Objekttyp an, der mit dieser Vorlage verknüpft ist. Wählen Sie zum Beispiel Request/Incident/Problem für eine Benachrichtigung aus, die sich auf ein Ticket bezieht.

Datensatzstatus

Gibt den Status der Vorlage entweder als aktiv oder inaktiv an. Legen Sie den Status auf Aktiv fest, um die Meldungsvorlage zu verwenden.

Automatische Benachrichtigung

Gibt an, dass die Benachrichtigung, die mit dieser Vorlage verknüpft ist, automatisch gesendet wird, wenn die Aktivität auftritt. Angenommen, Sie richten eine Anfangsbenachrichtigung, die zu benachrichtigenden Objekte und die Meldungsvorlage ein, möchten aber noch nicht die Benachrichtigungen aktivieren. In diesem Fall aktivieren Sie nicht "Automatische Benachrichtigung". Wenn Sie zum Starten von automatischen Benachrichtigungen bereit sind, aktivieren Sie das Kontrollkästchen. Die Benachrichtigung wird aktiviert und erfolgt wie definiert.

Benachrichtigungsebene

Zeigt die relative Gewichtung dieser Benachrichtigung an. Wählen Sie zum Beispiel "Notfall" aus, wenn die E-Mail-Benachrichtigung sofort an den Kontakt gesendet werden soll, wenn die verknüpfte Aktivität auftritt.

Titel der Benachrichtigungsmeldung

Gibt den Zusammenfassungstitel der Meldung an. Sie können Variablen verwenden, um die Incident-Nummer im Meldungstitel einzufügen. Zum Beispiel: @{call_req_id.type.sym} @{call_req_id.ref_num} @{type.sym}.

Benachrichtigungstext

Gibt den Inhalt der Meldung an. Sie können Variablen verwenden, um den Analystnamen, den Namen des Endanwenders und die Beschreibung in die Meldung einzufügen. Beispiel:

@{call_req_id.type.sym} @{call_req_id.ref_num} @{type.sym}.

Zugewiesen zu: @{call_req_id.assignee.combo_name}

Kunde: @{call_req_id.customer.combo_name}

Beschreibung: @{call_req_id.description}

Klicken Sie zum Anzeigen auf die folgende URL:

@{call_req_id.web_url}

Sie können das ARTEFAKT-Schlüsselwort benutzen, um anzugeben, wie Artefakte in ausgehenden Meldungen, Meldungsvorlagen, Benachrichtigungen und automatischen Antworten gehandhabt werden. Das ARTEFAKT-Schlüsselwort benutzt die folgenden Werte:

- **NONE:** Gibt an, dass Artefakte nicht validiert werden. Dieser Wert ist der gleiche, als ob Sie kein Schlüsselwort benutzen.
- **PROTECTED:** Tickets werden zur Bestätigung auf das Vorhandensein der Raute validiert. Wenn die Bestätigung scheitert, wird das Artefakt als ungültig angesehen, und das Filtern schlägt fehl, wenn das Filter die Suche nach einem Artefakt ({{object_id}}) bedeutet.
- **SICHER** - Entschlüsselt die Ticketnummer. Wenn der Wert kein gültiges Kennwort ist, wird das Artefakt als ungültig angesehen, und das Filtern schlägt fehl, wenn das Filtern die Suche nach einem Artefakt ({{object_id}}) bedeutet.

HTML-Meldung

Gibt die HTML-Meldung an, die dem Empfänger angezeigt wird. Wenn der Empfänger die Meldung auf einem Mobilgerät, wie z. B. einem Handy oder PDA, erhält, wird sie im Nur-Text-Format angezeigt. Klicken Sie auf HTML-Meldung bearbeiten, um den HTML-Editor zu öffnen.

Schnellansicht

Zeigt die Meldung an, wie sie für den Empfänger angezeigt wird.

HTML-Quelle

Zeigt die Meldung im HTML-Quellcode an.

4. Klicken Sie auf "Speichern".

Die Meldungsvorlage wird erstellt.

Erstellen eines E-Mail-Benachrichtigungsmakro

Sie können Makros erstellen, die verwendet werden können, um Objekten Aktionen hinzuzufügen oder eine Überprüfung auf bestimmte Merkmale oder Bedingungen durchzuführen.

Hinweis: Wenn die Mandantenfähigkeit installiert ist, wählen Sie in der Dropdown-Liste den entsprechenden Mandanten aus. Mit der Option "öffentlich (freigegeben)" wird das Objekt für alle Mandanten erstellt.

Gehen Sie wie folgt vor:

1. Wählen Sie auf der Registerkarte "Administration" die Optionen "Events und Makros", "Makros" aus.

Die Seite "Makroliste" wird geöffnet.

2. Klicken Sie auf "Neu erstellen".

Die Seite "Neues Makro erstellen" wird angezeigt.

3. Füllen Sie die Felder wie folgt aus:

Symbol

Geben Sie eine beschreibende Kennung für das Makro ein.

Makrotyp

Wählen Sie den Typ für dieses Makro aus. Vom ausgewählten Makrotyp wird kontrolliert, welche übrigen Daten bereitgestellt werden müssen.

Hinweis: Die Option "CA IT-PAM-Aktion ausführen" kann nur ausgewählt werden, wenn der CA IT-PAM-Workflow in CA SDM konfiguriert ist. Hinweis: Die Option "CA Workflow-Aktion ausführen" kann nur ausgewählt werden, wenn der CA Workflow in CA SDM konfiguriert ist.

Objektyp

Wählen Sie den Objektyp aus, auf dem das Makro ausgeführt werden kann.

4. Klicken Sie auf "Fortsetzen".

Auf Basis des ausgewählten Makrotyps wird die Seite mit den übrigen Daten ausgefüllt, die für das Makro erforderlich sind.

Hinweis: Wählen Sie wie im Beispiel das Marko [Mehrere Benachrichtigungen](#) (siehe Seite 274) als Makrotyp aus, um bei einer SLA-Verletzung eine E-Mail-Benachrichtigung zu senden. Weitere Informationen zu anderen Makrotypen finden Sie in der *Online-Hilfe*.

Makro "Mehrere Benachrichtigungen"

Mit einem Makro dieses Typs können Sie einem oder mehreren Kontakten eine Benachrichtigung senden. Sie können die zu sendende Meldung, die Empfänger der Meldung und die Dringlichkeitsstufe angeben.

Gehen Sie wie folgt vor:

1. Geben Sie den Vorlagennamen direkt in das Feld Meldungsvorlage ein, oder klicken Sie auf das Symbol "Suchen", um die gewünschte Vorlage auszuwählen. Diese Vorlage wird verwendet, um die Benachrichtigung zu erstellen.
2. Klicken Sie auf "Speichern".
3. Wählen Sie die zu benachrichtigenden Kontakte auf den folgenden Registerkarten aus:

Hinweis: Mit der Schaltfläche "Kontakte aktualisieren" auf jeder Registerkarte können Sie weitere Kontakte für die Benachrichtigung suchen und auswählen.

Objektkontakte

Zeigt die verfügbaren Organisationen, Anbieter und Configuration Items für den ausgewählten Objekttyp an, die eine Benachrichtigung zu Tickets erhalten. Zum Beispiel können Sie "Betroffener Endanwender" oder die Organisation der betroffenen Endanwender, die benachrichtigt werden sollen, auswählen.

Kontakte

Zeigt die Personen an, die dem Benachrichtigungsmakro hinzugefügt sind, unabhängig von ihrer Zuordnung zum Ticket.

Kontakttypen

Zeigt die Anwender an, die innerhalb der Benachrichtigungsmakro mit der gleichen Klassifizierung definiert sind, z. B. Analysten oder Kunden.

4. Klicken Sie auf "Speichern".

Das Makro "Mehrere Benachrichtigungen" wird erstellt.

Erstellen von Events

Erstellen Sie ein Event, und hängen Sie diesem Event ein Makro an. Dieses Event wird ausgeführt, nachdem ein bestimmter Zeitpunkt abgelaufen ist. Wenn ein Makro angehängt ist, dann wird eine Aktion ausgeführt.

Hinweis: Wenn die Mandantenfähigkeit installiert ist, wählen Sie in der Dropdown-Liste den entsprechenden Mandanten aus. Mit der Option "öffentlich (freigegeben)" wird das Objekt für alle Mandanten erstellt.

Gehen Sie wie folgt vor:

1. Wählen Sie auf der Registerkarte "Administration" die Optionen "Ereignisse und Makros", "Events" aus.

Die Seite Events - Liste wird geöffnet.

2. Klicken Sie auf "Neu erstellen".

Die Seite "Neues Event erstellen" wird geöffnet.

3. Füllen Sie die Event-Felder und die Konfigurationsinformationen aus.

Klicken Sie auf "Speichern".

4. Um diesem Event das Makro hinzuzufügen, geben Sie die [Aktionsinformationen](#) (siehe Seite 278) an.

Das neue Event wird gespeichert.

Weitere Informationen:

[Events - Felder](#) (siehe Seite 276)

[Konfigurationsinformationen - Felder](#) (siehe Seite 277)

[Felder der Aktionsinformationen](#) (siehe Seite 278)

Events - Felder

Füllen Sie folgende Felder aus, um ein Event hinzuzufügen oder zu bearbeiten:

Name

Der Name des Event.

Objekttyp

Zeigt an, ob das Event an ein Issue, einen Request, einen Change, eine Workflow-Aufgabe, ein Knowledge-Dokument, eine Knowledge-Berichtskarte, eine Unterstützungssitzung oder eine verwaltete Umfrage angehängt ist.

Dieses Feld kann nur beim Erstellen eines Events bearbeitet werden. Dieses Feld ist schreibgeschützt, wenn Sie das Event aktualisieren möchten.

Datensatzstatus

Zeigt an, ob das Event aktiv oder inaktiv ist. Es können nur aktive Events verwendet werden.

Konfigurationsinformationen - Felder

Füllen Sie folgende Felder aus, um die Konfigurationsinformationen hinzuzufügen oder zu bearbeiten:

Zeitverzögerung

Gibt den Zeitpunkt an, nach dem das Event ausgelöst wird.

Wiederholungszeitverzögerung

Gibt die Zeitspanne an, nach dem das Event erneut ausgelöst werden soll.

Zurücksetzen der Zeit zulassen

Gibt an, ob ein Service Desk-Analyst die Zeitverzögerung ändern kann. Diese Option muss ausgewählt werden, damit ein Event als Servicetyp-Event verwendet werden kann (ein Event, das mit einer Service-Ebene, wie z. B. der 4-Stunden-Lösung, verknüpft ist).

Schicht

Gibt die Daten, Tage und Stunden an, in denen der Servicetyp aktiv ist.

Markierung "Event abgeschlossen"

Gibt die Aktion an, die durchgeführt werden soll, sobald das Event abgeschlossen wurde.

Event wiederholen

Wiederholt das Event mit dem angegebenen Zeitintervall, bis der Issue geschlossen wird.

Verlauf speichern

Zeichnet den Verlauf der Aktivitäten für das Event auf.

Kein Verlauf

Es wird kein Verlauf für das Event aufgezeichnet. Das Event erscheint nicht im Fenster "Event-Verlauf".

Bedingung

Zeigt das Makro (wenn mit dem Event verknüpft) an, das die Bedingung anzeigt, die durch das Event geprüft wird.

Text

Definiert die Event-Konfiguration. Bei einigen Aktionsmakros wird dieses Feld für einen bestimmten Zweck genutzt. Im Aktionsmakro "Übertragung in Event-Kontakt" enthält es z. B. die Anwender-ID der Person, zu der Sie ein Ticket übertragen möchten.

Felder der Aktionsinformationen

Wählen Sie die Aktionen, die mit dem Event verbunden werden sollen, wie folgt aus:

1. Klicken Sie auf die Registerkarte "Aktionsinformationen".
2. Wählen Sie ein oder beide Kontrollkästchen "SLA-Verletzung für Aktionen nach Wahr-/Falsch-Makro festlegen" aktivieren. Wenn diese Kontrollkästchen aktiviert sind, wird bei einer wahren Bedingung oder einer falschen Bedingung für das Event eine SLA-Verletzung (Service Level Agreement) protokolliert.

Hinweis: Geben Sie entsprechende Makros für eine wahre oder falsche Bedingung unter der Aktionsliste an, um die SLA-Verletzungen zu protokollieren.

3. Klicken Sie auf "Aktionen bei 'Wahr' aktualisieren".

Die Seite "Makros - Suche" wird geöffnet.

4. Suchen Sie nach den Makros, die ausgeführt werden sollen, wenn die Event-Bedingung wahr ist.
5. Wählen Sie die gewünschten Makros aus der Liste auf der linken Seite aus, und klicken Sie auf "Weitere" (>).

Die ausgewählten Makros werden der Liste auf der rechten Seite hinzugefügt.

6. Wenn sich alle gewünschten Makros in der Liste auf der rechten Seite befinden, klicken Sie auf "OK".

Die ausgewählten Makros werden in der Liste "Aktionen bei Makroliste 'Wahr'" angezeigt.

7. Klicken Sie auf "Aktionen bei 'False' aktualisieren", und wiederholen Sie das vorherige Verfahren zur Auswahl der Makros, die ausgeführt werden sollen, wenn die Ereignisbedingung falsch ist.

Anpassen von Servicetypen

Sie können einen Servicetyp erstellen, der Ihre Anforderungen erfüllt. Sie können auch einen vordefinierten Servicetyp ändern.

Gehen Sie wie folgt vor:

1. Wählen Sie auf der Registerkarte "Administration" die Option "Service Desk" > "Servicetypen".

Die Seite "Serviceverträge - Liste" wird geöffnet.

2. Klicken Sie auf "Neu erstellen".

Die Seite "Neuen Servicetyp erstellen" wird geöffnet.

3. Wenn die Mandantenfähigkeit installiert ist, wählen Sie in der Drop-down-Liste den entsprechenden Mandanten aus. Mit der Option "öffentlich (freigegeben)" wird das Objekt für alle Mandanten erstellt.

4. Füllen Sie die folgenden Felder nach Wunsch aus:

Symbol

Definiert eine eindeutige ID für den Servicetyp. In diesem Beispiel weisen Sie das Symbol als "24_hr_resolution" zu.

Einstufung

Definiert eine Einstufung für den Servicetyp. In diesem Beispiel kann das Ticket der Hardware-Request mit mehreren Servicetypen verknüpft werden. Der Einstufungswert bestimmt den anwendbaren Servicetyp. Der Servicetyp mit der niedrigsten Einstufung hat die höchste Priorität.

Geben Sie 1 ein.

Schicht

Gibt die Daten, Tage und Stunden an, in denen der Servicetyp aktiv ist. Für Schichten gelten die folgenden Regeln:

- Wenn Sie eine Schicht auf einen Servicetyp anwenden, müssen Sie den Service anhalten und erneut starten, damit die Schicht sofort in Kraft tritt.
- Wenn eine Schicht für einen Servicetyp, jedoch nicht für ein Event angegeben ist, gilt die Schicht des Servicetyps.
- Wenn eine Schicht für ein Event, jedoch nicht für einen Servicetyp angegeben ist, wird die Schicht des Servicetyps ignoriert.
- Sind für das Event und den Servicetyp Schichten angegeben, wird die Schicht des Servicetyps ignoriert.

Zeitzone

Gibt die Zeitzone für den Servicetyp an. Diese Zeitzone wird zum Auslösen von Ereignissen im System verwendet, wenn die Option "Zeitzone des Endanwenders verwenden" nicht aktiviert ist.

Zeitzone des Endanwenders verwenden

Gibt die Zeitzone des betroffenen Endanwenders an, um die Events auszulösen.

Kosten der Verletzung

Gibt die Kosten an, die anfallen, wenn die Zeitbeschränkung für den Servicetyp überschritten wird.

5. Klicken Sie auf "Speichern".

Der Servicetyp wird gespeichert.

6. Um ein Servicetyp-Event anzuhängen, wählen Sie die entsprechende Registerkarte aus (Requests, Changes, Change-Aufgaben, Issues oder Issue-Aufgaben), und klicken Sie auf "Servicetyp-Event hinzufügen".

Die Seite "Neues Servicetyp-Event erstellen" wird geöffnet.

7. Klicken Sie auf Event.

Die Seite Events - Liste wird geöffnet.

8. Führen Sie eine der folgenden Aktionen aus:

- Klicken Sie auf "Neu erstellen", um ein neues Event zu erstellen. Füllen Sie die Event-Felder und die Konfigurationsinformationen aus. Um diesem Event ein Makro hinzuzufügen, geben Sie die [Aktionsinformationen](#) (siehe Seite 278) an.
- Wählen Sie ein vorhandenes Event aus der Liste. Sie können die Filterkriterien verwenden, um nach einem Event zu suchen.

Das ausgewählte oder erstellte Event wird im Feld Event angezeigt.

9. Klicken Sie auf "Fortsetzen".

Die Detailseite des Servicetypen wird mit dem angehängten Event angezeigt.

Anhängen des Servicetyps an ein Objekt

Servicetypen können mit verschiedenen Objekten, wie z. B. Kontakten, Organisationen, Kategorien und Prioritätscodes, verknüpft werden. Wie im Beispiel hängen Sie den Servicetyp an den Incident-Bereich an, in diesem Fall "Hardware".

Gehen Sie wie folgt vor:

1. Öffnen Sie das verknüpfte Ticket, für das Sie ein SLA zuweisen möchten.
2. Klicken Sie im Feld "Incident-Bereich" auf Hardware.
Das Fenster "Request-/Incident-/Problembereich aktualisieren" für Hardware wird angezeigt.
3. Klicken Sie auf "Bearbeiten".
4. Klicken Sie auf "Servicetyp".
Die Seite "Serviceverträge - Liste" wird geöffnet.
5. Suchen Sie nach dem Servicetyp "24_hr_resolution", den Sie erstellt haben.
6. Klicken Sie im Suchergebnis auf "24_hr_resolution".
Die Seite "Request-/Incident-/Problembereich aktualisieren" für Hardware wird mit dem aktualisierten Servicetyp geöffnet.
7. Klicken Sie auf "Speichern".
Der Servicetyp wird dem Incident-Bereich der Hardware angehängt.

Verzögern oder Fortsetzen eines Servicetyp-Event

Sie können Servicetyp-Events verzögern und fortsetzen.

So verzögern Sie ein Event:

1. Wählen Sie auf der Registerkarte "Service Desk" das gewünschte Ticket auf der Listenseite aus.
Die Seite "Ticket - Detail" wird angezeigt.
2. Wählen Sie die Registerkarte "Servicetyp" aus.
Es wird eine Liste aller dem Ticket hinzugefügten Servicetyp-Events angezeigt.
3. Klicken Sie auf "Verzögerung".
Die Seite "Grund" wird angezeigt.
4. Geben Sie den Grund für die Verzögerung des Event ein, und klicken Sie auf "OK".
Die Detailseite "Ticket" zeigt den Status des Event als "Verzögert" an.

So nehmen Sie ein Event wieder auf:

1. Wählen Sie auf der Registerkarte "Service Desk" das gewünschte Ticket auf der Listenseite aus.
Die Seite "Ticket - Detail" wird angezeigt.
2. Wählen Sie die Registerkarte "Servicetyp" aus.
Es wird eine Liste aller dem Ticket hinzugefügten Servicetyp-Events angezeigt.
3. Klicken Sie auf "Fortsetzen".
Die Seite "Grund" wird angezeigt.
4. Geben Sie den Grund für die Fortsetzung des Event ein, und klicken Sie auf "OK".
Die Detailseite "Ticket" zeigt den Status des Event als "In Bearbeitung" an.

Erstellen von Servicezielen

Um die SLA-Verletzungen zu minimieren, können Sie einen Satz von Servicezielvorlagen erstellen, um jede Stufe einer Ticket-Lösung zu messen. Wie Servicetypen enthält jedes Serviceziel eine Bedingung und eine Schätzung der Beendigungszeit. Allerdings bieten Serviceziele keinen Aktionsmechanismus.

Während der Ticket-Erstellung wird ein Servicetyp einem oder mehreren Servicezielen zugewiesen, damit jede Phase der Ticket-Lösung nachverfolgt werden kann. Immer, wenn sich ein Ticket ändert, bewerten die aktiven Serviceziele die Bedingung. Wenn die entsprechende Bedingung erfüllt ist, zeigen Ticket und Aktivitätsprotokoll die aktuelle Abschlusszeit an. Wenn die tatsächliche Zeit die geschätzte Zeit übersteigt, zeigt das Ticket die Zeitdifferenz zur Zielzeit an.

Mit Servicetypen können Sie folgende Aktionen durchführen:

- prüfen, ob Tickets desselben Servicetyps denselben Servicezielen folgen.
- überwachen, ob Tickets innerhalb der erforderlichen Zeitrahmen geschlossen werden.
- Informationen anzeigen, wie etwa die restliche Anzahl von Minuten, bevor ein Serviceziel abgeschlossen wird.

Berücksichtigen Sie beim Erstellen von Servicezielvorlagen die folgenden Punkte:

- Berücksichtigen Sie das erforderliche Ergebnis für das Erreichen des Serviceziels. Verwenden Sie eine existierende Bedingung oder ein standortdefiniertes Bedingungs makro, um Ticket-Daten auszuwerten. Passen Sie im Bedarfsfall ein Makro an oder schreiben Sie ein neues Makro für das Serviceziel.
- Kalkulieren Sie die erwartete Verletzung und die auf SLA-Abkommen basierten Abzüge.
- Weisen Sie einem Servicetyp mindestens eine Servicezielvorlage zu.

Gehen Sie wie folgt vor:

1. [Erstellen Sie eine Servicezielvorlage](#) (siehe Seite 285) zum Verwalten von Requests, Incidents, Problemen, Changes oder Issues.
2. [Verknüpfen Sie die Servicezielvorlage mit einem Servicetyp](#) (siehe Seite 286).
3. Weisen Sie das Detail der Servicezielvorlage einer Ticket-Kategorie zu, wie zum Beispiel Request-, Incident-, Problem-, Change- oder Issue-Tickets.

Bei der Ticket-Erstellung wird dem Ticket die entsprechende Vorlage auf der Basis des Servicetyps automatisch zugewiesen. Wenn ein Anwender ein Ticket erstellt, wird der Status des Serviceziels automatisch auf der Registerkarte "Servicetyp" angezeigt.

Erstellen von Servicezielvorlagen

Sie können eine Servicezielvorlage erstellen, um Serviceziele für Requests, Incidents, Probleme, Issues oder Changes zu messen. Nachdem Sie die Vorlage erstellt haben, können Sie sie mit einem Servicetyp verknüpfen.

Hinweis: Wenn die Funktion für mehrere Mandanten installiert ist, geben Sie den Mandanten im Feld "Mandant" an.

Gehen Sie wie folgt vor:

1. Wählen Sie auf der Registerkarte "Administration" die Option "Service Desk" > "Servicezielvorlagen".

Die Seite "Servicezielvorlage - Liste" wird angezeigt.

2. Klicken Sie auf "Neu erstellen".

Die Seite "Neue Servicezielvorlage erstellen" wird geöffnet.

3. Wählen Sie ein Tickettyp aus dem Feld Objekttyp aus, und klicken Sie auf "Fortfahren".

4. Füllen Sie die folgenden Felder nach Wunsch aus:

Name

Definiert eine beschreibende Kennung für das Serviceziel.

Objekttyp

Identifiziert den Ticket-Typ für das betreffende Serviceziel.

Zieldauer

Gibt die maximale Dauer bis zum Abschluss der Zielvorlage im Format hh:mm:ss an.

Schicht

Gibt die Schicht an, die einen Bereich von Arbeitsstunden enthält, die in Zeitberechnungen für ein Serviceziel verwendet werden. Zum Beispiel, M-F 08:00-17:00.

Kosten

Definiert Informationen, wie die geschätzten Kosten, die mit dem Verfehlen des Serviceziels verbunden sind.

Datensatzstatus

Zeigt an, ob dieses Ziel aktiv oder inaktiv ist.

Bedingung

Gibt den Namen des Bedingungs makros oder der standortdefinierten Bedingung an, das/die die Ticket-Daten auswertet und ermittelt, ob das Serviceziel erfüllt wird.

Erforderlicher Ausgang

Gibt einen Wahr- oder Falsch-Wert an, der anzeigt, ob das Serviceziel abgeschlossen ist.

Festlegen des Ist-Aufwands zulassen

Gibt an, ob es Anwendern erlaubt ist, Datum und Uhrzeit für ein Serviceziel festzulegen.

Zurücksetzen des Ist-Aufwands zulassen

Gibt an, ob es Anwendern erlaubt ist, Datum und Uhrzeit für ein Serviceziel zurückzusetzen.

5. Klicken Sie auf "Speichern".

Die Servicezielvorlage wird erstellt.

Verknüpfen einer Servicezielvorlage mit einem Servicetyp

Wenn Sie eine Servicezielvorlage mit einem Servicetyp verknüpfen, werden die Ziele beim Zuweisen des Servicetyps automatisch an ein Ticket angehängt. Sie können eine Servicezielvorlage nur einmal einem Servicetyp zuweisen. Es können viele verschiedene Serviceziele mit einem Servicetyp verknüpft werden.

Gehen Sie wie folgt vor:

1. Wählen Sie auf der Registerkarte "Administration" die Option "Service Desk" > "Servicetypen".

Die Seite "Serviceverträge - Liste" wird geöffnet.

2. Wählen Sie einen Servicetyp aus.

Die Seite "Servicetypen - Detail" wird geöffnet.

3. Wählen Sie die Zielregisterkarte für den ausgewählten Objekttyp aus. Wenn Sie zum Beispiel das Serviceziel für Requests erstellt haben, wählen Sie die Registerkarte "Request-Ziele" aus, um Problem-, Incident- und Request-Tickets zu verwalten.

4. Klicken Sie auf "Servicezielvorlage verknüpfen".

Die Seite "Neue verknüpfte Servicezielvorlage erstellen" wird geöffnet.

5. Sie können direkt einen Wert eingeben oder auf das Lupensymbol klicken, um nach einem Serviceziel zu suchen.

6. Klicken Sie auf "Fortsetzen".

7. Nehmen Sie im Bedarfsfall Änderungen an der Servicezielvorlage vor.

8. Klicken Sie auf "Speichern".

Die Servicezielvorlage wird mit dem Servicetyp verknüpft.

Anzeigen von Ticket-Zählern und -Timern für Serviceziele

Wenn ein Analyst einen Satz von Servicezielen einem Ticket zugewiesen hat, können Sie den Status und die Termine für den Abschluss jedes einzelnen Ziels anzeigen.

So zeigen Sie Ticket-Zähler und -Timer für ein Serviceziel an:

1. Zeigen Sie auf der Registerkarte "Service Desk" eine Liste von Incidents, Problemen, Requests, Changes oder Issues an.

Die Seite "Ticket - Detail" wird angezeigt.

2. Klicken Sie auf die Registerkarte "Servicetyp".

Unten auf dem Ticket werden weitere Servicetypinformationen angezeigt.

3. Klicken Sie in der Spalte "Ziel" auf das Serviceziel, um zusätzliche Informationen zu erhalten.

Der Abschnitt "Ticket-Zähler und -Timer" wird am unteren Rand der Detailseite des zugewiesenen Serviceziels angezeigt. Auf der Detailseite des zugewiesenen Serviceziels folgende Felder zur Verfügung:

Name

Zeigt den Namen des Serviceziels an.

Zieldauer

Zeigt den Zeitrahmen an, der zur Ausführung des Serviceziels vorgemerkt wurde. Sie können diesen Wert nur durch Bearbeiten des Tickets überschreiben.

Schicht

Zeigt den Ablaufplan für zeitliche Berechnungen im Zusammenhang mit dem Serviceziel an.

Bedingung

Zeigt die Bedingung oder das vom Standort definierte Bedingungs makro an, mit denen die Ticketdaten ausgewertet werden und errechnet wird, ob die Arbeit innerhalb des Zielzeitrahmens abgeschlossen werden kann.

Erforderlicher Ausgang

Zeigt das erforderliche Ergebnis der Bedingung oder des standortdefinierten Bedingungs makros an.

Kosten

Zeigt den für das Verfehlen des Zieles anfallenden Abzug an. Diese Informationen werden auch auf dem Ticket angezeigt.

Zieldatum/-uhrzeit

Zeigt den Fälligkeitstermin des Serviceziels an. Wenn ein Ticket zurückgestellt oder das Serviceziel erreicht wurde, ist dieses Feld leer.

Aktuelles Datum/Zeit

Gibt das Datum und die Uhrzeit des Zeitpunkts an, zu dem die Bedingung erfüllt wurde oder zu dem der Anwender auf "Festlegen des Ist-Aufwands" geklickt hat.

Restzeit

Zeigt den Zeitraum an, der zur Erreichung des Serviceziels noch verbleibt. Ein negativer Wert gibt den Betrag der Zeit an, um den der Zielzeitraum überschritten wurde.

Festlegen des Ist-Aufwands zulassen

Zeigt an, ob Sie den tatsächlichen Zeitraum angeben können. Ja bedeutet, dass Sie das tatsächliche Datum und die tatsächliche Uhrzeit eines Serviceziels im Feld "Aktuelles Datum/Zeit" angeben können. Nein bedeutet, dass Sie das tatsächliche Datum und die tatsächliche Uhrzeit nicht überschreiben können.

Zurücksetzen des Ist-Aufwands zulassen

Zeigt an, ob Sie den tatsächlichen Zeitraum neu starten können. Ja bedeutet, dass Sie das tatsächliche Datum und die tatsächliche Uhrzeit eines Serviceziels zurücksetzen können. Nein bedeutet, dass Sie das tatsächliche Datum und die tatsächliche Uhrzeit nicht zurücksetzen können.

Datum/Zeit der letzten Änderung

Zeigt das Datum an, zu dem dieses Ticket das letzte Mal geändert wurde.

Zuletzt geändert von

Zeigt den Namen der letzten Person an, die das Ticket bearbeitet hat.

Diensttyp

Zeigt den Namen des Servicetyps an, der an dieses Serviceziel angehängt ist.

Servicezielvorlage

Zeigt den Namen der Servicezielvorlage an, die mit dem zur Erstellung dieses Serviceziels verwendeten Servicetyp verbunden war.

Zieldatum/-zeit der Zurückstellungsneuberechnung sperren

Sperrt die Anzeige von Datum/Uhrzeit, damit sie nicht aktualisiert wird, wenn das Ticket zurückgestellt oder verzögert wird.

Datum/Zeit des letzten Starts

Zeigt den Zeitpunkt an, an dem der Serviceziel-Timer zum letzten Mal gestartet wurde.

Ticket-Status

Zeigt den Wert im Feld "Status" des Tickets an.

Status zurückstellen

Zeigt an, ob das Ticket durch den Ticket-Status zurückgestellt wurde.

Datum/Zeit der letzten Zurückstellung

Zeigt den Zeitpunkt an, an dem das Ticket zum letzten Mal zurückgestellt wurde.

Zählung zurückstellen

Gibt an, wie oft das Ticket zurückgestellt wurde.

Datum/Zeit der letzten Lösung

Zeigt den Zeitpunkt an, an dem das Ticket zum letzten Mal in den Status "Gelöst" übergestellt wurde.

Anzahl der Lösungen

Gibt an, wie oft das Ticket in den Status "Gelöst" übergestellt wurde.

Datum/Zeit der letzten Schließung

Zeigt den Zeitpunkt an, an dem das Ticket zum letzten Mal in den Status "Geschlossen" übergestellt wurde.

Abgeschlossene Zählung

Gibt an, wie oft das Ticket in den Status "Geschlossen" übergestellt wurde.

Datum/Zeit der letzten Ticket-Öffnung

Zeigt den Zeitpunkt an, an dem das Ticket geöffnet wurde.

Datum/Zeit der letzten Ticket-Lösung

Zeigt den Zeitpunkt an, an dem das Ticket gelöst wurde.

Datum/Zeit der letzten Ticket-Schließung

Zeigt den Zeitpunkt an, an dem das Ticket geschlossen wurde.

Anzeigen des Status des Serviceziels

In einem offenen Ticket können Sie den Status jedes Serviceziels anzeigen. Statusinformationen wie Restzeit oder Vertragsstrafe helfen Ihnen dabei, Ihre Arbeit zu priorisieren.

So zeigen Sie den Status eines Serviceziels an:

1. Zeigen Sie auf der Registerkarte "Service Desk" eine Liste von Incidents, Problemen, Requests, Changes oder Issues an.

Die betreffende Ticket-Liste wird geöffnet und zeigt folgende Informationen zum Serviceziel an:

Serviceziel

Zeigt den Zeitpunkt an, an dem das nächste Serviceziel fällig ist.

Projektierte Verletzung

Zeigt die bei Verletzung des Servicetyp-Zeitlimits verursachten Kosten an.

2. Wählen Sie das gewünschte Ticket in der Liste aus.

Die Seite "Ticket - Detail" wird angezeigt.

3. Wählen Sie die Registerkarte "Servicetyp" aus.

Hinweis: Serviceziele werden auf Tickets angezeigt, die die vom Administrator festgelegten Bedingungen erfüllen. Funktionen wie die automatische Prioritätsberechnung können für die Berechnung und Anzeige der Zielinformationen eine Rolle spielen.

Wenn das Ticket vordefinierten Zielbedingungen entspricht, enthält die Liste der Serviceziele folgende Informationen:

Aktion

Legt "Aktuelles Datum/Zeit" auf das Datum und die Uhrzeit des gegenwärtigen Zeitpunkts fest.

Ziel

Gibt das aktuelle Serviceziel des Tickets an.

Zieldatum/-uhrzeit

Gibt das Datum und die Uhrzeit der Fälligkeit dieses Serviceziels an. Wenn das Ticket den Status "Zurückgestellt" aufweist, ist dieser Wert leer.

Aktuelles Datum/Zeit

Gibt die Uhrzeit an, zu der die Zielbedingung erfüllt wurde. Wenn kein Wert angezeigt wird, wurde die Zielbedingung nicht erfüllt.

Restzeit

Gibt den Betrag der restlichen Zeit für das Serviceziel an, wenn das Ticket zurückgestellt ist. Wenn das Serviceziel erreicht wurde, wird unter "Restzeit" die nicht genutzte Zeit angezeigt. Ein negativer Wert gibt den Betrag der Zeit an, die seit dem verfehlten Zieldatum verstrichen ist.

Kosten der Verletzung

Zeigt den für das Verfehlen des Zieles anfallenden Abzug an. Diese Informationen werden auch auf dem Ticket angezeigt.

Serviceverträge

Das SLA-Modell enthält den Servicevertrag. Der Servicevertrag definiert den SLA für eine bestimmte Organisation, einschließlich der Servicetypen, der Anforderungsbereiche und der Issue- oder Change-Kategorien. Diese Definitionen werden als *private* Kategorien und *private* Servicetypen bezeichnet.

Hinweis: Die *privaten* Kategorien und Servicetypen können nur in Tickets verwendet werden, für die der Servicevertrag in Kraft ist.

Der auf ein Ticket anwendbare Servicevertrag wird durch die *betroffene Organisation* des Tickets bestimmt, die immer die Organisation des betroffenen Endanwenders im Ticket ist (das Feld "Organisation" in einem Kontaktdatensatz). Nur die im Servicevertrag aufgeführten Bereiche oder Kategorien können für das Ticket gewählt werden. Ferner sind die einzigen Servicetypen, die verwendet werden können, die im Vertrag aufgeführten *privaten* Servicetypen. Dadurch wird sichergestellt, dass die SLAs für eine Organisation nicht versehentlich mit den SLAs einer anderen Organisation vermischt werden.

Ein Dienstvertrag ordnet Diensttypen auch gemeinsamen Bezugsfeldern in einem Ticket zu, wie zum Beispiel Priorität und Anlage. Diese Zuordnung verbindet Servicetypen mit Attributen eines Tickets. Zum Beispiel kann der Vertrag einer Organisation jedem der fünf Prioritätsobjekte Servicetypen zuweisen. Wenn ein Ticket mit einer bestimmten Priorität erstellt wird, dann wird der zugeordnete Diensttyp angewandt.

Kategorien und Servicetypen können außerhalb eines Vertrags definiert werden und werden dann als *öffentlich* betrachtet. Diese öffentlichen Kategorien und Servicetypen werden verwendet, wenn für ein Ticket kein Servicevertrag in Kraft ist. Der Mangel an einem Servicevertrag kann auftreten, wenn der Endanwender keine Organisation hat, oder der Vertrag der Organisation inaktiv ist. Eine öffentliche Definition ist ein hilfreicher Sicherstellungs- oder Standardmechanismus. Öffentliche Diensttypen werden direkt für Kategorien und andere Bezugsfeldobjekte festgelegt.

Alle anwendbaren Servicetypen werden dem Ticket zugewiesen. Dadurch wird sichergestellt, dass alle Aspekte eines SLA dargestellt und durchgesetzt werden.

- Zum Beispiel kann ein Drucker einen Servicetyp haben, bei dem ein Techniker innerhalb von 2 Tagen entsandt werden muss.
- Der Servicetyp eines Prioritätsobjekts kann beispielsweise einen Rückruf innerhalb 1 Stunde erfordern.

Durch Anwendung beider Diensttypen werden diese erforderlichen Aktionen durchgesetzt.

Die Verfolgung mehrerer Diensttypen hilft auch bei der Festlegung der Priorität von Tickets. Zum Beispiel wird einem Ticket, das einen Tastaturausfall betrifft, ein Diensttyp mit einer niedrigen Priorität zugewiesen. Wenn der betroffene Endanwender dringend eine Tastatur benötigt, kann die Servicepriorität aber erhöht werden.

Hinweis: Das SLA-Modell wird standardmäßig erzwungen. In früheren Versionen von CA SDM wurde nur ein einzelner Diensttyp auf ein Ticket angewandt. Die Auswahl des Diensttyps umfasste die Suche nach dem Typ mit der höchsten *Einstufung* unter allen möglichen Diensttypen. Ein Modell, das das Bewertungsschema verwendet, kann nach wie vor durch Installieren der Option "classic_sla_processing" benutzt werden.

Migration von Serviceverträgen

Wenn CA SDM als Migration installiert wird, wird die Option "classic_sla_processing" standardmäßig aktiviert. Somit kann Ihre SLA-Verarbeitung wie zuvor fortgesetzt werden. Dadurch erhalten Sie Zeit, um passende Serviceverträge zu erstellen. Anschließend können Sie "classic_sla_processing" gegebenenfalls deaktivieren.

Bei der Erstellung von Serviceverträgen müssen Sie keine neuen Servicetypen, Anforderungsbereiche oder Kategorien erstellen. Mit der Schaltfläche „Kopieren“ in den Dienstvertragsdetails können Sie vorhandene Objekte in den Vertrag kopieren.

Wenn in der vorherigen Installation das Feld „support_lev“ für einen Tickettyp als erforderlich markiert war, muss diese Einschränkung aufgehoben werden. Wenn das Feld "support_lev" im aktuellen Modell weiterhin vorhanden, aber nicht festgelegt ist, hat dies bei neuen Tickets einen Fehler aufgrund erforderlicher Felder zur Folge. Dies betrifft die Objekte Anforderung (cr), Problemanfrage (iss) und Änderungsauftrag (chg).

Verletzungszeitpunkt

Wenn das neue SLA-Modell in Verwendung ist, kann das Verletzungszeitpunkt-System (TTV) von CA SDM Ihnen dabei helfen, Tickets zu verfolgen und ihre Priorität gemäß des erwarteten Verletzungszeitpunkts festzulegen. Dieses System überwacht alle aktiven Tickets und legt den erwarteten Verletzungszeitpunkt für jeden Diensttyp fest. Sie können nun Tickets auf der Basis ihres Verletzungszeitpunkts und der Kosten melden und sortieren. Dadurch können Sie die dringendsten und teuersten Issues zuerst lösen.

Das TTV-System überwacht alle aktiven Tickets und bewertet ihre SLA-Ereignisse im Hintergrund. Auf diese Weise bestimmt das System, welche Ereignisse die SLA-Verletzungsmarkierung setzen. Die Ereignisse werden nicht durchgeführt, aber das System betrachtet lediglich das Ergebnis eines jeden Ereignisses auf der Basis des aktuellen Status des Tickets. Wenn die Bewertung eine Aktion zur Folge hat, die die SLA-Verletzungsmarkierung setzt, wird der zugehörige Servicetyp des Tickets mit einem Verletzungszeitpunkt-Wert aktualisiert. Dieser Wert ist das Datum/die Uhrzeit, zu dem das Ereignis ausgelöst wird, das die SLA-Verletzung setzt.

Die Bewertung findet jedes Mal statt, wenn ein Ticket eingefügt oder aktualisiert wird. Da Tickets oft rasch hintereinander aktualisiert werden, wird die Bewertung für einen kurzen Zeitraum aufgeschoben. Das Verzögerungsintervall wird von der Option „ttv_evaluation_delay“ gesteuert. Nachdem die Verzögerung abläuft, bewertet das TTV-System alle SLA-Ereignisse, die die SLA-Verletzungsmarkierung setzen können.

Jedes Ereignis besitzt eine optionale Bedingung und eine Gruppe von Aktionen (Makros), die auf der Basis des Ergebnisses der Bedingung ausgelöst werden. Um eine angemessene Leistung sicherzustellen, werden Ereignisvorlageinformationen vom TTV-System im Cache gespeichert und regelmäßig aktualisiert. Prognosen des TTV-Systems zu kürzlich aktualisierten Ereignisvorlagen können einige Minuten lang ungenau sein.

Hinweis: Verletzungszeitpunkt-Prognosen werden auf der Registerkarte "Servicetyp" eines jeden Tickets angezeigt. Das TTV-System wird mit der Option „ttv_enabled“ aktiviert.

Zeitzone und Schichten

Um den komplexen Geschäftsanforderungen automatisierter Anwendungen gerecht zu werden, können Sie in CA SDM so viele Zeitzone und Schichten wie nötig definieren und sie aufzeichnen, um einfach auf sie zu verweisen.

- Zeitzone geben die Zeitzone an, in der sich der Anwender, das CI usw. befinden.
- Schichten definieren den Zeitraum, in dem die Event-Überwachung aktiv ist, oder die Arbeitszeit eines Servicetyps oder SLA.

Für die korrekte Handhabung von Events kann es äußerst wichtig sein, einen Aktionsverlauf auf der Basis des Zeitpunkts zu bestimmen, zu dem ein Event auftritt. Die von Ihnen definierten Zeitzone und Schichten stehen allen Funktionen von CA SDM zur Verfügung.

Weitere Informationen:

[Einrichten von Schichten](#) (siehe Seite 296)

[Zeitzone](#) (siehe Seite 475)

Einrichten von Zeitzonen

Zeitzonencodes definieren die Zeitzone, von der ein Benutzer normalerweise auf das System zugreift (d. h. die Ortszeitzone des Benutzers), oder die Zeitzone, in der sich ein CI befindet. Geschäftszeiten werden immer in der Zeitzone des CA SDM-Servers eingegeben. Das bedeutet, dass Geschäftszeiten immer einheitlich verglichen werden können.

Zeitzone dienen dazu, Dienstypen, Eskalationen und die Gesamtantwort für betroffene Endbenutzer auf der Basis der Fähigkeit von CA SDM zu verwalten, die korrekte Zeit über mehrere Zeitzone darzustellen. CA SDM passt die Verschiebung zwischen der Zeitzone, in der sich ein Benutzer anmeldet oder sich ein CI befindet, und der Zeitzone, in der der Server läuft, automatisch an. Zeitzone verwenden das Greenwich-Zeitformat (GMT).

Hinweis: Weitere Informationen zum Definieren von Zeitzone finden Sie in der *Online-Hilfe*.

Verwalten mehrerer Zeitzonen für Servicetypen

CA SDM-Server und -Benutzer können sich in verschiedenen Zeitzonen befinden. Der Zeitunterschied kann dazu führen, dass Benutzer Servicetyp-Ablaufzeiten versäumen.

Um den Zeitunterschied zu korrigieren, können Sie CA SDM konfigurieren, um Servicetypablaufzeiten in der Endbenutzerzeitzone zu zeigen. Wenn zwei Benutzer in verschiedenen Zeitzonen dasselbe Ticket ansehen, sieht jeder Benutzer Ablaufzeitwerte auf der Basis der lokalen Computerzeitzone. Die Startzeitwerte spiegeln allerdings immer die Zeitzone des Servers wider.

So konfigurieren Sie die Endbenutzerzeitzone:

1. Erstellen Sie einen Servercode, der den Servernamen und die Zeitzone identifiziert.
2. Erstellen oder aktualisieren Sie einen Servicetyp. Setzen Sie das Feld "Zeitzone des Endbenutzers verwenden" auf "Ja".

Wenn dieser Wert auf "Ja" eingestellt wird, wird die Ablaufzeit entsprechend der jeweiligen Zeitzone des Benutzers angezeigt und aktualisiert.

Beispiel: Anzeigen der Servicetypablaufdaten in einer beliebigen Zeitzone des Benutzers

In diesem Beispiel konfigurieren Sie CA SDM, um Servicetypablaufdaten in irgendeiner Zeitzone des Benutzers zu zeigen. Server und Benutzer verwenden verschiedene Computer und befinden sich in verschiedenen Zeitzonen.

So erstellen Sie einen Servercode, der den Servernamen und die Zeitzone identifiziert

1. Wählen Sie auf der Registerkarte "Administration" des Hostservers die Option "Service Desk, Anwendungscode" aus.
2. Klicken Sie auf "Codes", "Server".

Die Serverliste wird angezeigt.

3. Klicken Sie auf den Server "Lokaler Host".

Die Seite "Servername – Detail" wird angezeigt.

4. Stellen Sie die Zeitzone ein. Setzen Sie zum Beispiel die Zeitzone auf "GMT (EU)". Der lokale Hostname muss mit dem in "NX.env" für den Server gespeicherten NX_LOCAL_HOST-Wert übereinstimmen.

5. Klicken Sie auf "Speichern".

Der Hostserver verwendet die neue Zeitzone. Wenn der Benutzer ein Ticket anzeigt, spiegelt die Startzeit die Zeitzone des Servers wider.

So erstellen Sie einen Servicetyp

1. Wählen Sie auf der Registerkarte "Administration" die Option "Servicetypen" aus.

Die Liste der Servicetypen wird angezeigt.

2. Klicken Sie auf "Lösung der Priorität 1" oder einen anderen Servicetyp, der Anfragen mit Priorität 1 verwaltet.

Die Seite "Servicetyp aktualisieren" wird angezeigt.

3. Aktivieren Sie das Kontrollkästchen "Zeitzone des Endbenutzers verwenden".
4. Klicken Sie auf "Speichern".

Der Servicetypdatensatz wird aktualisiert.

So zeigen Sie die Zeitzonen auf dem Ticket an

1. Öffnen Sie auf einem anderen Computer ein Anfrage-Ticket, und setzen Sie die Priorität auf "1".

Hinweis: Wenn Sie Serviceziele verwenden, stellen Sie auf dem Ticket die Werte so ein, dass beim Ziel die Lösung der Priorität 1 verwendet wird.

2. Zeigen Sie das Ticket an, und klicken Sie auf die Registerkarte "Servicetyp".

Die Startzeit spiegelt die Zeitzone des Servers wider. Die Ablaufzeit spiegelt die Zeit auf dem lokalen Endbenutzer-Computer wider.

3. Schließen Sie die Seite, die das Anfrage-Ticket zeigt.
4. Ändern Sie die Zeitzone auf dem lokalen Endbenutzer-Computer.
5. Betrachten Sie den Ticketservicetyp auf dem lokalen Endbenutzer-Computer, um die entsprechenden Ablaufzeitwerte basierend auf der Zeitzone des Benutzers zu sehen.

Die Ablaufzeit spiegelt die neue Zeitzone wider.

Hinweis: Ausführliche Informationen zu Servertypen und Servercodes finden Sie in der *Online-Hilfe*.

Einrichten von Schichten

Schichten geben den Tag, das Datum und die Uhrzeit an, zu denen ein Ereignis oder ein Ablaufplan gültig ist. Sie können Tage oder Termine bzw. Tage und Termine angeben. Die Angabe einer Zeit ist optional.

Hinweis: Weitere Informationen zum Definieren von Schichten finden Sie in der *Online-Hilfe*.

Wenn Sie Ereignisse für Tickets überwachen, definieren Schichten, wann das Ereignis überwacht wird bzw., in anderen Worten, wann die Uhr läuft. Wenn zum Beispiel beim vordefinierten Ereignis "P1 aktiv - Zustand. benachr." ein Issue der Priorität 1 um 16:45 Uhr geöffnet wird und die Schicht für Arbeitsschichten 9:00 Uhr bis 17:00 lautet, sendet das überwachte Ereignis dem für Issues Zuständigen automatisch eine Benachrichtigung um 9:45 Uhr am nächsten Tag.

Hinweis: Zeitpläne werden auch zur automatischen Zuweisung von Tickets zu Kontakten verwendet.

Weitere Informationen:

[Einrichten einer Support-Struktur](#) (siehe Seite 403)

Sicherheit

Bevor andere Personen mit CA SDM arbeiten, müssen Sie die Sicherheit einstellen, um festzulegen,

- welche Anwender auf das System zugreifen dürfen,
- welche Zugriffsebenen für die Anwender freigegeben sind,
- wie Anwender authentifiziert werden, wenn sie sich anmelden.

Hinweis: Details zur Erfüllung der Sicherheitsadministrationsaufgaben finden Sie in der *Online-Hilfe*.

Konfigurationen für CA EEM- und CA Workflow-Benutzerdatenbanken

CA EEM ist ein zentrales Repository für Benutzerdaten (Identitäten). CA EEM definiert die Authentifizierung der Benutzer und ihren Zugriff auf weitere Anwendungen. Wenn Sie mehrere CA Technologies-Produkte installiert haben, verwenden einige dieser unter Umständen CA EEM zum Speichern von Identitäten und Zugriffsrichtlinien. CA SDM benutzt nur CA EEM zur Authentifizierung. CA EEM ist keine CA SDM-Konfigurationsoption und muss separat installiert werden.

Als Repository für Benutzerdatensätze verwendet CA EEM *eine* der folgenden beiden Quellen:

- ein externes LDAP-Verzeichnis
- die eigenen internen Tabellen in der MDB

CA EEM verfügt über eine LDAP-Schnittstelle, die genutzt wird, wenn CA EEM für die Verwendung der MDB konfiguriert wird.

Hinweis: Die von CA EEM benutzten MDB-Tabellen sind anders als die von CA SDM verwendeten Tabellen.

Wenn Ihr Unternehmen einen Verzeichnisserver verwendet, z. B. Active Directory oder eTrust Directory, sollten Sie CA EEM so konfigurieren, dass dieses Verzeichnis für Benutzer verwendet wird. Dadurch kann jede beliebige Anwendung, die CA EEM verwendet, auf die Benutzer in Ihrem Verzeichnis zugreifen. Da CA EEM die Zugangsverwaltung zentralisiert, wird es normalerweise auf einem einzelnen Server installiert.

Hinweis: Weitere Informationen zur Installation finden Sie im *Implementierungshandbuch*.

CA Workflow

Während CA SDM-Installation können Sie optional CA Workflow, eine eingebettete Workflow-Engine installieren. Da CA Workflow für alle Benutzerinformationen CA EEM verwendet, verwaltet CA EEM alle Authentifizierungsversuche und bestimmte Berechtigungen. CA Workflow erkennt die CA SDM-Kontaktdatensätze nicht.

Hinweis: Informationen zum Konfigurieren des Zugriffs für CA Workflow finden Sie im *Implementierungshandbuch*.

CA SDM

CA SDM speichert Kontaktinformationen in MDB-Tabellen. Diese Tabellen haben keine Beziehung zu CA EEM. CA SDM verwendet CA EEM nicht für die Zugangs- oder Identitätsverwaltung. CA SDM verwaltet den eigenen Zugriff und die eigene Sicherheit mit Hilfe von Zugriffstypen und Datenaufteilungen.

CA SDM benutzt CA EEM nur zur Authentifizierung. Wenn Sie mit CA EEM Anwender in CA SDM authentifizieren möchten, installieren Sie CA EEM. Wenn Sie CA SDM in CA EEM integrieren, ersetzt es die CA SDM-Betriebssystemauthentifizierung durch die CA EEM-Authentifizierung.

Hinweis: Informationen zum Installieren von CA EEM finden Sie im *Implementierungshandbuch*. Um CA EEM und CA SDM zu integrieren, müssen Sie die Optionen *eam_hostname*, *use_eiam_artifact* und *use_eiam_authentication* in "Optionsmanager > Sicherheit" festlegen. Weitere Informationen zu diesen Optionen finden Sie in der *Online-Hilfe*.

Die CA SDM-Anwenderdatenbank ist von der Datenbank von CA EEM und daher auch von der CA Workflow-Anwenderdatenbank getrennt. Der Vorteil für CA Workflow besteht darin, dass Workflow-Elemente Personen außerhalb von CA SDM zugewiesen und von diesen durchgeführt werden können. Dies ist nützlich, wenn CA EEM auf den LDAP-Server Ihrer Organisation verweist.

Die Herausforderung liegt in der CA SDM-Integration. Ein Arbeitsschritt kann dem eigentlichen CA SDM-Kontaktdatensatz nicht direkt zugewiesen werden. Die Arbeitsschritt-Zuweisung zu CA SDM-Kontakten kann nur durchgeführt werden, wenn beide der folgenden Bedingungen erfüllt werden:

- Der CA SDM-Kontakt hat einen entsprechenden Datensatz in CA EEM.
- Diese Datensätze haben übereinstimmende Anwender-IDs.

Zusammenfassung:

- CA SDM verwendet die MDB, um Kontaktinformationen zu speichern. CA SDM bietet auch LDAP-Integration, die es CA SDM erlaubt, neue Kontakte von einem LDAP-Server zu erstellen und vorhandene Kontakte mit dem Verzeichnis zu synchronisieren.
- CA EEM ist die Lösung von CA zur zentralisierten Anwenderverwaltung. Wenn Sie mehrere CA-Produkte installiert haben, verwenden eventuell alle von ihnen CA EEM, um Identitäten und Zugriffsrichtlinien zu speichern.
- CA EEM kann so konfiguriert werden, dass das Programm entweder auf ein externes (LDAP-) Verzeichnis verweist oder Anwenderdatensätze in der MDB speichert. CA EEM selbst verfügt über eine LDAP-Schnittstelle, die genutzt wird, wenn CA EEM für die Verwendung der MDB konfiguriert wird.
Hinweis: Die von CA EEM verwendeten Tabellen in der MDB unterscheiden sich von denen, die von CA SDM verwendet wurden.
- CA Workflow verwendet immer CA EEM für seine Anwenderinformationen und die Authentifizierung. Arbeitsschritte können nur Anwendern zugewiesen werden, die CA EEM bekannt sind. Außerdem können nur von CA EEM definierte Anwender auf die integrierte Entwicklungsumgebung (IDE, Integrated Development Environment) von CA Workflow und die Worklist-Web-Benutzerschnittstelle zugreifen.

Die folgenden Informationen behandeln die unterschiedlichen Konfigurationsoptionen für die Produkte und erläutern, wie diese die Integration von CA SDM und CA Workflow beeinflussen. Wählen Sie die Konfiguration aus, die Ihrer Verwendung von CA Workflow und (optional) einem LDAP-Verzeichnisserver am besten entspricht.

Weitere Informationen:

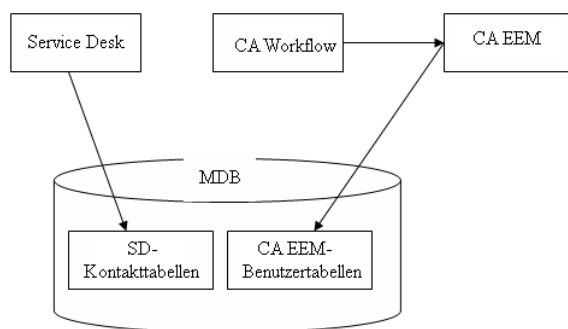
[Konfigurationen für CA EEM- und CA Workflow-Benutzerdatenbanken](#) (siehe Seite 297)
[CA EEM als LDAP-Konfiguration](#) (siehe Seite 301)

Standardkonfiguration

CA SDM und CA Workflow speichern Benutzerdaten nach einer Standardinstallation wie folgt:

- CA SDM speichert Benutzerdaten in den CA SDM-Kontakttabellen in der MDB.
- CA Workflow benutzt CA EEM, um Benutzerdaten in den CA-EEM-Benutzertabellen in der MDB zu speichern.

Das folgende Diagramm veranschaulicht, wo die Produkte Benutzerdaten speichern:

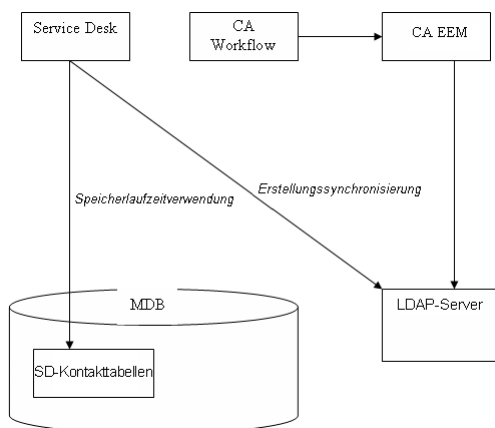


Ziehen Sie die Verwendung der Standardkonfiguration in Betracht, wenn Ihr Standort CA Workflow oder eine LDAP-Verzeichnisserver nur wenig oder überhaupt nicht verwendet. Diese Konfiguration kann einige Herausforderungen bedeuten. Jeder CA Workflow-Benutzer benötigt einen CA EEM-Benutzerdatensatz.

Externe LDAP Server-Konfiguration

Die Verwaltung von Kontakten wird vereinfacht, wenn CA SDM und CA Workflow den gleichen LDAP-Verzeichnisserver benutzen. Dies ist besonders nützlich, wenn Ihr Standort bereits einen LDAP-Server als Hauptverzeichnis für Benutzer verwendet. Aufgrund der LDAP-Fähigkeit von CA SDM entsprechen die Benutzer-IDs von Kontakteinträgen den IDs im Verzeichnis entsprechen, was eine problemlose Zuweisung von Arbeitselementen zu CA SDM-Analysten ermöglicht. Eine noch nahtlosere Integration erzielen Sie, wenn CA SDM CA EEM für die Authentifizierung nutzt.

Das folgende Diagramm zeigt ein Szenario, in dem alle Benutzern im LDAP-Verzeichnis automatisch Zugriff auf die CA Workflow-Worklist-Webanwendung haben. CA SDM verwendet weiterhin die Kontakttabellen in der MDB für seine Benutzerdatensätze. Diese Datensätze können aber vom LDAP-Server importiert und regelmäßig mit diesen synchronisiert werden.

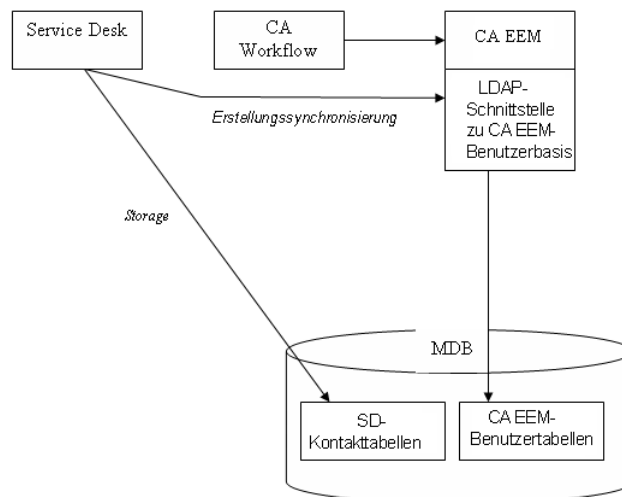


Weitere Informationen:

[LDAP-Verzeichnis-Daten](#) (siehe Seite 344)

CA EEM als LDAP-Konfiguration

Wenn CA EEM so konfiguriert wird, dass MDB anstatt ein externes Verzeichnis zum Speichern von Benutzerinformationen verwendet wird, legt CA EEM das Benutzerverzeichnis mit Hilfe einer LDAP-Schnittstelle offen. Wenn Ihr Standort keinen externen LDAP-Server verwendet, können Sie dennoch die Vorteile einer externen LDAP-Konfiguration nutzen, indem Sie CA SDM so konfigurieren, dass es CA EEM als LDAP-Quelle verwendet. Diese Konfiguration kann nützlich sein, wenn Ihr Standort keinen LDAP-Server verwendet, Sie aber die Benutzerverwaltung in CA EEM konzentrieren möchten. Andere CA-Produkte benutzen auch CA EEM, wodurch die Benutzerverwaltung sehr vereinfacht werden kann.



Hinweis: Diese Konfiguration ist wiederum nur anwendbar, wenn CA EEM für die Verwendung der MDB konfiguriert ist. Wenn CA EEM für einen externen LDAP-Server konfiguriert ist, konfigurieren Sie CA SDM so, dass es auf denselben LDAP-Server und *nicht* auf CA EEM verweist.

Aktualisieren

Wenn Sie die Migration einer früheren Version von CA SDM durchführen oder viele Kontakteinträge im Batchprozess laden, müssen Sie diese Benutzer manuell zu CA EEM hinzufügen, damit sie Zugriff auf CA Workflow erhalten.

Konfigurieren des CA EEM r8.4 SP4 CR05-Anwenderspeichers

Sie können CA EEM r8.4 SP4 CR05 so konfigurieren, dass Anwenderdatensätze in einem externen LDAP-Verzeichnis oder in den eigenen internen MDB-Tabellen gespeichert werden. Wenn CA EEM ein externes LDAP-Verzeichnis verwendet, handelt es sich um eine schreibgeschützte Schnittstelle, d. h., Sie können Anwender nicht über die CA EEM-Schnittstelle hinzufügen oder ändern.

Gehen Sie wie folgt vor:

1. Klicken Sie auf "Start" > "Programme" > "CA" > "Embedded Entitlements Manager" > "EEM UI".

Die CA EEM-Benutzeroberfläche wird angezeigt.

2. Klicken Sie auf die Registerkarte "Konfigurieren".
3. Klicken Sie auf die untergeordnete Registerkarte "EEM Server".
4. Wählen Sie im linken Fenster die Verknüpfung für globale Anwender und Gruppen.
5. Wählen Sie im rechten Fensterbereich eine der folgenden Optionen:
 - In internem Datenspeicher speichern
 - Referenz von einem externen Verzeichnis
 - Verweis von CA SiteMinder

Hinweis: Wenn Sie die Option der Referenz von einem externen Verzeichnis auswählen, werden Sie aufgefordert, die LDAP-Server-Details anzugeben.

6. Klicken Sie auf "Speichern".

Die Konfiguration des Benutzerspeichers in CA EEM ist abgeschlossen.

Hinweis: Weitere Informationen über CA EEM finden Sie in der CA EEM-Online-Hilfe.

Konfigurieren des CA EEM r12 CR02-Benutzerspeichers

Sie können CA EEM r12 CR02 so konfigurieren, dass Anwenderdatensätze in einem externen LDAP-Verzeichnis oder in den eigenen internen MDB-Tabellen gespeichert werden. Wenn CA EEM ein externes LDAP-Verzeichnis verwendet, handelt es sich um eine schreibgeschützte Schnittstelle, d. h., Sie können Anwender nicht über die CA EEM-Schnittstelle hinzufügen oder ändern.

Gehen Sie wie folgt vor:

1. Klicken Sie auf "Start" > "Programme" > "CA" > "Embedded Entitlements Manager" > "Admin UI".

Die CA EEM-Benutzeroberfläche wird angezeigt.

2. Klicken Sie auf die Registerkarte "Konfigurieren".
3. Klicken Sie auf die untergeordnete Registerkarte "Benutzerspeicher".
4. Klicken Sie auf dem linken Bereich auf die Verknüpfung "Benutzerspeicher".
5. Wählen Sie im rechten Fensterbereich eine der folgenden Optionen:

- In internem Datenspeicher speichern
- Referenz von einem externen Verzeichnis
- Verweis von CA SiteMinder

Hinweis: Wenn Sie die Option der Referenz von einem externen Verzeichnis auswählen, werden Sie aufgefordert, die LDAP-Server-Details anzugeben.

6. Klicken Sie auf "Speichern".

Die Konfiguration des Benutzerspeichers in CA EEM ist abgeschlossen.

Hinweis: Weitere Informationen über CA EEM finden Sie in der CA EEM-Online-Hilfe.

Hinzufügen von Anwendern und Gruppen

Wenn CA EEM so konfiguriert ist, dass es auf ein externes Verzeichnis verweist, können Sie über die CA EEM-Benutzerschnittstelle keine Anwender hinzufügen. Für den LDAP-Server ist CA EEM eine schreibgeschützte Schnittstelle. Zur Aktualisierung der Anwenderdatensätze müssen Sie die Schnittstelle verwenden, die von Ihrem LDAP-Serverprodukt bereitgestellt wird.

So fügen Sie einen neuen Anwenderdatensatz hinzu:

1. Klicken Sie auf "Start" > "Programme" > "CA" > "Embedded Entitlements Manager" > "Admin UI/EEM UI".
2. Melden Sie sich mit dem CA EEM-Administratoranwenderamen und -kennwort an. Diese werden während der CA EEM-Installation angegeben. CA EEM muss getrennt installiert werden und ist keine Konfigurationsoption für CA SDM.
3. Klicken Sie auf die Registerkarte "Identitäten verwalten".

4. Klicken Sie im linken Fensterbereich auf die Registerkarte "Anwender", um existierende Anwenderdatensätze zu suchen und zu aktualisieren.

Hinweis: Um CA EEM-Gruppen zu verwalten, wählen Sie die Registerkarte "Gruppen".

5. Klicken Sie auf das Symbol links neben dem Ordner "Anwender".
Das Formular zum Erstellen eines Anwenderdatensatzes wird angezeigt.
6. Füllen Sie die Felder aus, und klicken Sie auf "Speichern".
Der neue CA EEM-Anwenderdatensatz wird in der MDB abgespeichert.

Hinweis: Die Schritte, um einen existierenden Anwenderdatensatz zu bearbeiten und Gruppendatensätze zu verwalten, sind diesen Schritten ähnlich. Weitere Informationen finden Sie in der *Online-Hilfe von CA EEM*.

CA Workflow-Zugriff in CA EEM konfigurieren

Alle Anmeldungen bei CA Workflow werden von CA EEM authentifiziert. Damit ein Benutzer auf die IDE von CA Workflow oder die Worklist-Anwendung zugreifen kann, muss für den Benutzer ein Datensatz in CA EEM vorhanden sein. Der CA Workflow-Administrator, der während der Konfiguration von CA SDM angegeben wird, hat vollen Zugriff.

Standardmäßig wird dieser Benutzer von CA SDM für die Workflow-Integration verwendet. Dieses Benutzerkonto wird durch die Optionen „cawf_username“ und „cawf_password“ im Optionsmanager festgelegt. Sie müssen sich vergewissern, dass der in diesen Optionen festgelegte Benutzername und das Kennwort korrekt sind und der Benutzer innerhalb von CA EEM vollen Zugriff auf die CA Workflow-Ressourcen hat.

CA Workflow verwendet CA EEM auch, um den Zugriff auf bestimmte CA Workflow-Funktionen einzuschränken. Dieser Zugriff wird von zwei Ressourcenklassen, IDE und Process, gesteuert:

- Die IDE-Ressource besitzt eine einzelne Aktion mit der Bezeichnung *login*, die die Berechtigung zur Anmeldung in die IDE erteilt. Ein Benutzer muss die Berechtigung für diese Aktion besitzen, um sich in der IDE-Anwendung von CA Workflow anmelden zu können.
- Die Process-Ressource besitzt eine einzelne Aktion mit der Bezeichnung *start*, die die Berechtigung zum Starten einer Prozessinstanz erteilt. Ein Benutzer muss die Berechtigung für diese Aktion besitzen, um Prozesse innerhalb der Worklist-Web-Anwendung starten zu können.

Hinweis: Alle Benutzer, die CA EEM bekannt sind, haben Zugriff auf die CA Workflow-Worklist-Anwendung, um Arbeitsschrittaufgaben anzuzeigen und auszuführen. Diese Berechtigung dient nur zum Starten neuer Instanzen aus der Worklist heraus. Diese Ressourcenklassen werden in Verbindung mit der CA SDM-Anwendungsinstanz in CA EEM definiert. Wenn Sie sich in der CA EEM-Web-Benutzerschnittstelle anmelden, müssen Sie die CA SDM-Anwendungsinstanz angeben, um die hier beschriebenen Ressourcen, Richtlinien und Gruppen zu sehen.

Benutzer, die sich in der IDE anmelden oder Prozessinstanzen starten müssen, benötigen eine Autorisierung für die oben genannten Ressourcen und Aktionen. Die CA SDM-Konfiguration fügt CA EEM zwei Richtlinien hinzu, die Zugriff auf diese Ressourcen gewähren. Aus Zweckmäßigkeitsgründen gewähren die Richtlinien Zugriff auf zwei Gruppen in der zugehörigen Anwendungsinstanz: Workflow-Administratoren und Initiatoren für Workflow-Prozesse. Damit Benutzer Zugriff auf die IDE erhalten, können Sie die Benutzer einfach zur Gruppe der Workflow-Administratoren hinzufügen. Wenn Sie Benutzer zur Gruppe der Initiatoren für Workflow-Prozesse hinzufügen, sind diese Benutzer berechtigt, Prozesse innerhalb der Worklist-Anwendung zu starten.

So fügen Sie Benutzer zu den oben genannten Gruppen hinzu oder löschen sie daraus:

1. Melden Sie sich bei der CA EEMWeb-Oberfläche an.
2. Wählen Sie auf der Anmeldeseite die CA SDM-Anwendung aus, und geben Sie den CA EEM-Administratornamen und das Kennwort ein.
3. Wählen Sie auf der Hauptseite von CA EEM "Identitäten verwalten".
4. Wählen Sie die Benutzersuche. Geben Sie die Suchkriterien ein, und starten Sie die Suche.

5. Wählen Sie einen Benutzer aus der Ergebnisliste aus.
6. In der Benutzerdetailanzeige fügen Sie im Abschnitt „Application Group Membership“ die Gruppenmitgliedschaft hinzu oder entfernen sie.
Hinweis: Wenn dieser Abschnitt nicht angezeigt wird, müssen Sie gegebenenfalls auf die Schaltfläche "Benutzerdetails hinzufügen" klicken.
7. Klicken Sie nach Abschluss Ihrer Eingaben auf „Save“.
Der Benutzer wird entsprechend hinzugefügt oder entfernt.

Zuweisen von CA Workflow-Arbeitsschritten

Die Rolle eines CA Workflow-Arbeitsschritts kann menschlichen und nicht menschlichen Akteuren zugewiesen werden. Beispiele für nicht menschliche Akteure sind ein benutzerdefiniertes Java-Objekt, ein Befehlszeilenprozess oder eine andere CA Workflow-Prozessinstanz. Für menschliche Akteure wird die Arbeitsschrittrolle für die Liste der globalen Benutzer festgelegt, das Benutzer-Repository von CA EEM. Hierbei muss es sich um eine durch Semikola getrennte Liste von Benutzer-IDs handeln.
Beispiel:

ServiceDesk; abeju01; My Group

ordnet den Arbeitsschritt den Benutzern "ServiceDesk", "abeju01" und jedem Mitglied von "My Group" zu. Das bedeutet, dass jeder dieser Benutzer den Arbeitsschritt durchführen kann.

Hinweis: Alle diese Benutzer und Gruppen müssen CA EEM bekannt sein. Somit ist die Gruppe "My Group" eine Gruppe in CA EEM und keine Gruppe in CA SDM.

Um ein Arbeitselement einem einzelnen Benutzer dynamisch zuzuweisen, legen Sie für die Benutzerliste der Rolle „\$MyUser“ fest.

Hinweis: Setzen Sie die Zeichenfolge NICHT zwischen Anführungszeichen.

Erklären Sie in der Prozessdefinition ein Zeichenfolgenattribut mit der Bezeichnung MyUser. Bei der Erstellung des Arbeitselements wird für die Zuweisung des Arbeitselements der in MyUser enthaltene Wert verwendet. Das heißt, dass Sie MyUser einen gültigen Wert zuweisen müssen, entweder einen einzelnen Benutzernamen oder eine Liste von Benutzernamen, durch Semikola voneinander getrennt. Diese Zuweisung muss vor der Verwendung in einem Arbeitselement erfolgen.

Ein Beispiel für die Zuweisung von Benutzer-IDs zu Variablen finden Sie in der Demonstration einer PC-Definition. Es wird angenommen, dass die Benutzer-ID eines Kontaktdatensatzes von CA SDM mit der Benutzer-ID eines entsprechenden Benutzerdatensatzes in CA EEM übereinstimmt. Die Demonstration einer PC-Definition zeigt, wie Benutzer-IDs von CA SDM über die Webservices-Schnittstelle abgerufen werden. Die Benutzer-IDs können vom Ticket stammen (zum Beispiel Zuständiger, für Kategorie Zuständiger usw.).

So fassen Sie die Festlegung der Zuweisung eines Arbeitsschritts zusammen:

1. Starten Sie den CA Workflow-IDE-Client.
2. Doppelklicken Sie auf den Namen der Prozessdefinition, die Sie bearbeiten möchten.

Die Prozessdefinition wird im Fenster "Prozess-Designer" angezeigt.
3. Wählen Sie die Registerkarte „Rolle“.
4. Fügen Sie eine Rolle hinzu oder aktualisieren Sie diese.
5. Wählen Sie "Globale Benutzerliste" aus der Liste der verfügbaren Akteure aus und klicken Sie auf "Bearbeiten".
6. Geben Sie eine Liste mit CA EEM-Benutzer-IDs ein, die durch Semikola voneinander getrennt werden. Mit der Schaltfläche "Durchsuchen" können Sie auch nach Benutzern suchen und die in CA EEM bekannten Benutzer auswählen.

Sicherheitsempfehlungen

Wenn Sie CA SDM zum ersten Mal installieren, ist das System so eingerichtet, dass jeder Kontakt, für den kein expliziter Zugriffstyp in seinem Kontaktdatensatz definiert wurde, maximalen Zugriff erhält. Möglicherweise möchten Sie zusätzliche Änderungen an der vordefinierten Sicherheitsimplementierung vornehmen. Mindestens sollten Sie aber die folgenden Schritte ausführen, bevor Sie Personen erlauben, mit der Arbeit in der Anwendung zu beginnen:

1. Prüfen Sie die vordefinierten Zugriffstypen, um einen angemessenen Standardwert für Ihr System zu bestimmen.

"Administrator" ist als der Standard-Zugriffstyp festgelegt, welches für die meisten Standorte keine optimale Wahl darstellt. Einige Sites gewähren den meisten Mitgliedern der IT-Organisation beispielsweise nur schreibgeschützten Zugriff. Wenn Sie als Standard-Zugriffstyp "CMDDB-Benutzer" einstellen, müssen Sie den Zugriffstyp von neuen Benutzern nicht ändern, wenn sie keine zusätzlichen Berechtigungen benötigen. Dementsprechend können Sie auch "CMDDB-Analyst" als Standard-Zugriffstyp auswählen, wenn die meisten Benutzer die Berechtigung zum Schreiben von Konfigurationsinformationen benötigen.
2. Ordnen Sie den verbleibenden Kontakten die Zugriffstypen explizit zu.

Wenn Sie zum Beispiel "CMDDB-Benutzer" als Standard-Zugriffstyp auswählen, ändern Sie die Kontaktdatensätze für Ihre Analystenkontakte, um ihnen einen Analysten-Zugriffstyp zuzuweisen.

Hinweis: Weitere Informationen hierzu finden Sie in der *Onlinehilfe*.

CA EEM-Authentifizierung für CA Process Automation

CA SDM und CA Process Automation kommunizieren unter Verwendung eines Webservices-Austauschs über HTTP miteinander. Obwohl bei jedem Vorgang darauf geachtet wird, dass nur geringe Mengen an sensiblen Informationen zwischen den Produkten ausgetauscht werden, kann eine böswillig gesinnte Organisation Zugriff auf Benutzernamen, Kennwörter und geistiges Eigentum erlangen. Sie können Schritte unternehmen, um die Serverkommunikation zu sichern.

Beachten Sie für die CA Process Automation-Authentifizierung die folgenden Empfehlungen:

- Eine Option für Sie ist, CA Process Automation so zu konfigurieren, dass CA EEM als Authentifizierungsserver verwendet wird. CA Process Automation implementiert Standardgruppen und -richtlinien in CA EEM. Sie können die Standardgruppen und -richtlinien bearbeiten, um sie an die Anforderungen Ihrer Organisation anzupassen.
- Durch das Verwenden von CA EEM ist es nicht erforderlich, Nur-Text-Benutzernamen und -Kennwörter zur Authentifizierung einzugeben. Wenn Sie Mandantenfähigkeit benutzen, ist CA EEM für die Aktivierung von Mandantenfähigkeit innerhalb CA Process Automation erforderlich.

Hinweis: Um Authentifizierungssicherheit in dieser Integration zu erreichen, ist es nicht notwendig, CA SDM für die Verwendung von CA EEM zu konfigurieren. Allerdings ist CA EEM für das Implementieren von Mandantenfähigkeit in CA Process Automation erforderlich. Weitere Informationen zum Implementieren von Mandantenfähigkeit mit CA Process Automation finden Sie in der CA Process Automation-Benutzerdokumentation. Weitere Informationen darüber, wie Sie CA Process Automation für die Verwendung von CA EEM als Authentifizierungsserver konfigurieren können, finden Sie in der CA Process Automation-Installations- und Konfigurationsdokumentation.

- Konfigurieren Sie CA Process Automation für die sichere Kommunikation über HTTPS. HTTPS-URLs verwenden SSL/TLS, um Nur-Text-Kommunikation zu unterbinden und so geistiges Eigentum und sonstige sensible Daten vor einer zufälligen oder böswilligen Offenlegung zu schützen.

Hinweis: Informationen zur Konfiguration von CA Process Automation für HTTPS finden Sie in der CA Process Automation-Installations- und Konfigurationsdokumentation.

Benutzerauthentifizierung

CA SDM bietet eine Lösung für die Benutzerauthentifizierung, die Sie als Teil des Zugriffstyps anpassen können. Die gleiche Authentifizierung wird von allen CA SDM-Schnittstellen und von anderen CA-Produkten verwendet.

Hinweis: Sie können die Benutzerauthentifizierung von CA SDM auf einem separaten Computer einrichten, wenn dies Ihren Bedürfnissen entspricht. Weitere Informationen finden Sie im *Implementierungshandbuch*.

Die Authentifizierung ist flexibel, so dass Sie externe Authentifizierungsmechanismen nutzen können, wie zum Beispiel Windows, HTTPD-Benutzervalidierung oder LDAP-Authentifizierung. Sie können auch zwischen verschiedenen internen Authentifizierungsoptionen wählen, einschließlich Betriebssystemkennwort, PIN, Gastnutzer-Zugriff oder Zugriffsverweigerung.

Authentifizierung von Benutzern durch CA SDM

CA SDM authentifiziert Benutzer auf Basis der Benutzer-ID die in ihrem Kontaktdatensatz definiert ist. Die Anwendung reagiert wie folgt, wenn ein Benutzer Zugriff auf das System verlangt:

1. Wenn eine externe Benutzer-ID verfügbar ist (von der HTTPD- oder Windows-Validierung), sucht CA SDM den Kontakt über die Anmelde-ID. Wenn der Kontakt gefunden wird und dieser einen Zugriffstyp hat, der die externe Authentifizierung zulässt, erhält der Benutzer Zugang zur Anwendung.
2. Wenn keine erfolgreiche externe Authentifizierung vorliegt, fordert CA SDM den Benutzer zur Eingabe einer Benutzer-ID und eines Kennworts auf. Die Anwendung sucht einen Kontaktdatensatz für die Benutzer-ID, ruft den Zugriffstyp ab und authentifiziert den Benutzer dann entsprechend des Zugriffstyps.

Für viele Installationen sind die vordefinierten Zugriffstypen zur Definition der Authentifizierung für den betreffenden Benutzertyp angemessen. In einigen Fällen müssen Sie aber die Authentifizierungsinformationen für einen vordefinierten Zugriffstyp gegebenenfalls ändern oder einen neuen Zugriffstyp definieren, um eine andere Authentifizierungsmethode für einige Ihrer Benutzer zu verwenden. Prüfen Sie die Authentifizierungseinstellungen für die vordefinierten Zugriffstypen, um zu entscheiden, ob sie Ihre Bedürfnisse erfüllen oder ob Sie sie ändern oder zusätzliche Typen definieren müssen.

Externe Authentifizierung

CA SDM erlaubt Anwendern den Zugriff auf das System ohne Eingabe einer Anwender-ID, wenn alle folgenden Voraussetzungen erfüllt sind:

- Für den Anwender wurde eine externe Authentifizierung festgelegt.
- Die Anwenderkennung des extern authentifizierten ist einem Kontakt in der Kontakttabelle zugeordnet.
- Der Kontaktdatensatz verfügt über einen Zugriffstyp, dessen Authentifizierungsdefinition eine externe Authentifizierung erlaubt.

Die externe Authentifizierung erlaubt Anwendern in den folgenden Fällen keinen Zugriff auf das System:

- Ein Anwender versucht, über einen ungesicherten Server auf das System zuzugreifen.
- Ein Anwender versucht, auf das System zuzugreifen, ihm ist jedoch ein Zugriffstyp zugewiesen, der keine externe Authentifizierung erlaubt.

Keiner der vordefinierten Zugriffstypen verwendet die externe Authentifizierung. Wenn Sie die externe Authentifizierung für Anwender verwenden möchten, sollten Sie erwägen, für die Zugriffstypen für Mitarbeiter, Analysten und Administratoren die externe Authentifizierung zu aktivieren. Ob Sie die externe Authentifizierung zulassen, hängt von den individuellen Anforderungen Ihres Standorts und den verschiedenen Arten von Anwendern ab. Wenn die externe Authentifizierung verwendet wird, steuert die Serverkonfiguration den Zugriff auf Dateien und Verzeichnisse. Wenn Sie die Authentifizierung für einen Zugriffstyp festlegen, können Sie die Verwendung entsprechend den folgenden Richtlinien einschränken.:

- Verwenden Sie keine bereits implementierte externe Authentifizierung, wie die Anwenderanmeldung unter Windows oder die Validierung über einen HTTPD-Server.
- Verwenden Sie eine bereits implementierte Authentifizierung, und erteilen Sie Berechtigungen auf der Grundlage dieser Authentifizierung.

Hinweis: Wenn keine externe Authentifizierung erlaubt ist, wird der Anwender auf der Grundlage der angegebenen Validierungsart authentifiziert.

Nachfolgend finden Sie einige Beispiele für externe Authentifizierung:

- Wenn sich ein Anwender mit Administratorrechten an einen Windows-Computer anmeldet, kann der Anwender administrative Aufgaben ausführen, ohne weitere Anmeldeinformationen angeben zu müssen.

- Wenn ein Anwender über einen HTTPD-Server authentifiziert wurde, er auf die Web-Schnittstelle zugreifen, ohne weitere Anmeldeinformationen angeben zu müssen. Da der Zugriffstyp "Administrator" den Web-Anwendertyp "Analytiker" angibt, wird die entsprechende Web-Schnittstelle für den Analytiker automatisch aufgerufen.

Hinweis: Weitere Details zur externen Authentifizierung finden Sie im Szenario *So implementieren Sie integrierte Windows-Authentifizierung für CA SDM*.

Validierungstypen

Validierungstypen authentifizieren Benutzer nur unter den folgenden Umständen:

- Der Zugriffstyp des Benutzers lässt keine externe Authentifizierung zu.
- Der Zugriffstyp des Benutzers lässt die externe Authentifizierung zu, aber der Benutzer wurde nicht extern validiert (der Benutzer hat zum Beispiel versucht, Zugriff über einen nicht sicheren Server zu erhalten).

CA SDM ermöglicht die folgenden Validierungsoptionen:

- **Kein Zugriff** - Benutzer dieses Typs haben keinen Zugriff, es sei denn, eine externe Authentifizierung ist zulässig und gültig.
- **Offen** - Benutzer dieses Typs haben Zugriff, ohne dass eine zusätzliche Authentifizierung erforderlich ist.
 - **Betriebssystem** - Benutzer dieses Typs geben ihr Betriebssystemkennwort ein, um Zugriff zu erhalten. Das für die Validierung verwendete Betriebssystem ist das Betriebssystem, das den Benutzervalidierungs-Host ausgeführt. Diese Option ist der Standardvalidierungstyp für die Zugriffstypen "Administrator", "Analyst" und "Mitarbeiter".
- **PIN** - Benutzer dieses Typs erhalten Zugriff, indem sie als Kennwort den korrekten Wert für das PIN-Feld in ihrem Kontaktdatensatz eingeben. Sie definieren das PIN-Feld, indem Sie den Attributnamen des Felds eingeben, wenn Sie "PIN" als Validierungstyp wählen. Dies ist der Standardvalidierungstyp für den Zugriffstyp "Kunde", der den Wert im Feld "Kunden-ID" (contact_num) als PIN verwendet.

Hinweis: Eine Liste der Attributnamen für das "cnt"-Objekt für die Kontakttable finden Sie im *Technischen Referenzhandbuch*.

Anzahl angemeldeter Anwender und Sitzungsanzahl

Folgende KPIs zählen die Anzahl der eindeutig lizenzierten Anwender, die im System angemeldet sind (zum Beispiel CA SDM-Web-Benutzeroberfläche, SOAP-Webservices, REST-Webservices usw.), unabhängig davon, wie viele Sitzungen jeder Anwender geöffnet hat:

Hinweis: Stellen Sie bei einem lizenzierten Anwender sicher, dass das Kontrollkästchen "Lizenziert?" auf der Seite "Zugriffstyp" des Kontakts aktiviert ist (navigieren Sie auf der Registerkarte "Administration" zu Sicherheit- und Rollenmanagement, Zugriffstyp, und suchen Sie nach dem Kontakt).

- webConcurrentLicenseCt
- webConcurrentSOAPLicenseCt
- webConcurrentRESTLicenseCt
- webConcurrentTotalLicenseCt

Folgende KPIs zählen die Anzahl der eindeutig nicht lizenzierten Anwender, die im System angemeldet sind, unabhängig davon, wie viele Sitzungen jeder Anwender geöffnet hat:

- webConcurrentNonLicenseCt
- webConcurrentSOAPNonLicenseCt
- webConcurrentRESTNonLicenseCt
- webConcurrentTotalNonLicenseCt

Folgende KPIs zählen die Anzahl der eindeutigen Sitzungen an, die während des Intervalls gestartet wurden:

- webSessionCt
- webSOAPSessionCt
- webRESTSessionCt

Weitere Informationen zur KPI-Beschreibung finden Sie auf der KPI-Detailseite (navigieren Sie auf der Registerkarte "Administration" zu Service Desk, KPI, und suchen Sie nach dem KPI). Weitere Informationen darüber, wie diese KPIs aus verschiedenen Sitzungstypen zählen, finden Sie unter dem Thema [So zählen KPIs aus verschiedenen Sitzungstypen](#). (siehe Seite 313)

So zählen KPIs aus verschiedenen Sitzungstypen

Es gibt verschiedene Sitzungstypen, die im System definiert sind. Folgende Tabelle zeigt, wie KPI diese Sitzungen zählen:

Hinweis: Alle vordefinierten KPIs werden als "Inaktiv" installiert. Damit ein KPI in Ihrem System funktionieren kann, muss das zugehörige Feld auf "Aktiv" gesetzt werden. Navigieren Sie auf der Registerkarte "Administration" zu Service Desk, KPI, und suchen Sie nach dem inaktiven KPI. Öffnen Sie den KPI, und klicken Sie auf "Aktivieren".

Wichtig! Es können nicht mehrere Versionen eines KPI mit demselben Namen gleichzeitig aktiv sein.

Sitzungstyp	Beschreibung des Sitzungstyps	Von KPIs gezählt
Webclient	Webbrowser-Sitzung	■ webSessionCt ■ webConcurrentLicenseCt ■ webConcurrentNonLicenseCt ■ webConcurrentTotalLicenseCt ■ webConcurrentTotalNonLicenseCt
Java-Client	Java-Client-Sitzung	■ webConcurrentTotalLicenseCt ■ webConcurrentTotalNonLicenseCt
Webservices	SOAP-Webservice-Sitzung	■ webSOAPSessionCt ■ webConcurrentSOAPLicenseCt ■ webConcurrentSOAPNonLicenseCt
Hilfsprogramm	Server-Hilfsprogrammsitzung	■ webConcurrentTotalLicenseCt ■ webConcurrentTotalNonLicenseCt
Portal	Portal-Sitzung	■ webConcurrentTotalLicenseCt ■ webConcurrentTotalNonLicenseCt
Knowledge-Chat	Knowledge-Chat-Sitzung	■ webConcurrentTotalLicenseCt ■ webConcurrentTotalNonLicenseCt
Mail Server	Mail Server-Sitzung	■ webConcurrentTotalLicenseCt ■ webConcurrentTotalNonLicenseCt
Anwenderspezifische Anwendung	Anwenderspezifische Anwendungssitzung	■ webConcurrentTotalLicenseCt ■ webConcurrentTotalNonLicenseCt

PDA-Client	PDA-Client-Sitzung	■ webSessionCt ■ webConcurrentLicenseCt ■ webConcurrentNonLicenseCt ■ webConcurrentTotalLicenseCt ■ webConcurrentTotalNonLicenseCt
REST-Client	REST-Webservice-Sitzung	■ webRESTSessionCt ■ webConcurrentRESTLicenseCt ■ webConcurrentRESTNonLicenseCt ■ webConcurrentTotalLicenseCt ■ webConcurrentTotalNonLicenseCt

Beispiel: KPI berechnet Anwenderanzahl

Ein lizenzierter Endanwender (mit aktiviertem Kontrollkästchen "Lizenziert?") und zwei nicht lizenzierte Endanwender sind in der Web-Self-Service-Schnittstelle angemeldet und überprüfen einige Ankündigungen.

Gleichzeitig sind fünf lizenzierte Analysten (mit aktiviertem Kontrollkästchen für den entsprechenden Zugriffstyp) bei der Analystenschnittstelle angemeldet und arbeiten an Incidents. Einer der Analysten meldet sich auch bei der SOAP-Webservices-Schnittstelle an.

- Der KPI "webConcurrentLicenseCt" zeigt die Zahl 6 an. Das bedeutet, dass derzeit sechs Lizenzen verwendet werden, unabhängig von der Anzahl der Schnittstellen, die jeder Anwender verwendet.
- Der KPI "webConcurrentNonLicenseCt" zeigt die Zahl 2 an. Das bedeutet, dass zwei nicht lizenzierte Anwender im System angemeldet sind, unabhängig von der Anzahl der Schnittstellen, die jeder Anwender verwendet.
- Der KPI "webSessionCt" zeigt die Zahl 8 an. Das bedeutet, es sind insgesamt acht Anwender auf der CA SDM-Web-Benutzeroberfläche angemeldet.
- Der KPI "webSOAPSessionCt" zeigt die Zahl 1 an. Das bedeutet, dass ein Anwender bei der SOAP-Webservice-Schnittstelle angemeldet ist.

(Kann nur für die Konfiguration für erweiterte Verfügbarkeit angewendet werden) Beispiel: KPIs berechnen Anwenderanzahlen aus verschiedenen Knoten

Ein lizenzierter Analyst meldet sich über den Hintergrundserver bei der Analystenschnittstelle an und arbeitet an Incidents. Der gleiche Analyst meldet sich über den Anwendungsserver bei der Analystenschnittstelle an. Der KPI "webConcurrentLicenseCt" zeigt die Zahl 1 an. Das bedeutet, dass derzeit eine Lizenz verwendet wird, unabhängig von der Anzahl der Knoten oder Server, über die der Anwender angemeldet ist.

Interne Protokolle

Sie können festlegen, ob ein bestimmter Zugriffstyp die Anzeige interner Protokolle zulässt. Wenn ein Kontakt interne Protokolle anzeigen darf, wird in den Protokollaktivitätsfenstern ein Kontrollkästchen mit der Bezeichnung "Intern" angezeigt. Der Kontakt kann dieses Kontrollkästchen aktivieren, um die Aktivität als intern zu kennzeichnen. Wenn Aktivitäten als intern gekennzeichnet sind, können nur Kontakte mit einem Zugriffstyp, der die Anzeige interner Protokolle zulässt, die Aktivität anzeigen oder davon benachrichtigt werden.

CA SDM-Integration

Der Zugriffstyp identifiziert auch den Benutzertyp, der mit diesem Zugriffstyp verbunden ist, wenn Benutzer andere CA-Produkte mit CA SDM verwenden. Wenn ein Kontakt mit diesem Zugriffstyp ein anderes Produkt verwendet, werden die Benutzerrechte für das Produkt anhand der im Zugriffstyp angegebenen Werte bestimmt.

Zuordnungen von Datenpartitionen

Datenpartitionen können individuellen Kontakten zugeordnet werden, aber die bevorzugte Methode ist, basierend auf dem Zugriffstyp Datenpartitionen zuzuweisen. Nach der Zuordnung von Datenpartitionen zu verschiedenen Zugriffstypen können Sie einen Kontakt mit einem bestimmten Zugriffstyp verknüpfen und dadurch seine Datenpartition definieren. Der Zugriffstyp verfügt über eine spezielle Option zum Überschreiben der Kontaktdatenpartition.

Um eine Datenpartition einem Zugriffstyp zuzuordnen, legen Sie die Datenpartitionen so fest, dass sie für Ihren Standort Sinn machen, und wählen dann eine der Datenpartitionen aus, wenn Sie einen Zugriffstyp definieren oder ändern.

Wichtig! Andere CA SDM-Sicherheitseinstellungen haben möglicherweise Vorrang vor der Datenpartition.

So richten Sie eine Datenpartition ein

Eine Datenpartition ist eine Untermenge einer CA SDM-Datenbank, die den Zugriff eines Anwenders auf Tickets und andere Datensätze auf der Basis ihres Inhalts steuert.

Zum Beispiel können Sie die Ansicht eines Anwenders der Datenbank nur auf die Konfigurationselemente beschränken, die der Organisation des Anwenders zugewiesen wurden. Sie können außerdem einen Anwender so einschränken, dass er nur zugewiesene Tickets aktualisieren kann; für andere Konfigurationselemente erhält er nur schreibgeschützten Zugriff.

Eine Datenaufteilung besteht aus einem Satz von Bedingungen. Die Datenaufteilungsbedingungen geben die Tabelle an, die von der Datenaufteilung und dem Bedingungstyp gesteuert wird. Bedingungstypen geben an, was der Anwender innerhalb der Datenaufteilung tun kann, zum Erstellen, Löschen, Aktualisieren, Anzeigen usw. Nachdem Sie einem Zugriffstyp eine Datenpartition zugewiesen haben, den Sie wiederum dem Kontaktdatensatz eines Anwenders zuweisen, steuern die Einschränkungen und Einschränkungstypen den Zugriff des Anwenders auf die Datensätze in der CA SDM-Datenbanktabelle.

Sie können Bedingungen auch unabhängig von der Datenaufteilung, in der sie verwendet werden, anzeigen. Zum Beispiel können Sie alle Bedingungen für eine bestimmte Tabelle anzeigen, unabhängig von der Datenaufteilung.

Überprüfen der Voraussetzungen

Bevor Sie die Datenpartition einrichten, überprüfen Sie die folgenden Voraussetzungen:

- [Struktur und Richtlinie der Datensicherheit](#) (siehe Seite 316)
- [Einrichten von Datenaufteilungen](#) (siehe Seite 317)
- [Angaben von Bedingungen](#) (siehe Seite 318)

Struktur und Richtlinie der Datensicherheit

Planen der Datensicherheit umfasst das Durchsetzen von Zugriffseinschränkungen auf den spezifischen Teil der Datenbank. Diese Einschränkungen können auf individuellen Kontakten entweder über Rollen oder über Zugriffstypen durchgesetzt werden:

Rollen

Definiert die Funktionalität, auf die Anwender in der Rolle zugreifen dürfen. Sie können eine oder mehrere Rollen einem individuellen Kontaktdatensatz oder einem Zugriffstyp zuweisen, um den funktionellen Zugriff für alle Zugriffstypen, die mit Kontakten verknüpft sind, zu definieren.

Zugriffstyp

Gibt an, wie Kontakte authentifiziert werden, wenn sie sich bei der Webschnittstelle anmelden. Zum Beispiel legt ein Zugriffstyp fest, ob die Kontakte Webformulare oder das Datenbankschema mit Web Screen Painter ändern können und welche Rollen für die Kontakte verfügbar sind.

Als Service Desk-Administrator können Sie die vordefinierten Zugriffstypen ändern, und Sie können neue Zugriffstypen erstellen. Sie können die Einschränkung über Rollen auf die individuellen Anwender oder auf eine Gruppe von Anwendern durchsetzen.

Identifizieren Sie Folgendes:

- Die Objekte und der Typ der Einschränkungen, die Sie auf diese Objekten durchsetzen möchten.
- Die Anwender oder Rollen, auf die die Datenpartition angewendet werden soll. Datenpartitionen können direkt auf Kontakte angewendet werden. Die bevorzugte Methode ist jedoch, die Datenpartitionen basierend auf der Rolle zuzuweisen und diese Rolle direkt zu allen Kontakten oder über den Zugriffstyp zuzuweisen.

Spezifikationen zum Einrichten von Datenpartitionen

Sie können eine unbegrenzte Anzahl von Datenaufteilungen definieren. Jede Datenpartition besteht aus einem Satz von Bedingungen und Validierungen für jede Datenbanktabelle, die von der Datenaufteilung eingeschränkt wird. Für jede Tabelle in einer Datenpartition können Sie unabhängige Berechtigungen zum Anzeigen, Aktualisieren, Erstellen oder Löschen von Datensätzen erteilen. Hierzu geben Sie Kriterien in einem ähnlichen Format wie in einer SQL WHERE-Klausel an. Sie können die Einschränkung auf der Basis eines beliebigen Attributs im Datensatz angeben, auf den zugegriffen wird, in Kombination mit beliebigen Daten im Kontaktdatensatz des Anwenders. Dadurch erhalten Sie eine große Flexibilität bei der Definition von Datenaufteilungen. Wenn Sie zum Beispiel das Feld „Anbieter“ in der Tabelle „Contact“ verwenden, können Sie Datenpartitionseinschränkungen für Anbieter festlegen, die direkt auf CA SDM zugreifen dürfen.

Aus Gründen der Leistung sind in CA SDM keine Datenaufteilungsbedingungen möglich, die eine Verbindung als kartesisches Produkt enthalten. Eine Verbindung als kartesisches Produkt resultiert aus einer Einschränkung, die den Operator „OR“ enthält, der eine völlige Einschränkung aller verknüpften Tabellen auf beiden Seiten des OR-Operators bewirkt. Um sicherzustellen, dass Ihre Datenaufteilungsbedingung keine Verbindung als kartesisches Produkt erzeugt, geben Sie den folgenden Befehl ein:

Windows

```
bop_cmd -f $NX_ROOT\bopcfg\interp\bop_diag.frg "check_queries()"
```

UNIX

```
bop_cmd -f $NX_ROOT/bopcfg/interp/bop_diag.frg "check_queries()"
```

Wichtig! Alle Datenaufteilungen, die von diesem Programm gekennzeichnet werden, müssen entsprechend aktualisiert werden.

Angeben von Bedingungen

Einschränkungen und Validierungstests können Sie in Majic mit Hilfe der Meta-Sprache für Objektdefinitionen festlegen.

Hinweis: Informationen finden Sie im *Technischen Referenzhandbuch*.

In Majic definierte Bedingungen ähneln stark einer SQL WHERE-Klausel, mit den folgenden Ausnahmen:

- Attributnamen in der Einschränkung sind Objekt-Attributnamen und nicht der Datenbank-Attributname aus dem Schema.
- Sie können auf den Wert eines Attributs im Kontaktdatensatz des angemeldeten Benutzers mit einem Namen im folgenden Format verweisen, wobei *att_name* der Majic-Name des gewünschten Attributs ist:

@root.att_name

Zum Beispiel gibt @root.location die Positions-ID (location) des aktuellen Kontakts an.

Sie geben Verbindungen im folgenden Format an, wobei *foreign-key* der Majic-Name des SREL-Attributs in der Tabelle ist, für das Sie die Datenpartitionseinschränkung schreiben, und *attribute-in-referenced-table* der Majic-Name des Attributs in der zu verknüpfenden Tabelle ist:

foreign-key.attribute-in-referenced-table

Geben Sie zum Beispiel Folgendes an, um auf den Wartungsanbieter des Assets zu verweisen, das zu einem Incident-Bericht gehört:

resource.vendor_repair

Diese Angabe ist rekursiv. Zum Beispiel können Sie auf den Namen des Anbieters auch mit dem folgenden Namen verweisen:

resource.vendor_repair.name

Die folgende Tabelle enthält gültige Einschränkungen für die Tabelle "Change_Request" (in der Change-Informationen gespeichert werden):

Bedingungstyp	Code und Beschreibung
Ansicht	<code>assignee.organization = @root.organization</code> Gibt an, dass der Benutzer Changes nur dann anzeigen kann, wenn die Organisation des Zuständigen mit der Organisation des Benutzers identisch ist.
Vor-Aktualisierung	<code>requestor = @root.id</code> Gibt an, dass der Benutzer Changes nur dann aktualisieren kann, wenn er der Anrufer oder der Anforderer ist.

Jedoch ist es nicht möglich, eine Einschränkung zu erstellen, die Verbindungen auf beiden Seiten des Ausdrucks verwendet, wie im folgenden Beispiel gezeigt:

`assignee.org = requestor.org`

Anzeigen von durch Datenpartitionen gesteuerte Tabellen

Eine gesteuerte Tabelle ist eine Liste der Tabellen, auf denen ein Service Desk-Administrator mithilfe von Datenpartitionen Einschränkungen durchsetzen kann. Diese Tabellen geben Ihnen einen Einblick auf die Objekte und Tabellen, für die Sie den Anwenderzugriff beschränken können.

Hinweis: Sie können gesteuerte Tabellen nicht hinzufügen oder löschen oder deren Objektnamen ändern.

Gehen Sie wie folgt vor:

1. Wählen Sie auf der Registerkarte "Administration" die Option "Sicherheits- und Rollenmanagement", "Datenpartitionen", "Über Datenpartitionen gesteuerte Tabellen".
Die Liste der gesteuerten Tabellen wird geöffnet.
2. (Optional) Klicken Sie auf "Filter anzeigen", und füllen Sie mindestens ein Suchfeld aus.
3. Wählen Sie den Namen der anzuzeigenden Tabelle aus.
Die Seite Über Datenpartition gesteuerte Tabellen - Detail wird geöffnet.

Erstellen einer Datenpartitionseinschränkung

Datenpartitionseinschränkungen schränken den Zugriff auf den Datenbankdatensatz für Anwender ein, die der Datenpartition zugewiesen werden.

Gehen Sie wie folgt vor:

1. Wählen Sie auf der Registerkarte "Administration" die Option "Sicherheits- und Rollenmanagement" > "Datenpartitionen" > "Datenpartitionseinschränkungen".

Die Seite "Datenpartitionseinschränkungen - Liste" wird geöffnet.

2. Klicken Sie auf "Neu erstellen".

Die Seite "Neue Datenpartitionseinschränkung erstellen" wird geöffnet.

3. Füllen Sie die [Felder in Datenpartitionseinschränkungen](#) (siehe Seite 321) nach Bedarf aus.

4. Füllen Sie die Informationen auf den Registerkarten nach Bedarf aus:

Bedingung

Gibt die Kriterien für die Datensätze in der Tabelle an, die von einem der Datenpartition zugewiesenen Anwender angezeigt, erstellt, aktualisiert oder gelöscht werden können. Sie können zum Beispiel angeben, dass Anwender nur Issues aktualisieren können, die ihnen zugewiesen sind. Fordert ein Anwender in der Datenpartition einen Datensatz an, der diese Bedingung nicht erfüllt, ist der Datensatz schreibgeschützt.

Grenze: 4000 Byte

SQL-Übersetzung

Zeigt die Definition der Bedingung im SQL-Format an. Die Bedingung, die Sie auf der Registerkarte "Einschränkung" eingegeben haben, wird überprüft, und die zugrunde liegende SQL-WHERE-Klausel wird erstellt. Diese Übersetzung wird zur Verifizierung auf der Registerkarte "SQL-Übersetzung" angezeigt.

5. Klicken Sie auf "Speichern".

Die Einschränkung wird gespeichert und der Datenpartition hinzugefügt.

Beispiel: Erstellen einer Datenpartitionseinschränkung für CAB-Zuweisungen

Sie können eine Datenpartitionseinschränkung erstellen, die Anwender nur Changes aktualisieren lässt, die einem CAB zugewiesen sind, dem der angemeldete Anwender angehört.

Um eine Datenpartitionseinschränkung für CAB-Change-Benutzerzuweisungen zu erstellen, weisen Sie die folgenden Einschränkungswerte für eine "Change_Request"-kontrollierte Tabelle in einer Datenpartition zu:

- Constraint type: Pre-Update
- Constraint specification: cab.[group]group_list.member IN (@root.id)

Der angemeldete Benutzer kann nur Changes aktualisieren, die einem CAB zugewiesen wurden, dem der Benutzer angehört.

Siehe auch:

[Felder in Datenpartitionseinschränkungen](#) (siehe Seite 321)

[Definition von Bedingungen](#) (siehe Seite 323)

Felder in Datenpartitionseinschränkungen

Füllen Sie die folgenden Felder aus, um die Felder in Datenpartitionseinschränkungen hinzuzufügen oder zu ändern:

Name der Datenaufteilung

Gibt den Namen der Datenpartition an, für die die Einschränkung definiert wird.

Tabellenname

Gibt die Datenbanktabelle an, die von der Einschränkung gesteuert wird.

Bedingungstyp

Definiert den Einschränkungstyp, der definiert wird. Es gibt für jede Tabelle in einer Datenpartition sechs Bedingungstypen.

Erstellen

Gibt die Kriterien an, die vor der Erstellung eines Datensatzes erfüllt sein müssen. Wenn ein Anwender in der Datenpartition die Erstellung eines Datensatzes versucht, der nicht der Erstellungstestbedingung entspricht, gibt CA SDM die mit der Bedingung verbundene Fehlermeldung aus und speichert den Datensatz nicht.

Standardeinstellungen

Gibt eine oder mehrere Zuweisungsanweisungen an, durch Semikola getrennt, zur Definition der Werte, die leeren Feldern in einem neuen Datensatz zum Zeitpunkt seiner Speicherung zugewiesen werden. Die Syntax jeder Zuweisungsanweisung lautet wie folgt, wobei *att_name* der Name eines Majic-Attributs aus dem Datensatz ist und *value* eine Ganzzahl, eine Zeichenfolge zwischen Anführungszeichen oder ein Verweis der Form *@root.att_name* auf ein Majic-Attribut im Kontaktdatensatz für den aktuellen Anwender sein kann:

att_name=value

Für Tabellen, die für Tickets aktualisiert werden, werden Standardwerte in den Datensatz zum Zeitpunkt seiner Anzeige eingefügt und werden in der ursprünglichen Anzeige eines neuen Datensatzes angezeigt. Sie können einem Bezugsfeld einen Standardwert zuweisen (Majic SREL), indem Sie den Wert in Form einer permanenten ID kodieren. Eine permanente ID ist ein Objektname, der von einem Doppelpunkt und einer Ganzzahl-ID gefolgt wird. Zum Beispiel können Sie einen Standardwert für Kategorie festlegen, indem Sie Folgendes in der Standardwertspezifikation angeben, wobei PCAT das Ziel von SREL (gemäß der Majic-Datei) und 12345 die ID-Nummer der gewünschten Kategorie ist:

```
category='PCAT:12345'
```

Sie können permanente IDs für ein Objekt mit einem Befehl im folgenden Format auflisten:

```
bop_odump domsrvr pcat "" sym
```

Löschen

Gibt die Kriterien an, die zum Löschen eines Datensatzes erfüllt sein müssen. Wenn ein Anwender in der Datenpartition einen Datensatz zu löschen versucht, der nicht der Löschbedingung entspricht, gibt CA SDM die mit der Bedingung verbundene Fehlermeldung aus und löscht den Datensatz nicht.

Vor-Aktualisierung

Gibt die Datensätze in der gesteuerten Tabelle an, die ein Benutzer in der Datenaufteilung aktualisieren kann. Wenn ein Anwender in der Datenpartition einen Datensatz anfordert, der nicht der Vor-Aktualisierungsbedingung entspricht, versetzt CA SDM den Datensatz in den schreibgeschützten Status und gibt die mit der Bedingung definierte Fehlermeldung aus.

Update

Gibt die Kriterien an, die zum Speichern eines Datensatzes erfüllt sein müssen. Wenn ein Anwender in der Datenpartition einen Datensatz zu speichern versucht, der nicht der Aktualisierungsbedingung entspricht, gibt CA SDM die mit der Bedingung verbundene Fehlermeldung aus und speichert den Datensatz nicht.

Ansicht

Gibt die Datensätze in der gesteuerten Tabelle an, die ein Benutzer in der Datenaufteilung anzeigen kann. Diese Bedingung gilt automatisch für alle Listen, die von einem Benutzer in dieser Datenaufteilung gewählt wurden, zusätzlich zu den vom Benutzer explizit angegebenen Auswahlkriterien.

„Anzeigen“ kann Verbindungen zu anderen Tabellen und Verweise der Form `@root.att_name` auf Majic-Attribute im Kontaktdatensatz für den aktuellen oder angemeldeten Benutzer enthalten. Gültige Beispiele sind:

```
requestor.organization = @root.organization
```

```
requestor.organization.name = 'MIS'
```

```
assignee = @root.id
```

```
assignee.organization = @root.organization
```

Hinweis: Die Einschränkungstypen "Erstellen", "Löschen" und "Voraktualisieren" unterstützen jetzt Verknüpfungen mit anderen Tabellen. Sie können auch Referenzen vom Typ `@root.attribute` zu Attributen im Kontaktdatensatz des aktuellen Benutzers einschließen.

Datensatzstatus

Gibt an, ob die Einschränkung aktiv oder inaktiv ist.

Fehlermeldung

Gibt die Meldung an, die an den Anwender zurückgegeben wird, wenn die Kriterien für die Bedingung nicht erfüllt sind. Beispiel: "Sie können nur die Ihnen zugewiesenen Issues aktualisieren" oder "Sie können nur Issues für Ihre Organisation erstellen" oder "Sie können ihren Kontaktdatensatz aktualisieren, aber Sie können nicht die Datenpartition verändern".

Definition von Bedingungen

Geben Sie die Bedingung im Majic-Format an (Metasprache zum Definieren von CA SDM-Objekten).

Beim Bedingungstyp "Anzeigen" kann die Bedingung Verbindungen zu anderen Tabellen und Referenzen im Format "@root.att_name" zu Majic-Attributen im Kontaktdatensatz für den angemeldeten Anwender enthalten. Ansonsten kann er keine Verbindungen zu anderen Tabellen enthalten. Er kann jedoch Referenzen im Format "@root.att_name" zu Majic-Attributen im Kontaktdatensatz für den angemeldeten Anwender enthalten.

Ist der Bedingungstyp "Standardwerte", können Sie ein oder mehrere Zuweisungsanweisungen (getrennt durch Semikolons) angeben, die Werte enthalten, die in leere Felder eines neuen Datensatzes eingefügt werden, wenn der Datensatz gespeichert wird. Die Syntax für jede Zuweisungsanweisung lautet:

```
att_name=value
```

"att_name" ist hierbei der Name eines Majic-Attributs aus dem Datensatz, und der Wert kann eine Ganzzahl, eine Zeichenfolge in Anführungszeichen oder eine Referenz im Format "@root.att_name" zu einem Majic-Attribut im Kontaktdatensatz für den angemeldeten Anwender sein. Die Art und Weise, auf die CA SDM Standardwerte verwendet, hängt von der Tabelle ab, auf die sie sich auswirken.

Für Tabellen, die von CA SDM aktualisiert werden, wie zum Beispiel Issues, werden die Standardwerte in den Datensatz geschrieben, wenn er angezeigt wird, und sie werden sofort angezeigt, wenn ein neuer Datensatz erstellt wird. Ein Standardwert kann einem Referenzfeld (einem Majic SREL) zugewiesen werden, indem er in Form einer permanenten ID codiert wird (ein Tabellename gefolgt von einem Doppelpunkt und einer ganzzahligen ID). Zum Beispiel können Sie den Standardwert für die Kategorie setzen, indem Sie in das Folgende in die Spezifikation "Standardwerte" einfügen:

```
category='PCAT:12345'
```

"PCAT" ist hierbei das Ziel der SREL wie in der Majic-Datei gezeigt, und "12345" ist die ID-Nummer der gewünschten Kategorie. Permanente IDs für eine Tabelle können Sie mit einem Befehl im folgenden Format auflisten:

```
bop_odump domsrvr pcat "" sym
```


Erstellen von Datenpartitionen

Eine Datenpartition ist eine Untermenge einer CA SDM-Datenbank, die den Zugriff eines Anwenders auf Tickets und andere Datensätze auf der Basis ihres Inhalts steuert.

Gehen Sie wie folgt vor:

1. Wählen Sie auf der Registerkarte "Administration" die Option "Sicherheits- und Rollenmanagement", "Datenpartitionen", "Datenpartitionen - Liste".

Die Seite "Datenpartitionen - Liste" wird geöffnet.

2. Klicken Sie auf "Neu erstellen".

Die Seite "Neue Datenpartition erstellen" wird geöffnet.

3. Füllen Sie die Felder nach Bedarf aus:

Datenaufteilung

Gibt ein eindeutiges Kennzeichen für die Datenpartition an.

Datensatzstatus

Gibt an, ob die Partition aktiv oder inaktiv ist.

4. Klicken Sie auf "Speichern".
5. Klicken Sie auf Neue Einschränkung, und hängen Sie Einschränkungsdefinitionen an die Partition an.
6. Klicken Sie auf "Speichern".

Die Datenpartition wird mit der Datenpartitionseinschränkung gespeichert.

Siehe auch:

[Erstellen einer Datenpartitionseinschränkung](#) (siehe Seite 320)

Erstellen eines Zugriffstyps

Die Zugriffstypen definieren alle Aspekte der Sicherheit. Es sind mehrere vordefinierte Zugriffstypen enthalten. Sie können diese ändern oder auch neue definieren. Jeder Zugriffstyp für einen Anwender steuert die folgenden Aspekte des Systemverhaltens:

- So führen Sie eine CA SDM-Web-Authentifizierung beim Einloggen eines Anwenders durch.
- Die Zugriffsebene für den Anwender.
- Ob der Anwender Webformulare oder das Datenbankschema mit Web Screen Painter ändern kann.
- Was sind die für den Anwender verfügbaren Rollen.

Gehen Sie wie folgt vor:

1. Wählen Sie auf der Registerkarte "Administration" die Option "Sicherheit und Rollenmanagement" > "Zugriffstypen".

Die Seite "Zugriffstypen - Liste" wird geöffnet.

Standard: 15

2. Klicken Sie auf Neu erstellen, und füllen Sie die [Zugriffstypenfelder](#) (siehe Seite 326) auf der Seite Neuen Zugriffstyp erstellen nach Bedarf aus.
3. Verwenden Sie die Registerkarten, um die folgenden Aufgaben abzuschließen:
 - [Konfigurieren der Webauthentifizierung für einen Zugriffstyp](#) (siehe Seite 327)
 - [Zuweisen von Web Screen Painter-Berechtigungen zu Zugriffstypen](#) (siehe Seite 328)
 - [Zuweisen von Rollen zu einem Zugriffstyp](#) (siehe Seite 329)
4. Klicken Sie auf "Speichern".

Der Zugriffstyp ist nun erstellt.

Zugriffstypfelder

Die nachstehenden Felder werden auf den Seiten "Zugriffstyp erstellen", "Zugriffstyp - Detail" und "Zugriffstyp aktualisieren" angezeigt.

Symbol

Gibt einen eindeutigen Bezeichner für den Zugriffstyp an.

Standard?

Zeigt an, ob dieser Zugriffstyp der Standardwert ist, der mit Kontakten verbunden ist.

Datensatzstatus

Gibt an, ob dieser Zugriffstyp aktiv oder inaktiv ist.

Beschreibung

Beschreibt den Zugriffstyp. Mit diesem Feld führen Sie die Merkmale des Zugriffstyps auf.

Interne Benachrichtigung erhalten

Bestimmt, ob die mit dem Zugriffstyp verbundenen Kontakte eine interne Benachrichtigung über Aktivitäten im Zusammenhang mit Tickets erhalten.

Zugriffsebene

Bestimmt, welche Zugriffstypen ein Anwender einem anderen Anwender gewähren kann. Ein Anwender kann dem Kontaktdatensatz eines anderen Anwenders einen Zugriffstyp nur dann zuweisen, wenn die Zugriffsebene des Zugriffstyps, den er zuweisen will, denselben wie oder einen niedrigeren Rang aufweist als die Zuweisungsebene des eigenen Zugriffstyps. Die Ebenen sind wie folgt eingestuft:

- Admin (höchste)
- Analyst
- Kunde/Mitarbeiter
- Kein (niedrigste)

Lizenziert?

Bestimmt, ob dieser Kontakt ein lizenzierter Zugriffstyp ist. Kontakte, die unlicenzierten Zugriffstypen zugewiesen sind, können lediglich ihre eigenen personenbezogenen Daten anzeigen und aktualisieren.

Hinweis: KPIs zählen die gleichzeitigen Verwendungen der Anwender vom System aus (zum Beispiel, CA SDM-Web-Benutzeroberfläche, SOAP-Webservices, REST-Webservices usw.). Zum Beispiel zählt der KPI `webConcurrentLicenseCt` die Höchstanzahl von eindeutigen Anwendern (mit der Option "Lizenziert?" ausgewählt), die bei der CA SDM-Web-Benutzeroberfläche während des Intervalls angemeldet sind. Weitere Informationen über die Anzahl angemeldeter und lizenzierter Anwender finden Sie im *Administrationshandbuch*.

Konfigurieren der Webauthentifizierung für einen Zugriffstyp

Sie können die Webauthentifizierung und den Validierungstyp konfigurieren, um anzugeben, wie die diesem Zugriffstyp zugewiesenen Rollen authentifiziert werden, wenn Anwender versuchen, auf CA-Produkte zuzugreifen. Füllen Sie die folgenden Felder in der Registerkarte Webauthentifizierung aus.

Externe Authentifizierung ermöglichen

Aktivieren Sie dieses Kontrollkästchen, wenn Sie zulassen möchten, dass Kontakte extern authentifiziert werden, z. B. vom HTTPD-Server oder Betriebssystem. Wenn Sie diese Option auswählen, werden Anwender mit diesem Zugriffstyp mithilfe der entsprechenden externen Methode, die bei der Installation konfiguriert wurde, validiert. Überprüfungen gewährleisten, dass keine externe Validierung stattgefunden hat (z. B. dass der Anwender nicht versucht hat, über einen unsicheren Server zuzugreifen) und dass der Anwender im System als gültiger Kontakt definiert ist und eine Anmelde-ID verwendet. Danach verwendet das System den Zugriffstyp, um die richtige Schnittstelle für die Verwendung zu bestimmen.

Validierungstyp

Definiert, wie Anwender authentifiziert werden, wenn eine externe Authentifizierung entweder nicht erlaubt ist oder fehlschlägt (wenn der Anwender zum Beispiel versucht, über einen nicht sicheren Server zuzugreifen). Folgende Optionen stehen zur Verfügung:

Kein Zugriff

Verweigert den Zugriff auf CA-Produkte, es sei denn, die externe Authentifizierung ist zulässig und gültig.

Öffnen

Der Zugriff auf CA-Produkte ist immer zulässig, wobei keine zusätzliche Authentifizierung erforderlich ist.

OS

Der Zugriff auf CA-Produkte ist über den Anwendernamen und das Kennwort des Betriebssystems zulässig.

PIN / PIN-Nummer

Anwender dieses Typs haben nur dann Zugriff, wenn sie in ihrem Kontaktdatensatz den richtigen Wert für das PIN-Feld eingeben. Wenn Sie die PIN-Option ausgewählt haben, können Sie wählen, in welchem Feld des Kontaktdatensatzes die PIN gespeichert ist, indem Sie den Feldattributnamen im Bearbeitungsfeld "PIN-Feld" eingeben.

CA EEM

Zugriff auf die CA-Produkte wird durch CA EEM erlaubt. Diese Option ist nur dann verfügbar, wenn CA SDM in CA EEM integriert ist.

Zuweisen von Web Screen Painter-Berechtigungen zu Zugriffstypen

Mit dem Hilfsprogramm Web Screen Painter (WSP) können CA SDM-Anwender Webformulare und Schemen erstellen und veröffentlichen. Die Registerkarte Web Screen Painter steuert auch den Datenbankzugriff für Web Screen Painter-Vorschausitzungen. Sehen Sie für die Details über WSP die *Online-Hilfe zu Web Screen Painter* an.

Wählen Sie auf der Registerkarte Web Screen Painter die Berechtigungen aus, die Sie für einen Zugriffstyp erlauben möchten.

Formulare ändern

Ermöglicht den Anwendern, Änderungen an vorhandenen Formularen vorzunehmen, ohne die Änderungen allen Anwendern zur Verfügung zu stellen.

Schema ändern

Ermöglicht den Anwendern, Änderungen an einem vorhandenen Schema vorzunehmen, ohne die Änderungen allen Anwendern zur Verfügung zu stellen.

Formulare veröffentlichen

Ermöglicht den Anwendern, ihre überarbeiteten Formulare allen Anwendern zur Verfügung zu stellen.

Schema veröffentlichen

Ermöglicht den Anwendern, ihr überarbeitetes Schema allen Anwendern zur Verfügung zu stellen.

Vorschausitzung kann Datenbank aktualisieren

Ermöglicht den Anwendern, Änderungen an der Datenbank während einer Vorschausitzung vorzunehmen. Standardmäßig sind Änderungen an der Datenbank während einer Vorschausitzung nicht zulässig.

Zuweisen von Rollen zu einem Zugriffstyp

Durch das Zuweisen der Rollen zu einem Zugriffstyp beschränken Sie den Zugriff der Kontakte, die den Rollen zugewiesen sind, auf bestimmte Funktionsbereiche.

Gehen Sie wie folgt vor:

1. Wählen Sie die folgenden Rollen für diesen Zugriffstyp aus:

Berichterstellungsrolle

Definiert den Zugriff auf die Berichterstellung für diesen Typ.

REST-Webservice-API-Rolle

Definiert den Zugriff auf die REST-Webservices für diesen Typ.

SOAP-Webservice-API-Rolle

Definiert den Zugriff auf die SOAP-Webservices für diesen Typ.

Befehlszeilendienstprogramm - Rolle

Definiert den Zugriff auf die Befehlszeilenhilfsprogramme für diesen Typ.

2. Klicken Sie auf "Rollen aktualisieren".
Die Seite "Rollen - Suche" wird geöffnet.
3. Geben Sie beliebige Suchkriterien ein, mit denen die Liste auf die gewünschten Rollen beschränkt werden soll, und klicken Sie auf Suchen.
Die Seite Zugewiesene Rollen - Aktualisierung wird geöffnet; hier werden die Rollen aufgeführt, die den Suchkriterien entsprechen.
4. Markieren Sie in der linken Liste die Rollen, die Sie diesem Zugriffstyp zuweisen möchten. Halten Sie die STRG-Taste gedrückt, während Sie mit der linken Maustaste klicken, um mehrere Elemente auszuwählen.
5. Klicken Sie auf die doppelten Rechtspfeile, nachdem Sie alle gewünschten Rollen ausgewählt haben.
Die markierten Rollen werden in die rechte Liste "Zugewiesene Rollen" aufgenommen.
6. Klicken Sie auf OK.
Die Seite "Zugriffstyp - Details" wird geöffnet; hier werden die zugewiesenen Rollen auf der Registerkarte "Rollen" aufgeführt.
7. Klicken Sie auf "Speichern".
Die Seite "Zugriffstyp - Details" wird geöffnet, und es wird eine Bestätigungsmeldung angezeigt, dass Ihre Änderungen gespeichert wurden.
8. Markieren Sie die Rolle, die beim Anmelden standardmäßig für diesen Zugriffstyp verwendet werden soll, und klicken Sie auf "Standardrolle festlegen".
Ihre Auswahl für die Standardrolle wird gespeichert.

Hinzufügen der Datenpartition zu einer Rolle

Wechseln Sie zu der Rolle, zu der die Datenpartition verknüpft war. Die Rolle hat nur Zugriff auf diese Datenpartition, die ihr zugewiesen ist.

Gehen Sie wie folgt vor:

1. Wählen Sie auf der Registerkarte "Administration" "Sicherheit und Rollenmanagement", "Rollenverwaltung", "Rollenliste" aus.
Die Seite Rollenliste wird angezeigt.
2. Wählen Sie eine Rolle aus, und klicken Sie auf Bearbeiten.
3. Gehen Sie zur Registerkarte Autorisierung und klicken Sie auf Datenpartitionsname.
4. Suchen und wählen Sie den Datenpartitionsnamen aus der Liste "Datenpartition" aus.
5. Wählen Sie auf der Registerkarte Autorisierung die Option Kontaktdatenpartition überschreiben aus. Wenn "K Kontaktdatenpartition überschreiben" ausgewählt ist, dann wird die Rollendatenpartition durchgesetzt, anderenfalls wird die Kontaktdatenpartition durchgesetzt.
6. Klicken Sie auf "Speichern".

Testen der Datenpartitionseinschränkungen

Testen Sie die Datenpartitionseinschränkungen, um sicherzustellen, dass die von Ihnen erstellte Einschränkung entsprechend auf den Kontakten durchgesetzt ist. Versuchen Sie, Datensätze anzuzeigen oder zu bearbeiten, für die die Datenpartitionseinschränkung den Zugriff beschränken sollte.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei CA SDM mithilfe des Kontakts an, für den Sie die Datenpartitionseinschränkungen durchgesetzt haben.
2. Versuchen Sie, auf die Objektdaten zuzugreifen, auf denen Datenpartitionseinschränkungen durchgesetzt sind.

Wenn die Einschränkungen wie geplant funktionieren, dann ist dies ein Hinweis darauf, dass die Datenpartition erfolgreich erstellt und angewendet wurde.

Konfigurieren von Knowledge Management-Datenpartitionseinschränkungen für rollenbasierte Berechtigungen

Knowledge Management-Datenpartitionen sind in CA SDM standardmäßig für die Unterstützung von Gruppen- und Rollenberechtigungen aktiviert. Wenn Sie ein Upgrade von einer Vorversion durchführen, können Sie mit Hilfe des Migrations-Tools Ihre bestehenden Datenpartitionsbeschränkungen aktualisieren.

Wenn Sie benutzerdefinierte Datenpartitionseinschränkungen verwendet haben, um Wissensberechtigungen in Vorversionen zu verwalten, aktualisieren Sie die Beschränkungen für die Tabellen O_INDEXES und SKELETONS manuell. Sie können die Standard-Datenpartitionseinschränkungen anzeigen und Änderungen durchführen, wenn dies für Ihre Umgebung erforderlich ist.

Gehen Sie wie folgt vor:

1. Wählen Sie auf der Registerkarte "Administration" die Option "Sicherheits- und Rollenmanagement" > "Datenpartitionen" > "Datenpartitionseinschränkungen".
Die Seite "Datenpartitionseinschränkungen - Liste" wird geöffnet.
2. Klicken Sie auf Filter zeigen, und suchen Sie mit den folgenden Suchkriterien:
 - **Service Desk-Analyst** in der Datenpartitionssuche.
 - **O_INDEXES** in der Tabellensuche.
3. Bearbeiten Sie den Einschränkungstyp Anzeige, indem Sie auf der Registerkarte Einschränkung "READ_PGROUP in @root.pgroups" folgendermaßen ersetzen:
`READ_PGROUP in @root.pgroups OR
READ_PGROUP.[pgroup]contained_roles.role IN @root.id`
4. Speichern Sie die Einschränkung.
5. Bearbeiten Sie die Einschränkungstypen Löschen und Vor-Aktualisierung, indem Sie auf der Registerkarte Einschränkung "WRITE_PGROUP in @root.pgroups" folgendermaßen ersetzen:
`WRITE_PGROUP in @root.pgroups OR WRITE_PGROUP.[pgroup]contained_roles.role IN
@root.role`
6. Speichern Sie die Einschränkungen.
7. Wiederholen Sie diese Schritte, um die Einschränkungen Anzeigen, Löschen und Voraktualisierung in der Tabelle SKELETONS in Ihrer Datenpartition zu aktualisieren.
Die Datenpartitionseinschränkungen werden aktualisiert.

Umfragen

Über Kundenumfragen können CA SDM-Administratoren Kunden-Feedback zur Service Desk-Leistung systematisch sammeln und analysieren. Sie können Umfragen den Anforderungen Ihres Standorts entsprechend anpassen.

Konfigurieren Ihres Systems für Umfragen

Bevor Sie Umfragen verwenden können, müssen Sie Ihr System entsprechend konfigurieren. Dies umfasst zwei Schritte:

1. Installieren Sie und konfigurieren Sie die CA SDM Web-Schnittstelle. Wenn ein Benutzer den URL für eine Umfrage aufruft, formatiert die Web-Schnittstelle die Umfrage und trägt die Umfragedaten ein. Weitere Informationen finden Sie im *Implementierungshandbuch*.
2. Konfigurieren und installieren Sie die Option „web_cgi_url“ mit dem Optionsmanager, um den Speicherort der Web-Engine von CA SDM anzugeben. Ausführliche Informationen finden Sie im Kapitel "Steuern des Systemverhaltens" und in der *Online-Hilfe*.

Vorbereiten einer Umfrage

Sie bereiten Umfragen im Fenster „Kundenumfrage – Liste“ vor, das ein typisches Listenfenster ist. Zum Beispiel können Sie in diesem Fenster alle Umfragen oder eine Untermenge der Umfragen auf der Basis der eingegebenen Suchkriterien anzeigen. Sie können neue Umfragen erstellen, Details zu einer bestimmten Umfrage anzeigen und einen Bericht für die aktuell aufgelisteten Umfragen erstellen.

Jede Umfrage hat die folgenden Merkmale, die Sie definieren können:

- Einen Namen, den Sie für die Suche und für Berichtszwecke verwenden können.
- Eine Einführung, in der Sie den Kunden den Zweck der Umfrage erklären können.
- Eine sortierte Liste mit Fragen, die der Kunde beantworten soll, wobei jede Frage einen Satz möglicher Antworten umfasst.
- Einen optionalen Bereich, in den der Benutzer formatfreie Kommentare eingeben kann.
- Eine Abschlussmeldung, die angezeigt wird, nachdem der Benutzer die Umfrage abgesendet hat.

Hinweis: Weitere Informationen zur Erstellung von Umfragen finden Sie in der *Online-Hilfe*.

Definieren von Umfragebenachrichtigungen

Auf der Registerkarte "Umfrage" auf der Seite "Aktivitätsbenachrichtigung aktualisieren" können Sie eine Umfragebenachrichtigung für eine Aktivitätsbenachrichtigung definieren. Wenn die ausgewählte Aktivitätsbenachrichtigung ausgelöst wird, empfängt der Kontakt, der das Ticket ausgelöst hat, die ausgewählte Umfragebenachrichtigung. Ein Aktivitätsprotokoll wird generiert, zum einen, wenn eine Umfragebenachrichtigung gesendet wird, und zum anderen, wenn eine Umfrage von einem Kunden empfangen wird.

So richten Sie eine Umfragebenachrichtigung ein:

1. Wählen Sie auf der Registerkarte "Administration" die Option "Benachrichtigungen" > "Aktivitätsbenachrichtigungen" aus.
Die Liste der Aktivitätsbenachrichtigungen wird angezeigt.
2. Wählen Sie die gewünschte Aktivitätsbenachrichtigung aus.
Die Detailseite wird angezeigt.
3. Klicken Sie auf die Schaltfläche "Bearbeiten".
Die Seite "Aktivitätsbenachrichtigung aktualisieren" wird angezeigt.
4. Bearbeiten Sie die Felder nach Bedarf.
5. Wählen Sie in der Dropdown-Liste den entsprechenden Objekttyp aus.
6. Klicken Sie auf die Registerkarte "Umfrage".

Diese Registerkarte enthält die folgenden Felder:

Umfrage senden

Mit diesem Kontrollkästchen können Sie die Umfrage aktivieren oder deaktivieren. Wenn Sie dieses Kontrollkästchen aktivieren, wird die Umfrage an den Kontakt gesendet, sobald die markierte Aktivitätsbenachrichtigung ausgelöst wird.

Standardumfrage

Legen Sie eine Standardumfrage über das Suchsymbol fest, oder geben Sie eine eigene Umfrage im Textfeld an.

Benachrichtigungsmethode

Wählen Sie *eine* der folgenden Benachrichtigungsmethoden aus:

- E-Mail
- Benachrichtigung
- Pager_Email

Titel der Umfragemeldung

Geben Sie den Titel für die Umfrage ein.

Text der Umfragemeldung

Geben Sie eine Nachricht für den Kontakt ein. Wenn ein Benutzer eine Benachrichtigung über eine Umfrage empfängt, enthält der Meldungstext automatisch eine URL, auf die der Benutzer über seinen Webbrowser zugreifen kann, um das Umfrageformular aufzurufen und auszufüllen.

7. Speichern Sie die Aktivitätsbenachrichtigung.

Wenn die ausgewählte Aktivitätsbenachrichtigung ausgelöst wird, empfängt der Kontakt, der das Ticket ausgelöst hat, die ausgewählte Umfragebenachrichtigung.

Berichte zu Umfragen

Innerhalb von CA SDM können Sie Berichte zu Umfragen innerhalb der Registerkarte „Administration“ des Webclients auf alle üblichen Arten erstellen. Zum Beispiel können Sie im Fenster „Kundenumfrage – Liste“ im Menü „Datei“ die Option „Berichte“ und dann „Übersichtsbericht“ oder „Detailbericht“ wählen. Außerdem können Sie in den verschiedenen Detailfenstern „Formular drucken“ wählen, um die Formulardaten für Ihre Umfragen, Fragen und Antworten zu drucken.

Sie können auf der Basis der Umfragedaten, die in der CA SDM-Datenbank verwaltet werden, auch Ihre eigenen Berichte entwerfen.

Verwaltete Umfrage

Mit der Funktion „Verwaltete Umfrage“ kann der CA SDM-Administrator eine gewünschte ausgefüllte Beispielumfrage auswählen und sie einer bestimmten Umfrage zuordnen. Der Administrator kann dann gezielte Requests verteilen, damit Befragte die Umfrage zu einem bestimmten Zeitpunkt durchführen. Dies gibt dem Administrator die Flexibilität, offene Umfragezeitspannen zu erstellen, während die Möglichkeit aktivitätsbasierter und kategoriebasierter Umfragen im Zusammenhang mit Requests, Changes und Issues beibehalten wird.

Der Zweck von verwalteten Umfragen ist, einen Mechanismus für die Verwaltung von Umfragen zu liefern. Diese Funktion kann für Umfrageformulare nützlich sein, die von Zeit zu Zeit überwacht werden müssen (zum Beispiel Umfragen, die nur während einer kurzen Zeitspanne jedes Jahr verwendet werden, oder Umfragen, die zu lange offline waren).

Wichtig! Wenn Sie die Umfrage an eine große Anzahl von Kontakten senden möchten, legen Sie den Standardwert für `NX_SURVEY_ILIMIT` in `NX.env` auf ein höheres Limit, z. B. 1073741824, fest.

Hinweis: Weitere Informationen zur Erstellung von verwalteten Umfragen finden Sie in der *Online-Hilfe*.

Webservices

Webservices entsprechen Datenaustauschstandards, die Folgendes ermöglichen:

- Kommunikation von Anwendungen über HTTP mit verschiedenen Servern unabhängig von der Betriebsumgebung
- Zugreifen auf die CA-Produkt-Funktionen durch die meisten Anwendungen
- Erstellen von Tickets, Aktualisieren von Assets, Durchsuchen der Knowledge Base usw. durch Webservice-Clients

Hinweis: Weitere Informationen finden Sie im *Implementierungshandbuch* unter "Verwalten von Webservices".

Kapitel 8: Konfiguration von Anwenderkonten

Dieses Kapitel enthält folgende Themen:

[Kontakte](#) (siehe Seite 337)

[Kontaktdefinitionen](#) (siehe Seite 337)

[Gruppen](#) (siehe Seite 339)

[Kontakttypen](#) (siehe Seite 340)

[Spezielle Verarbeitungs-Typen](#) (siehe Seite 341)

Kontakte

Ein wichtiger Teil der Einrichtung eines funktionierenden Service Desk ist die Definition der Benutzer, die auf den Service Desk zugreifen. In CA SDM werden Benutzer *Kontakte* genannt, und Sie können mehrere Aufgaben durchführen, um sie einzurichten und zu verwalten:

- Kontakte manuell einrichten
- Kontakte in Gruppen organisieren, die Verantwortungsbereiche definieren
- Kontakttypen einrichten, um die CA SDM-Kontakte auf der Basis ihrer Art der Nutzung des Systems in logische Gruppen zu unterteilen
- Importieren Sie LDAP-Benutzerinfo in einen CA SDM-Kontakt Datensatz.
- Weisen Sie einer Rolle einen Kontakt zu, um die aufrufbaren Systemfunktionen zu definieren.
- Weisen Sie einem Kontakt einen speziellen Verarbeitungstyp wie prominente Persönlichkeit (VIP) zu.

Kontaktdefinitionen

Jede Person, die CA SDM nutzt, muss als Kontakt definiert werden. Der Kontaktdatensatz eines Anwenders definiert die Anwenderinformationen, die das System benötigt, folgendermaßen:

Grundlegende Informationen

Definiert grundlegende Identifikationsdaten wie den Name des Anwenders und den Kontakttyp. Der Name eines Kontakts wird als primärer Kennzeichner verwendet, wenn ein Kontakt gewählt wird oder Kontaktinformationen in einem anderen Kontext eingetragen werden.

Login

Definiert Anmeldeinformationen, wie die Anwender-ID und in einigen Fällen ein PIN-Feld, das als Kennwort verwendet werden muss und den Anwender bei der Anmeldung authentifiziert. Die Anwender-ID wird verwendet, um den Anwender für Authentifizierungszwecke in der Kontakttabelle zu identifizieren und um die ihm zugewiesenen Zugriffstypen zu bestimmen. Abhängig davon, wie der Administrator die Sicherheit eingerichtet hat, kann ein anderes Feld, z. B. die Kontakt-ID, als PIN-Feld angegeben werden, und der Anwender kann diese ID als Kennwort für die Anmeldung eingeben.

Sicherheit

Definiert der Zugriffstyp, der in ihrem Kontaktdatensatz oder von einem Standard-Zugriffstyp zugewiesen wird, je nachdem, wie Sie die Sicherheit für Ihr System einrichten. Zudem kann der Zugriffstyp eines Anwenders auf der Basis der Mitgliedschaft des Anwenders in einer LDAP-Verzeichnisgruppe zugewiesen werden.

Der Zugriffstyp eines Anwenders bestimmt alle Aspekte der Sicherheit, einschließlich der Art ihrer Authentifizierung im System, welche Web-Schnittstellen sie sehen und auf welche Produktfunktionen sie zugreifen können.

Das Security Management ist eine Funktion der Web-Schnittstelle.

Diensttyp

Legt den Service Level fest, den ein Anwender erhält. Der Diensttyp eines Kontakts definiert die Dienstebene, die ein Anwender erhalten soll. Mit CA SDM-Kunden werden Service Level Agreements (SLAs) ausgehandelt, und Diensttypen dienen als Mechanismus für CA SDM zur Implementierung von SLAs. Indem Sie dem Kontaktdatensatz eines Anwenders einen Servicetyp zuweisen, können Sie garantieren, dass bei der Erstellung eines Tickets für einen als betroffener Endanwender identifizierten Anwender der Servicetyp für das Ticket mindestens dem Servicetyp des Kontakts entspricht.

Die Einrichtung von SLAs mit Hilfe von Diensttypen ist eine Funktion, die Sie als Administrator über die Web-Schnittstelle durchführen.

Automatische Zuweisung

Definiert Informationen über automatische Zuweisungen, wie zum Beispiel Schichten und Verfügbarkeit (nur für den Kontakttyp "Analyst" verwendet). Sie können Analystenkontakte einrichten, um festzulegen, ob sie für die automatische Zuweisung verfügbar sind. Die automatische Zuweisung gilt nur für Requests und wird als Teil der Definition von Request-Bereichen festgelegt. Des Weiteren wird sie mit den Gruppen verbunden, denen der Analyst angehört.

Senden von Benachrichtigungsmeldungen an Anwender

Definiert die Benachrichtigungsinformationen eines Kontakts, die folgende Angaben enthalten:

- mehrere E-Mail-Adressen und Telefonnummern für Benachrichtigungen
- zu verwendende Methode für die Benachrichtigungen mit unterschiedlichen Dringlichkeitsstufen
- Schichten, während derer Benachrichtigungen empfangen werden

In der Berechnung der Benachrichtigungsverzögerung wird die Zeitzone des Kontakts berücksichtigt. Wenn keine Zeitzone für den Kontakt festgelegt ist, wird stattdessen die Zeitzone des Servers verwendet. Wenn die Zeitzone des Servers verwendet wird, können Benachrichtigungen möglicherweise zu Zeiten ausgelöst werden, die nicht in die gängigen Arbeitszeiten fallen.

Durch organisatorische Informationen (wie zum Beispiel Lokation, Organisation und Abteilung) können Sie Kontakte auf der Basis der Organisation, der sie angehören, gruppieren. Wenn Sie zum Beispiel einen Kontakt mit einem Ort verbinden, wird der Kontakt mit einer physischen Adresse verknüpft, was auch die Bestimmung der automatischen Zuweisung unterstützt. Der Organisation kann ein Dienstyp zugewiesen werden, was es einfacher macht, SLAs nach Organisation und nicht nach einzelnen Kontakten zu verwalten.

Gruppen, denen ein Anwender angehört

Fasst Kontakte in Gruppen zusammen, die bestimmte Verantwortungsbereiche innerhalb Ihres Service Desk darstellen. Sie können Kontakte über die Web-Schnittstelle einrichten und definieren.

Gruppen

Eine Gruppe ist eine Sammlung von Kontakten, die einen gemeinsamen Verantwortungsbereich teilen. In CA SDM sind Gruppen durch den vordefinierten Kontakttyp "Gruppe" implementiert, wodurch eine Gruppe nur eine besondere Art von Kontakt ist. Eine Gruppe hat die gleichen grundlegenden Informationen wie ein Kontakt, mit der wichtigen zusätzlichen Funktion, dass Gruppen einer der Schlüssel für die automatische Zuweisung von Anforderungen sind. Sie können einer Gruppe Anforderungsbereiche, Positionen und einen Zeitplan zuweisen. Diese Attribute bestimmen, ob und wann die Kontakte in der Gruppe die automatische Zuweisung einer Anforderung annehmen können.

Hinweis: Informationen zur Definition von Gruppen finden Sie in der *Online-Hilfe*.

Kontakttypen

Kontakttypen werden verwendet, um CA SDM-Benutzer auf der Basis ihrer Art der Nutzung des Systems in logische Gruppen zu unterteilen. Zum Beispiel sind einige der vielen vom System vordefinierten Kontakttypen „Analytiker“, „Kunde“ und „Gruppe“. Diese vordefinierten Kontakttypen entsprechen den Bedürfnissen der meisten CA SDM-Implementierungen; wenn es Ihre Umstände jedoch erforderlich machen, können Sie die vordefinierten Kontakttypen ändern und Kontakttypen erstellen. Wenn Sie Benutzer als Kontakte definieren, weisen Sie jedem einen Kontakttyp zu.

Hinweis: Weitere Informationen zur Definition von Kontakttypen finden Sie in der *Online-Hilfe*.

Bestimmen des Verhaltens auf der Basis des Kontakttyps

Der *Kontakttyp* bestimmt, welche Kontakte in verschiedenen Situationen angezeigt werden (und die entsprechende Berechtigung haben). Wenn Sie zum Beispiel eine beliebige Art von Ticket, wie eine Anfrage oder ein Issue, manuell zuweisen, müssen Sie in dem Feld für den Zuständigen eine Person mit dem Kontakttyp "Analyst" angeben. Wenn Sie einen Kontakt für dieses Feld aus einer Auswahlliste auswählen, werden in der Auswahlliste nur Kontakte mit des Typs „Analytiker“ angezeigt. Wenn Sie einen Kontakt mit einem anderen Typ eingeben, wird nur das Analytikersuchfenster angezeigt.

Hinweis: Eine wichtige Funktion des Kontakttyps ist die Implementierung von Gruppen von Kontakten über den vordefinierten Kontakttyp "Gruppe".

Einrichten von Benachrichtigungen auf der Basis von Kontakttypen

Sie können Benachrichtigungen auf Kontakttyp basieren, wodurch Sie eine Benachrichtigungsmeldung an alle Kontakte eines bestimmten Typs senden können.

Weitere Informationen:

[Benachrichtigungen](#) (siehe Seite 199)

Auswählen von Kontakten auf der Basis des Kontakttyps

Sie können Benutzer in verschiedenen Kontexten auf der Basis des Kontakttyps auswählen. Zum Beispiel verfügen die meisten Listen- und Auswahlfenster, die Kontakte anzeigen, über ein Suchfeld, in dem Sie einen Kontakttyp als Suchkriterium auswählen können.

Spezielle Verarbeitungs-Typen

Sie können besondere Verarbeitungstypen definieren, die Kontakte identifizieren, die besondere Aufmerksamkeit benötigen. Sie können die besonderen Verarbeitungstypen benutzen, für CA SDM zur Verfügung stellt, oder Ihre eigenen Typen erstellen. Sie können Ticket anzeigen und lokalisieren, die einen betroffenen Endanwender angeben, welcher besondere Aufmerksamkeit benötigt. Zum Beispiel können Analysten den V.I.P. durchsuchen. im Scoreboard zur Identifizierung von Tickets durchsuchen, die einen VIP als betroffenen Endanwender angeben.

Die folgenden Beispiele sind Kontakte, die besondere Verarbeitungstypen angeben können:

- VIPs (Very Important Persons), z. B. Führungskräfte
- Kunden, für die der Support gerade erneuert wird
- Kunden mit Behinderungen, die spezielle Verarbeitungsmethoden oder Geräte erfordern
- Besucher
- Kontakte, die des Missbrauchs von Systemressourcen verdächtig sind

Wenn ein oder mehrere besondere Verarbeitungstypen einem Kontakt zugewiesen werden, zeigen Tickets, die den Kontakt im Feld "Betroffener Endanwender" ein Warnungsbanner, ein Warnsymbol oder beides an. Mit Hilfe von Ticket-Feldern und speziellen Verarbeitung-Typen können Sie Tickets verfolgen und zwischen zwei verwandten, aber möglicherweise unterschiedlichen Kontakttypen unterscheiden. Zum Beispiel hat ein VIP (Betroffener Endanwender) einen Assistenten (Requestor), der im eigenen Namen handelt. Wenn es sich bei dem betroffenen Endanwender um einen Kontakt handelt, der einem speziellen VIP-Verarbeitung-Typ zugewiesen ist, können Tickets von einem Analysten genauer priorisiert werden.

Weitere Informationen:

[Konfigurieren von Kontakten zur speziellen Verarbeitung](#) (siehe Seite 342)

[Zuordnen von Kontakten zu bestimmten Verarbeitungstypen](#) (siehe Seite 343)

[LDAP-Verzeichnis-Daten](#) (siehe Seite 344)

Konfigurieren von Kontakten zur speziellen Verarbeitung

So konfigurieren Sie Kontakte zur speziellen Verarbeitung:

1. Erstellen Sie spezielle Verarbeitungstypen.
2. [Verknüpfen Sie einen Kontakt mit einer beliebigen Anzahl spezieller Verarbeitungstypen](#) (siehe Seite 343). Genauso kann ein spezieller Verarbeitungstyp mit vielen Kontakten verknüpft sein.

Ein Kontakt, der mit einem oder mehreren speziellen Verarbeitungstypen verknüpft ist, wird im Kontaktdetailformular und im Ad-hoc-Profil-Browser mit Hilfe eines Banners am oberen Rand jeder Seite optisch unterschieden. Dieses Banner zeigt das Warnsymbol und den Alert-Text für jeden dem Kontakt zugewiesenen speziellen Verarbeitungstyp an.

Außerdem wird auf alle Tickets, die den Kontakt als betroffenen Endanwender identifizieren, wie folgt hingewiesen:

- Warnsymbole und Alert-Text werden in einem Banner am oberen Rand des Ticket-Detailformulars angezeigt.
- Warnsymbole werden in der Ticketliste angezeigt.
- Das Scoreboard enthält einen V.I.P.-Ordner und -Unterordner für jeden Ticket-Typ. Der V.I.P. enthalten Tickets für betroffene Endanwender, die VIP-Kontakte zur speziellen Verarbeitung sind.

Hinweis: Der V.I.P.-Scoreboard-Ordner wird für Analystenrollen angezeigt.

Weitere Informationen

[Zuordnen von Kontakten zu bestimmten Verarbeitungstypen](#) (siehe Seite 343)
[LDAP-Verzeichnis-Daten](#) (siehe Seite 344)

Zuordnen von Kontakten zu bestimmten Verarbeitungstypen

Sie können Kontakten einen besonderen Verarbeitungstyp zuweisen, so dass Analysten bei Tickets, die Endanwender mit besonderen Anforderungen (beispielsweise visuell beeinträchtigte Personen, Kontakte, die ein Sicherheitsrisiko darstellen, usw.) betreffen, automatisch vom System entsprechend gewarnt werden.

So ordnen Sie Kontakten einen bestimmten Verarbeitungstyp zu:

1. Wählen Sie auf der Seite "Kontakt - Detail" die Registerkarte "Besondere Verarbeitung".

In der Registerkarte "Zugeordnete besondere Verarbeitung" werden besondere Verarbeitungstypen aufgelistet, die für einen Kontakt gelten.
2. Klicken Sie auf die Schaltfläche "Besondere Verarbeitung des Kontakts aktualisieren".

Der Suchfilter wird angezeigt.
3. Suchen Sie nach dem besonderen Verarbeitungstyp, den Sie dem Kontakt zuordnen möchten.

Die Seite "Besondere Verarbeitung aktualisieren" wird angezeigt.
4. Wählen Sie in der linken Spalte einen oder mehrere Verarbeitungstypen aus und verwenden Sie die Schaltfläche zum Verschieben (>>), um die Typen in die rechte Spalte zu verschieben. Klicken Sie auf "OK".

Hinweis: Sie können eine Zuordnung zu einem Kontakt aufheben, indem Sie unter Verwendung der Schaltfläche zum Verschieben (<<) Typen aus der rechten Spalte in die linke Spalte zurückverschieben. Klicken Sie das auf Suchsymbol, um den gewünschten Wert zu suchen.

Der Verarbeitungstyp wird dem Kontakt zugeordnet.

CA SDM zeigt je nach Verarbeitungstyp Folgendes an, wenn ein Ticket den Kontakt im Feld "Betroffene Endanwender" angibt:

- Für den betroffenen Endanwender auf dem Ticket wird auf der Seite "Kontakt - Details" ein Warnbanner angezeigt.
- Der Text der Warnung wird oben auf der Ticket-Detailseite und im Schnellprofil als Banner angezeigt.
- In Ticket-Listen sind die Kontaktzeile hervorgehoben und mit einer Warnkennzeichnung versehen.
- Der Ordner V.I.P. wird im Scoreboard für Analystenrollen angezeigt. Der Ordner enthält alle Tickets, die Kontakten (betroffene Endanwender) zugeordnet sind, die über einen besonderen VIP-Verarbeitung verfügen.

LDAP-Verzeichnis-Daten

Lightweight Directory Access Protocol (LDAP) ist ein Netzwerkkommunikationsprotokoll für die Abfrage und die Änderung von Verzeichnisdiensten, die über ein TCP/IP-Netzwerk laufen. Ein LDAP-Verzeichnis ist eine Baumstruktur, die Einträge für die Verwaltung von Anwendern, Gruppen, Computern, Druckern und anderen Entitäten in einem Netzwerk enthält.

CA SDM kann so konfiguriert werden, dass auf ein LDAP-Verzeichnis zugegriffen wird, welches Ihnen erlaubt, LDAP-Daten auf verschiedene Art und Weise zu verwenden:

- Synchronisieren Sie Kontakte mit LDAP-Anwenderdatensätzen. Die Synchronisierung kann folgendermaßen geschehen:
 - **Bei Anmeldung** - Wenn ein Anwender sich am Produkt anmeldet und ein LDAP-Datensatz für diesen Anwender existiert, aber ein entsprechender Kontaktdatensatz fehlt, wird ein Kontaktdatensatz automatisch auf der Basis der LDAP-Informationen erstellt.
 - **Neuer Kontakt** - Wenn Sie einen Kontaktdatensatz manuell erstellen, können Sie einen LDAP-Datensatz auswählen und seine Attributwerte mit ihren entsprechenden Feldern im neuen Kontaktdatensatz zusammenführen.
 - **Batch-Aktualisierung** - Sie können Stapelverarbeitungsaufträge laufen lassen, um die Prozesse für den Import und die Aktualisierung von Kontaktdatensätzen mit Daten aus den entsprechenden LDAP-Datensätzen zu automatisieren.
- Hinweis:** Synchronisierung mit LDAP funktioniert nur in eine Richtung. LDAP-Daten können benutzt werden, um Kontakte zu erstellen und zu aktualisieren. Das Produkt unterstützt allerdings keine Aktualisierungen des LDAP-Verzeichnisses.

- Weisen Sie auf der Basis von LDAP-Gruppen-Mitgliedschaften CA SDM-Zugriffstypen zu.
- Implementieren Sie eine Alternativmethode zur Durchführung der CA SDM-Authentifizierung.

Die Komponente "ldap_virtb" stellt die Funktion zur LDAP-Integration auf folgenden Servern bereit, abhängig von Ihrer CA SDM-Konfiguration und unabhängig vom Betriebssystemtyp:

- Konventionell: Primärserver oder Sekundärserver.
- Erweiterte Verfügbarkeit: Hintergrundserver oder Anwendungsserver.

Hinweis: Weitere Informationen zur Komponente "ldap_virtb" finden Sie im *Implementierungshandbuch*. Die Datei "\$NX_ROOT/bopcfg/majic/ldap.maj" gibt die Zuordnung zwischen LDAP-Attributen und Kontaktdatensatzattributen an.

Wichtig! Bei CA SDM müssen LDAP-Datensätze einen Eintrag im Feld "Nachname" haben, um die LDAP-Daten zu suchen, anzuzeigen und zu importieren.

Wichtig! CA SDM unterstützt *seitenbasierte Suchvorgänge*, bei denen alle Datensätze in Ihrem LDAP-Verzeichnis durchsucht werden. Paginiertes Suchen ermöglicht Ihnen auch, neue Kontaktdatensätze zu importieren oder bestehende Kontaktdatensätze aus einer beliebigen Anzahl von LDAP-Datensätzen zu synchronisieren. Diese Möglichkeiten sind allerdings eingeschränkt, wenn Sie Sun Java System Directory Server oder Novell eDirectory verwenden, weil diese LDAP-Server keine paginierte Suche unterstützen. In diesem Fall können Sie nur die Anzahl von LDAP-Datensätzen suchen, importieren und synchronisieren, die durch NX_LDAP_MAX_FETCH angegeben wird. Weitere Informationen über seitenbasierte Suchvorgänge finden Sie in der Datei "[NX.env](#)" (siehe Seite 360)".

Konfigurieren von LDAP-Optionen

Sie können CA SDM so konfigurieren, dass der Zugriff auf LDAP-Verzeichnisdaten möglich ist.

So konfigurieren Sie CA SDM für den Zugriff auf LDAP-Verzeichnisdaten:

1. Installieren Sie manuell LDAP-Optionen, die den Optionsmanager der Web-Schnittstellen verwenden.

Hinweis: Die für eine grundlegende LDAP-Integration notwendigen Optionen sind nach Bedarf in der folgenden Tabelle in der Spalte "Beschreibung" angegeben. Die als optional gekennzeichneten Optionen sind Funktionen, die Sie nur dann hinzufügen können, wenn die obligatorischen Optionen installiert wurden. Die Werte, die Sie beim Installieren dieser Optionen angeben, werden in die Datei "\$NX_ROOT/NX.env" geschrieben. Weitere Informationen über die LDAP-Optionen und Anweisungen für ihre Installation finden Sie in der *Online-Hilfe*.

2. Starten Sie den CA SDM-Service neu.
Die Änderungen werden nun wirksam.

Option	Standardwert	Beschreibung
default_ldap_tenant		Für das Installieren von Mandantenfähigkeit erforderlich. Definiert die standardmäßige Zuweisung von Mandanten für Kontakte, die aus LDAP importiert wurden. Sie müssen die Mandanten-UUID verwenden, wenn Sie das Feld "Optionswert" ausfüllen. Hinweis: Sie können die Mandanten-UUID mit einer Datenbankabfrage abrufen. Beispiel: "SELECT * FROM ca_tenant".
ldap_enable	Ja	Erforderlich. Aktiviert LDAP-Integration in CA SDM.
ldap_host		Erforderlich. Gibt den Hostnamen oder die IP-Adresse des LDAP-Datenbankservers an.
ldap_port	389	Erforderlich. Gibt die Portnummer für den LDAP-Server an.
ldap_dn		Erforderlich. Gibt den eindeutigen Namen für die LDAP-Server-Anmeldung an. Beispiel: CN=Joe, CN=Users, DC=KLAND, DC=AD, DC=com Wenn der LDAP-Server anonyme Verbindungen unterstützt, kann dieser Wert leer sein.
ldap_pwd		Erforderlich. Gibt das Kennwort für den eindeutigen Namen der LDAP-Server-Anmeldung an. Wenn der LDAP-Server anonyme Verbindungen unterstützt, kann dieser Wert leer sein.
ldap_search_base		Erforderlich. Gibt den Startpunkt für Suchläufe in der LDAP-Schemastruktur an: (UNIX) Sie müssen einen Startcontainer angeben. Beispiel: CN=Users, DC=KLAND, DC=AD, DC=com (Windows) Sie brauchen keinen Container anzugeben. Sie können an der Spitze des Schemabaums starten. Beispiel: DC=KLAND, DC=AD, DC=com

Option	Standardwert	Beschreibung
ldap_filter_prefix	(&(objectClass=user)	Gibt das Präfix an, das beim Suchen nach LDAP-Anwendern auf einen automatisch erstellten Filter angewendet wird. Hinweis: Diese Variable wurde durch die Option "ldap_user_object_class" ersetzt. Sie ist nicht im Optionsmanager verfügbar, kann jedoch manuell in der Datei "NX.env" festgelegt werden.
ldap_filter_suffix	)	Gibt das Suffix an, das beim Suchen nach LDAP-Anwendern auf einen automatisch erstellten Filter angewendet wird. Hinweis: Diese Variable wurde durch die Option "ldap_user_object_class" ersetzt. Sie ist nicht im Optionsmanager verfügbar, kann jedoch manuell in der Datei "NX.env" festgelegt werden.
ldap_user_object_class	Person	Erforderlich. Gibt den Wert des LDAP-objectClass-Attributs an, das auf einen automatisch erzeugten Filter angewendet wird, wenn man nach LDAP-Anwendern sucht.
ldap_enable_group	Ja	Optional. Aktiviert die Zuweisung eines CA SDM-Zugriffstyps basierend auf der Mitgliedschaft zu einer LDAP-Gruppe.
ldap_group_object_class	Gruppe	Nur erforderlich, wenn "ldap_enable_group" installiert ist. Gibt den Objektnamen an, der beim Suchen nach Gruppen auf einen automatisch erstellten Filter angewendet wird.
ldap_group_filter_prefix	(&(objectClass=group)	Gibt das Präfix an, das beim Suchen nach LDAP-Anwendern auf einen automatisch erstellten Filter angewendet wird. Hinweis: Diese Variable wurde durch die Option "ldap_group_object_class" ersetzt. Sie ist nicht im Optionsmanager verfügbar, kann jedoch manuell in der Datei "NX.env" festgelegt werden.
ldap_group_filter_suffix	)	Gibt das Suffix an, das beim Suchen nach LDAP-Gruppen auf einen automatisch erstellten Filter angewendet wird. Hinweis: Diese Variable wurde durch die Option "ldap_group_object_class" ersetzt. Sie ist nicht im Optionsmanager verfügbar, kann jedoch manuell in der Datei "NX.env" festgelegt werden.
ldap_enable_auto	Ja	Optional. Aktiviert das automatische Generieren von Kontaktdatensätzen aus LDAP-Daten.

Option	Standardwert	Beschreibung
ldap_sync_on_null	Ja	Optional. Überschreibt bestehende CA SDM-Kontaktattribute mit ungültigen Daten, wenn das entsprechende LDAP-Anwenderattribut einen ungültigen Wert enthält.
ldap_service_type	Active Directory	Optional. Wählen Sie diese Option, wenn Windows als CA SDM-Betriebsumgebung verwendet wird und das LDAP-Verzeichnis <i>nicht</i> Active Directory ist (z. B. eTrust oder Novell). Hinweis: In der UNIX-Betriebsumgebung wird die Funktion "Non-AD" nur verwendet, wenn diese Option <i>nicht</i> installiert ist. Wenn sie installiert wird, wird der Servicetyp auf "Active Directory" gesetzt.
ldap_enable_tls	Nein	Optional. Gibt an, ob die Transportschichtssicherheit (Transport Layer Security, TLS) während der LDAP-Verarbeitung aktiviert ist.

Überprüfen der LDAP-Integration

Nachdem Sie die notwendigen LDAP-Optionen installiert haben, können CA SDM-Benutzer LDAP-Daten fallweise importieren. Dadurch entfällt die Notwendigkeit, alle Kontaktattributfelder manuell auszufüllen.

Um zu überprüfen, dass die LDAP-Integration richtig konfiguriert wird, führen Sie mit Hilfe der Web-Schnittstelle die unten beschriebenen Schritte durch. Informationen zur Lösung von Problemen finden Sie unter [Fehlerbehebung](#) (siehe Seite 359).

So überprüfen Sie, dass Sie LDAP-Datensätze suchen und importieren können:

1. Wählen Sie auf der Registerkarte "Service Desk" die Optionen "Datei" und dann "Neuer Kontakt" aus.

Das Fenster "LDAP-Verzeichnisse – Suche" wird angezeigt.

2. Legen Sie Filterkriterien fest, und klicken Sie auf "Suchen". Sie können beispielsweise "b%" im Feld "Nachname" eingeben, um eine Liste der LDAP-Benutzereinträge mit Nachnamen abzurufen, die mit dem Buchstaben B beginnen.

Note: Wenn Ihr LDAP-Verzeichnis Tausende von Einträgen enthält und Sie Ihre Suche nicht filtern, versucht die Anfrage, *alle* LDAP-Benutzerdatensätze zu finden. Dies kann zur Zeitüberschreitung der Anfrage und einem Zurücksetzen auf null Datensätze führen.

Mit den Filterkriterien übereinstimmende Suchergebnisse werden angezeigt.

3. Wählen Sie einen Eintrag aus.

Das Fenster "Neuen Kontakt erstellen" wird angezeigt, das die importierten LDAP-Attributwerte enthält.

4. Klicken Sie auf "Speichern".

Der Kontaktdatensatz wird erstellt.

So überprüfen Sie, dass Sie einen Kontakt mit LDAP-Daten aktualisieren können:

Hinweis: Bevor Sie dieses Verfahren durchführen, können Sie zu Testzwecken eines der verfügbaren LDAP-Bearbeitungstools verwenden, um einen oder mehrere Attributwerte des Eintrags zu ändern, den Sie in dem vorherigen Vorgang verwendet haben. Sie können überprüfen, ob der Kontakt mit den neuesten LDAP-Daten aktualisiert wurde.

1. Wählen Sie auf der Registerkarte "Service Desk" die Option "Suche" und anschließend "Kontakte".

Das Fenster "Kontakt" wird angezeigt.

2. Legen Sie Filterkriterien fest, um nach einem Kontakt zu suchen, für den ein entsprechender LDAP-Benutzereintrag vorhanden ist. Sie können beispielsweise nach dem Kontakt suchen, den Sie im vorherigen Verfahren erstellt haben.

Mit den Filterkriterien übereinstimmende Suchergebnisse werden angezeigt.

3. Wählen Sie den Kontakt aus, den Sie mit LDAP-Daten aktualisieren wollen.

Die Seite " Kontaktdetails" wird mit eingetragenen CA SDM-Kontaktinformationen angezeigt.

4. Klicken Sie auf "Bearbeiten".

Die Seite "Kontakt aktualisieren" wird angezeigt.

5. Klicken Sie auf "LDAP zusammenführen".

Die Seite "LDAP-Einträge - Liste" zeigt eine Liste mit LDAP-Benutzereinträgen an, die zu dem ausgewählten CA SDM-Kontakt gehören.

Um in dem LDAP-Verzeichnis nach anderen Einträgen zu suchen, klicken Sie auf "Filter anzeigen", legen Sie die Filterkriterien fest, und klicken sie anschließend auf "Suchen".

Hinweis: Wenn Ihr LDAP-Verzeichnis Tausende von Einträgen enthält und Sie Ihre Suche nicht filtern, versucht die Anfrage, *alle* LDAP-Benutzerdatensätze zu finden. Dies kann zur Zeitüberschreitung der Anfrage und einer Zurückgabe von null Datensätzen führen.

6. Klicken Sie auf den gewünschten LDAP-Eintrag.

Die LDAP-Detailseite zeigt die Attributwerte für den ausgewählten Eintrag an. Überprüfen Sie, dass Sie den richtigen Eintrag für den Kontakt ausgewählt haben, den Sie aktualisieren wollen. Klicken Sie dann auf "Fenster schließen".

7. Klicken Sie auf der Seite "LDAP-Einträge - Liste" mit der rechten Maustaste auf den Eintrag, der mit dem zu aktualisierenden Eintrag am meisten übereinstimmt, und klicken Sie dann auf "Zu Kontakt zusammenfügen".

Die Seite zur Kontaktaktualisierung wird erneut angezeigt, jetzt aufgefüllt mit den aktuellen LDAP-Attributwerten. Wenn die LDAP-Daten sich geändert haben, seitdem Sie den Kontakt erstellt oder zum letzten Mal aktualisiert haben, dann finden sich diese Änderungen in den Kontaktattributfeldern wieder.

Hinweis: Wenn Sie die Option "ldap_sync_on_null" installiert haben, und der LDAP-Eintrag enthält ungültige Werte für Attributfelder von Kontaktattributen, die in diesem Moment Werte enthalten, dann werden beim Speichern der Kontaktdaten die Werte in dem Kontaktdatensatz mit ungültigen Werten überschrieben.

8. Klicken Sie auf der Seite zur Aktualisierung des Kontakts auf "Speichern".
Der Kontakt wird mit den entsprechenden LDAP-Daten aktualisiert.

Automatisches Erstellen von Kontakten

Sie können CA SDM so konfigurieren, dass immer automatisch ein Kontakt aus einem entsprechenden LDAP-Benutzerdatensatz erstellt wird, wenn sich ein neuer Benutzer in CA SDM anmeldet.

Sie müssen alle obligatorischen LDAP-Optionen sowie die Option "ldap_enable_auto" installieren, um diese Funktion zu aktivieren.

Der Kontaktdatensatz wird automatisch folgendermaßen erstellt:

1. Wenn sich ein Benutzer in CA SDM anmeldet, von dem noch kein Kontaktdatensatz verfügbar ist, aber dessen Benutzerkennung in einem LDAP-Datensatz existiert, dann werden die LDAP-Daten automatisch importiert und ein Kontaktdatensatz wird erstellt.
2. Der automatisch erstellte Kontaktdatensatz erbt die Sicherheitseinstellungen des Standard-Zugriffstyps.
3. Sie können dem Kontakt dann einen speziellen Zugriffstyp zuweisen, oder der Zugriffstyp kann basierend auf der Mitgliedschaft des Benutzers in einer LDAP-Gruppe zugewiesen werden.

Dieser Prozess ist für den Benutzer vollständig transparent und wird ihm wie jede andere Anmeldungssitzung dargestellt.

Zugriffstypenzuweisungen von LDAP-Gruppen aus

Sie können CA SDM konfigurieren, um Kontakten basierend auf der LDAP-Gruppenmitgliedschaft automatisch Zugriffstypenwerte zuzuweisen. Wenn bei aktivierter automatischer Zugriffstypenzuweisung ein LDAP-Benutzerdatensatz, der für die Erstellung eines Kontakts benutzt wurde, einer LDAP-Gruppe gehört, die einem der CA SDM-Zugriffstypen zugeordnet ist, wird jener Zugriffstyp dem Kontakt automatisch zugewiesen. Andernfalls erbt der Kontakt den Standardzugriffstyp.

Um die automatische Zugriffstypenzuweisung zu aktivieren, müssen Sie die Optionen "ldap_enable_group" und "ldap_group_object_class" installieren.

Hinweis: Details zur Installation der notwendigen Optionen zum Zuordnen von LDAP-Gruppen mit Zugriffstypen finden Sie in der *Online-Hilfe*.

Batch-Import von Kontakten anhand von LDAP-Daten

Sie können das pdm_ldap_import-Befehlszeilenhilfsprogramm ausführen, um CA SDM-Kontakte im Stapelmodus anhand von LDAP-Daten zu erstellen.

Hinweis: Zusätzlich zum Erstellen von Kontakten aktualisiert bringt pdm_ldap_import existierende Kontakte auf den neuesten Stand, wenn sie nicht mit ihren entsprechenden LDAP-Einträgen synchronisiert werden. Sie können den pdm_ldap_sync-Stapelprozess benutzen, um existierende Kontakte auf den neuesten Stand zu bringen, aber nicht um neue zu erstellen.

pdm_ldap_import weist die folgende Syntax auf:

```
pdm_ldap_import -l "ldap_where_clause" [-c "contact_where_clause"] [-u "userid"]
```

-l "ldap_where_clause"

Spezifiziert die Anwender-IDs von zu durchsuchenden LDAP-Datensätzen. Zu ersetzende Variablen werden durch das Fragezeichen (?) angegeben. Zum Beispiel, für *userid = ?*. Der Standardwert ist *userid = ?*. In diesem speziellen Fall wird ID dem Kontaktattribut "ldap_dn" zugeordnet.

Hinweis: Verwenden Sie die Schlüsselwörter gemäß der Definition in der Datei *ldap.maj*. Sie können für die Suche auch die Syntax *memberOf = 'group_dn'* verwenden.

-c "contact_where_clause"

(Optional) Gibt an, wie festgelegt wird, ob der Kontaktdatensatz schon existiert. Wenn der Kontaktdatensatz nicht existiert, wird ein neuer Kontaktdatensatz eingefügt. Wenn der Kontaktdatensatz existiert und mit den gegenwärtigen LDAP-Daten nicht synchronisiert ist, wird der Kontaktdatensatz aktualisiert.

-u "userid"

(Optional) Spezifiziert die Anwenderkennung, unter der das pdm_ldap_import-Programm läuft.

Hinweis: Sie können Platzhalter mit pdm_ldap_import benutzen, um mehrere Datensätze anzugeben.

Beispiele: Batch-Importe anhand von LDAP-Daten

Dieses Beispiel importiert einen einzelnen LDAP-Datensatz für Anwender-ID jsmith11:

```
pdm_ldap_import -l "Anwender-ID = 'jsmith11'"
```

Dieses Beispiel importiert alle LDAP-Datensätze mit einer Anwender-ID, die mit dem Buchstaben C anfängt:

```
pdm_ldap_import -l "userid = 'c%'"
```

Dieses Beispiel importiert alle LDAP-Anwenderdatensätze im Verzeichnis:

```
pdm_ldap_import -l "userid = '%'"
```

Weitere Informationen:

[Batch-Aktualisierung von Kontakten anhand von LDAP-Daten](#) (siehe Seite 355)

Stapel-Import von Kontakten nach Datum und Uhrzeit

Sie können das pdm_ldap_import-Dienstprogramm konfigurieren, um LDAP-Datensätze zu importieren, die vor oder nach einem bestimmten Datum und einer bestimmten Uhrzeit erstellt wurden. Um diese Funktion zu aktivieren, erstellen Sie eine ldap.mod-Datei mit dem folgenden Inhalt:

```
OBJECT ldap {  
  ATTRIBUTES LDAP_Entry {  
    whenCreated whenCreated STRING ;  
  };  
};
```

Damit wird das *whenCreated*-Attribut zum LDAP-Objekt hinzugefügt.

Die Regeln zum Filtern von Datensätzen mit Hilfe des *whenCreated*-Attributs sehen folgendermaßen aus:

- Benutzen Sie nur den Operator ">=" oder "<=".
- Geben Sie *alle* Zeichen für den Datums-/Uhrzeit-Wert an, einschließlich des Z. Setzen Sie ein 0 an einer beliebigen Stelle, die nicht ausdrücklich angegeben werden soll (zum Beispiel, die Tageszeit).

- Setzen Sie die Datums-/Uhrzeitangabe an den Beginn des Filters; benutzen Sie keine vorangestellten Nullen am Anfang der Zeichenkette.
- Lassen Sie die vorangestellte Jahrhundertangabe weg. Um zum Beispiel das Jahr 2008 anzugeben, benutzen Sie 08.

Hinweis: der Datums-/Uhrzeit-Wert muss von einzelne Anführungszeichen umschlossen werden.

Beispiel: Verwenden des whenCreated-Attributs zum Importieren von LDAP-Einträgen

Das folgende Beispiel benutzt das whenCreated-Attribut, um nach dem 11.03.08 erstellte LDAP-Einträge zu importieren.

```
Pdm_ldap_import -l "whenCreated >= '080312000000Z'"
```

Beispiel: Verwenden des whenCreated-Attributs, um nach LDAP-Datensätzen zu suchen

Das folgende Beispiel benutzt das whenCreated-Attribut mit pdm_ldap_test, um nach LDAP-Datensätzen zu suchen, die nach dem 11.03.08 erstellt wurden.

```
pdm_ldap_test.exe -f "whenCreated>=080312000000Z" -a whenCreated
Starting ldap_test.exe...
LDAP Directory Type : active directory
Service Desk Platform : windows
Search Base : DC=kirklandsd,DC=ca,DC=com
Search Filter : (&(objectClass=person)(whenCreated>=080312000000Z))
Administrator Username :
CN=Administrator,CN=Users,DC=kirklandsd,DC=ca,DC=com
Administrator Password : *****
LDAP Host : gecko.kirklandsd.ca.com
LDAP Port : 389
LDAP API Version : 3
DN: CN=aixmail,CN=Users,DC=kirklandsd,DC=ca,DC=com
whenCreated(17)(0): 20080312035327,0Z
DN: CN=hpmail,CN=Users,DC=kirklandsd,DC=ca,DC=com
whenCreated(17)(0): 20080312035425,0Z
DN: CN=sunmail,CN=Users,DC=kirklandsd,DC=ca,DC=com
whenCreated(17)(0): 20080312035726,0Z
3 Total LDAP records found...
```

Batch-Importe - Zusammenfassung und Protokolldaten

Mit dem Befehl pdm_ldap_import kann ein detailliertes Protokoll der Aktivität zu einzelnen Ausführungen erstellt und angezeigt werden. Die Protokolldatei ("ldap_logging.0-n</cs>") befindet sich im Verzeichnis "\$NX_ROOT/log</cs>".

Nachstehend finden Sie eine Zusammenfassung, wie sie beim Aufruf von "pdm_ldap_import" an der Befehlszeile zurückgegeben wird:

```
pdm_ldap_import wird gestartet...  
pdm_ldap_import-Zusammenfassung: Verarbeitet(21) Aktualisiert(1) Keine  
Übereinstimmungen(7) Keine Änderungen(11) Mehrere Übereinstimmungen(0) Leerer  
Filter(2) Fehler(0)  
pdm_ldap_import wird beendet...
```

Die folgende Tabelle enthält eine Aufschlüsselung der Zusammenfassungsdaten:

Status	Anzahl	Beschreibung
Verarbeitet	21	Die Anzahl von CA SDM-Kontakten mit entsprechenden LDAP-Einträgen.
Aktualisiert	1	Die Anzahl an Kontaktdatensätzen, die aktualisiert wurden, weil der entsprechende LDAP-Eintrag abweichende Information enthielt
Keine Übereinstimmungen	7	Die Anzahl von CA SDM-K Kontaktdatensätzen ohne entsprechende LDAP-Einträge.
Neue Kontakte	11	Die Anzahl an neuen Kontaktdatensätzen, die auf der Basis von entsprechenden LDAP-Einträgen erstellt wurden
Mehrere Übereinstimmungen	0	Die Anzahl an LDAP-Einträgen mit mehreren übereinstimmenden Kontaktdatensätzen, wie über die Option "ldap_search_base" festgelegt
Leerer Filter	2	Die Anzahl der LDAP-Einträge, die nicht zur Generierung eines gültigen Suchfilters verwendet werden können.
Fehler	0	Gibt die LDAP-Einträge an, bei deren Verarbeitung ein Fehler aufgetreten ist. Zum Beispiel werden LDAP-Datensätze, die in einem von CA SDM benötigten Feld (wie "Nachname") keinen Wert enthalten, als Fehler angesehen und können nicht importiert werden.

Batch-Aktualisierung von Kontakten anhand von LDAP-Daten

Sie können das Dienstprogramm "pdm_ldap_sync" ausführen, um Kontaktdatensätze im Stapelmodus anhand von LDAP-Daten zu aktualisieren.

Wichtig! Dieses Dienstprogramm überschreibt den vorhandenen Mandanten des in CA SDM definierten LDAP-Kontakts. Wenn Sie den Mandantenwert beibehalten wollen, müssen Sie "NX.env" ändern, indem Sie die Variable "NX_RETAIN_TENANT_VALUE" manuell hinzufügen und auf "ja" festlegen. Wenn diese Variable auf "nein" festgelegt wird, fehlt oder nicht richtig festgelegt wird, überschreibt das Dienstprogramm die Mandanteninformationen.

Hinweis: Das Dienstprogramm "pdm_ldap_sync" synchronisiert vorhandene Kontakte mit entsprechenden LDAP-Einträgen, erstellt jedoch keine Kontakte. Zum Erstellen von Kontakten können Sie den Batch-Vorgang "pdm_ldap_import" verwenden.

"pdm_ldap_sync" weist die folgende Syntax auf:

```
pdm_ldap_sync -l "ldap_where_clause" [-c "contact_where_clause"] [-u "userid"]
```

-l "ldap_where_clause"

Bestimmt, wie nach übereinstimmenden LDAP-Datensätzen gesucht wird. Zu ersetzende Variablen werden durch das Fragezeichen (?) angegeben. Zum Beispiel ist für *userid = ?* der Standardwert *id = ?*. In diesem speziellen Fall wird ID dem Kontaktattribut „ldap_dn“ zugeordnet.

-c "contact_where_clause"

(Optional) Bestimmt, welche Kontakte bei der Suche nach übereinstimmenden LDAP-Datensätzen verwendet werden.

Standard: "ldap_dn IS NOT NULL"

-u "userid"

(Optional) Gibt die Anwender-ID an, unter der "pdm_ldap_sync" ausgeführt wird.

Hinweis: Sie können Platzhalter mit "pdm_ldap_sync" verwenden, um mehrere Datensätze anzugeben.

Beispiele:

Dieses Beispiel richtet eine Baseline von Kontaktdatensätzen ein, die einen entsprechenden LDAP-Datensatz aufweisen:

```
pdm_ldap_sync -l "userid = ?" -c ""
```

Dieses Beispiel verwendet die Standardparameter zum Aktualisieren aller Kontakte, die einen LDAP-"distinguishedName" haben:

```
pdm_ldap_sync
```

Dieses Beispiel aktualisiert einen einzelnen Kontakt:

```
pdm_ldap_sync -l "userid = ?" -c "userid = 'jsmith11'"
```

Weitere Informationen:

[Batch-Import von Kontakten anhand von LDAP-Daten](#) (siehe Seite 351)

Zusammenfassung und Protokolldaten der Stapelaktualisierung

Der Befehl "pdm_ldap_sync" pflegt ein detailliertes Protokoll aller Aktivitäten für jeden Lauf. Die Datei "ldap_logging.0-n" befindet sich im Verzeichnis \$NX_ROOT/log.

Im Folgenden finden Sie ein Beispiel der Zusammenfassungsdaten, die "pdm_ldap_sync" auf der Befehlszeile zurückgibt:

```
pdm_ldap_sync Starting...
pdm_ldap_sync Summary: Verarbeitet(21) Aktualisiert(1) Keine Übereinstimmungen(7)
Keine Änderungen(11) Mehrere Übereinstimmungen(0) Leerer Filter(2) Fehler(0)
pdm_ldap_sync Complete...
```

Die folgende Tabelle beschreibt die Zusammenfassungsdaten:

Status	Anzahl	Beschreibung
Verarbeitet	21	Die Anzahl von CA SDM-Kontakten mit entsprechenden LDAP-Einträgen
Aktualisiert	1	Die Anzahl der LDAP-Einträge, deren Informationen sich von ihren entsprechenden CA SDM-Kontakteinträgen unterscheiden
Keine Übereinstimmungen	7	Die Anzahl von CA SDM-Kontaktdatensätzen ohne entsprechende LDAP-Einträge.
Keine Änderungen	11	Die Anzahl der LDAP-Einträge, deren Informationen mit ihren entsprechenden CA SDM-Kontakteinträgen übereinstimmen
Mehrere Übereinstimmungen	0	Die Anzahl der LDAP-Einträge mit mehreren übereinstimmenden Kontaktdatensätzen in CA SDM, wie durch die ldap_search_base-Option definiert
Leerer Filter	2	Die Anzahl der LDAP-Einträge, die nicht zur Generierung eines gültigen Suchfilters verwendet werden können.
Fehler	0	Die Anzahl der LDAP-Einträge, für die ein Fehler während der Verarbeitung auftrat

LDAP-Authentifizierung

Sie können mit Hilfe von LDAP Anwender authentifizieren, die sich in CA SDM anmelden. Die DAP-Authentifizierung ist verfügbar, wenn die CA EEM-Authentifizierungskomponente in CA SDM integriert ist; sie ersetzt die vom Hostbetriebssystem durchgeführte Standardvalidierung. Die LDAP-Authentifizierung ist nur anwendbar, wenn CA EEM für die Verwendung eines externen LDAP-Verzeichnisses konfiguriert wurde und Sie für den Validierungstyp eines Anwenders in einem Zugriffstypdatensatz die Authentifizierung durch das Betriebssystem gewählt haben.

Wenn eine CA EEM-Funktion aktiviert ist, werden Anmeldeanfragen durch den CA EEM-Server geprüft. Eine Anmeldeanfrage wird nur bewilligt, wenn Folgendes eintritt:

- Die angegebene Anwender-ID stimmt mit einem CA SDM-Kontaktdatensatz überein.
- Die Anwender-ID stimmt mit einem Anwenderprofil in CA EEM überein.
- Die Kombination aus Anwender-ID und Kennwort wird von >EEM> bestätigt.

Hinweis: Weitere Informationen über das Verwenden von CA EEM für die Authentifizierung und über das Verschieben des Authentifizierungsmoduls zu externem Server finden Sie im *Implementierungshandbuch*. Weitere Informationen zum Setup des Zugriffstyps finden Sie in der *Online-Hilfe*.

Transport Layer Security

Sie können CA SDM so konfigurieren, dass während der LDAP-Verarbeitung TLS (Transport Layer Security) benutzt wird. TLS, ein sicheres Kommunikationsprotokoll, ist der Nachfolger von SSL v3 (Secure Sockets Layer). Zur Aktivierung installieren Sie die `ldap_enable_tls`-Option.

Wichtig! Wenn diese Funktion aktiviert ist, werden alle Kommunikationen zwischen CA SDM und dem LDAP-Server verschlüsselt. Wenn diese Funktion *nicht* aktiviert ist, werden alle Datenübertragungen (einschließlich des Anmeldenamens und des Kennworts des Administrators zum Zugriff auf den LDAP-Server) im Klartext übermittelt.

Hinweis: Information zur Konfiguration von TLS finden Sie auf Ihrem LDAP-Server und der Dokumentation des Betriebssystems. Informationen zur Verwendung der Option `"ldap_enable_tls"` finden Sie in der *Online-Hilfe*.

Attributzuordnung

Attributwerte von CA SDM-Kontaktdatensätzen werden basierend auf den Attributzuordnungsdefinitionen in der Datei `"$NX_ROOT/bopcfg/majic/ldap.maj"` mit Attributwerten von LDAP-Benutzern synchronisiert.

Der folgende Auszug aus "ldap.maj" illustriert eine Zuordnung. Bei den Attributnamen in der linken Spalte ("id") handelt es sich um die CA SDM-Kontaktattributnamen. Die mittlere Spalte ("distinguishedName") enthält die entsprechenden LDAP-Attributnamen.

id	distinguishedName	STRING 512;
last_name	sn,pzLastName	STRING ;
first_name	givenName,pzFirstName	STRING ;
middle_name	initials,pzMiddleName	STRING ;
userid	uid,sAMAccountName,pzUserName	STRING ;
phone_number	telephoneNumber,pzWorkPhoneNumber	STRING ;

Wenn ein SREL (eine einzelne Beziehung oder ein Fremdschlüssel in einer anderen Datenbanktabelle) auf CA SDM existiert, wird der Kontaktattributwert mit dem entsprechenden LDAP-Wert synchronisiert. Wenn der SREL nicht bereits existiert, wird er nicht automatisch während der Verarbeitung der LDAP-Synchronisierung erstellt.

Hinweis: Standardmäßig wird die Attributzuordnung für das Microsoft Active Directory-LDAP-Schema konfiguriert. Im Bedarfsfall können Sie die Zuordnung durch die Verwendung einer mod-Datei ändern.

Ändern der Attributzuordnung

Sie können die Standardattributzuordnung ändern.

Verfahren Sie wie folgt, um das Standardattribut zu ändern:

1. Navigieren Sie zu "\$NX_ROOT/site/mods/majic", und öffnen Sie die mod-Datei.
2. Verwenden Sie die MODIFY-Anweisungen in der mod-Datei wie folgt.
 - Die MODIFY-Anweisungen müssen in der Datei immer am Anfang stehen.
 - Im Anschluss an die MODIFY-Anweisungen sollten beliebige zusätzliche Felder, die nicht in der Datei "ldap.maj" enthalten sind, mit der Syntax im folgenden Beispiel angegeben werden.
 - Wenn Sie ein Feld definieren, das ein Bindestrichzeichen im Attributnamen enthält, müssen Sie den Namen in einfache Anführungszeichen setzen. Andernfalls bewirkt das Attribut beim Erstellen der mod-Datei einen Syntaxfehler. Zum Beispiel muss der folgende Attributname in einzelne Anführungszeichen eingeschlossen werden:

```
c_nx_string1-'swsd-sicherheitsfrage' STRING ;
```

3. Speichern und schließen Sie die mod-Datei.
4. Starten Sie den CA SDM-Service neu.

Wichtig! Die Web-Engine wird nicht gestartet, wenn es eine Diskrepanz in der Syntax oder bei der Groß-/Kleinschreibung gibt.

Ihre Änderungen treten in Kraft.

Beispiel: Verwenden von MODIFY-Anweisungen

Das folgende Beispiel veranschaulicht, wie zwei Felder geändert und ein zusätzliches Feld hinzugefügt wird.

```
//
// Map CA SDM userid attribute to ADAM Userid
//
MODIFY ldap userid cn ;
MODIFY ldap middle_name middleName ;
OBJECT ldap LDAP {
ATTRIBUTES LDAP_Entry{
contact_num employeeNumber STRING ;
};
} ;
```

Fehlerbehebung

Bei der Behandlung von Problemen der Kommunikation mit LDAP-Servern ist zu berücksichtigen, dass es selten zwei vollständig identische LDAP-Implementierungen gibt. CA SDM-Dienstprogramme können überprüfen, ob die LDAP-Integration ordnungsgemäß funktioniert.

Hinweis: CA SDM wird nur für die Integration in Microsoft-Active-Directory, eTrust, und iPlanet vorkonfiguriert. Die Integration mit anderen LDAP-Servern erfordert oft Änderungen und Anpassungen auf beiden Seiten.

Anzeigen des Status von Daemons oder Prozessen

Der ldap_virtldb-Prozess verwaltet Interaktionen zwischen CA SDM und der virtuellen LDAP-Datenbank.

So zeigen Sie den Status aller Daemons (UNIX) oder Prozesse von CA SDM an:

1. Führen Sie "pdm_status" in der Befehlszeile ohne Parameter aus:

```
pdm_status
```

"pdm_status" zeigt den Status aller Daemons (UNIX) oder Prozesse (Windows) von CA SDM auf dem System an, auf dem der Befehl ausgeführt wird, z. B.:

```
DAEMON                                STATUS      HOST        PID    SLUMP CONNECT TIME
-----
--
Agent anthill Running anthill 455 Tue Feb 17 17:55:12
Ddict_rd (ddictrd) Completed anthill
Data Dictionary (ddictbuild) Completed anthill
...
User Validation (boplgin) Running anthill 456 Tue Feb 17 17:55:21
```

2. Prüfen Sie die Befehlsausgabe für den Status des Prozesses "ldap_virtldb".

slstat-Befehl

Führen Sie den folgenden Befehl ohne Parameter aus, um zu überprüfen, ob eine Verbindung zu bopLDAP besteht:

```
slstat
```

Prüfen Sie die Befehlsausgabe, um den Status von bopLDAP zu sehen.

Datei "NX.env"

Prüfen Sie die Datei "\$NX_ROOT/NX.env", ob die grundlegenden LDAP-Optionen korrekt installiert sind.

Je nachdem, welche LDAP-Optionen installiert werden, sollte die Datei "NX.env" Zeilen enthalten, ungefähr folgendermaßen aussehen:

```
@NX_LDAP_DN=quser
@NX_LDAP_ENABLE=Yes
@NX_LDAP_ENABLE_AUTO=Yes
@NX_LDAP_HOST=myserver
@NX_LDAP_PORT=389
@NX_LDAP_PWD=OBUNQXo7CmgbThZLCiMKIwJlA3UXdVNA0jUpHjstfDt2LBIDPgwTWA==
@NX_LDAP_SEARCH_BASE=dc=mycontroller, dc=xyz, dc=com
@NX_LDAP_SERVICE_TYPE=Active Directory
@NX_LDAP_SYNC_ON_NULL=Yes
@NX_LDAP_USER_OBJECT_CLASS=person
```

Wichtig! Weil der Sun Java System Directory Server-Server und die Novell-eDirectory-Server das paging-basierte Suchen nicht unterstützen, sind die LDAP-Suche, der LDAP-Import und die LDAP-Synchronisierung auf den Wert von NX_LDAP_MAX_FETCH Datensätzen pro Ausführung beschränkt. Der Standardwert lautet 100. Wenn Sie einen dieser LDAP-Server benutzen, möchten Sie vielleicht NX_LDAP_MAX_FETCH zu Ihrer Datei "NX.env" hinzufügen, um die größtmögliche Anzahl von LDAP-Datensätzen anzugeben. Sie können NX_LDAP_MAX_FETCH auf einen beliebigen Wert unter dem Wert von LDAP_SIZELIMIT_EXCEEDED oder LDAP_ADMINLIMIT_EXCEEDED auf Ihrem LDAP-Server festlegen.

Weitere Informationen:

[Konfigurieren von LDAP-Optionen](#) (siehe Seite 345)

pdm_ldap_test

Benutzen Sie das `pdm_ldap_test`-Befehlszeilenhilfsprogramm, um die Verbindung mit einem LDAP-Verzeichnis zu testen, um sicherzustellen, dass die Suchoptionen richtig konfiguriert sind, und um die TLS-Konfiguration zu testen.

Standardmäßig verwendet `pdm_ldap_test` die Parametereinstellungen, die in die `$NX_ROOT/NX.env`-Datei eingegeben werden, wenn Sie LDAP-Optionen installieren, bearbeiten oder deinstallieren. Um die Standardvorgaben zu überschreiben, können Sie Parameter in der `pdm_ldap_test`-Befehlszeile angeben.

Um die verfügbaren Parameter für diesen Befehl zu sehen, geben Sie folgenden Befehl ein:

```
pdm_ldap_test -h
```

Wichtig! Bei UNIX muss der `LIBPATH` vor der Ausführung mehrerer CA SDM-Dienstprogramme festgelegt werden. Verwenden Sie `pdm_task`, um den `LIBPATH` vor der Ausführung eines Dienstprogramms festzulegen. Geben Sie zum Beispiel "`pdm_task pdm_clean_attachments ...`" ein.

Prüfen der Verbindung zum LDAP-Server

Um die Verbindung mit dem LDAP-Server zu überprüfen, führen Sie `pdm_ldap_test` ohne Parameter aus:

```
pdm_ldap_test
```

Erfolgreiche Verbindung zum LDAP-Server

Wenn die Verbindung erfolgreich ist, erhalten eine Ausgabe, die der folgenden ähnelt:

```
Starting pdm_ldap_test...
LDAP service type=active directory
Service Desk platform=windows
Using search base=DC=mycontroller,DC=xyz,DC=com
Using filter=(&(objectCategory=person))
ldap_init(myserver.mycontroller.xyz.com,389): (Success)
ldap_bind_s(Administrator) (Erfolg)
LDAP API Verion 3
```

Fehlgeschlagene Verbindung: Serverausfall oder falscher Name/Port

Wenn die Verbindung fehlschlägt, weil der Server ausgefallen ist oder Sie einen falschen LDAP-Servernamen oder Port angegeben haben, erhalten Sie eine Ausgabe, die der folgenden ähnelt:

```
Starting pdm_ldap_test...
LDAP service type=active directory
Service Desk platform=windows
Using search base=DC=mycontroller,DC=xyz,DC=com
Using filter=(&(objectCategory=person))
ldap_init(junk,389): (Success)
ldap_bind_s(Administrator) (Server Down)
```

Fehlgeschlagene Verbindung: LDAP_DN oder LDAP_PWD ungültig

Wenn die Verbindung fehlschlägt, weil Sie LDAP_DN oder LDAP_PWD nicht korrekt angegeben haben, erhalten Sie eine Ausgabe, die der folgenden ähnelt:

```
Starting pdm_ldap_test...
LDAP service type=active directory
Service Desk platform=windows
Using search base=DC=mycontroller,DC=xyz,DC=com
Using filter=(&(objectCategory=person))
ldap_init(myserver.mycontroller.xyz.com,389): (Success)
ldap_bind_s(junk) (No Such Object or Invalid Credentials)
```

Anzeigen von Suchparametern

Um zu überprüfen, ob die Suchparameter richtig konfiguriert sind, lassen Sie pdm_ldap_test ohne Parameter laufen:

```
pdm_ldap_test
```

Erfolgreiche Suche

Wenn Ihre Suche erfolgreich ist, erhalten Sie eine Ausgabe, die der folgenden ähnelt:

```
DN: CN=John A. Smith,CN=Users,DC=COMPUTERTEST
    c(2)(0): US
    displayName(14)(0): John A. Smith
    mail(14)(0): account02@mycompany.com
    givenName(4)(0): John
    initials(1)(0): a
    distinguishedName(38)(0): CN=John a.

Smith,CN=Users,DC=COMPUTERTEST
    objectGUID(3)(0): 314738
    pager(12)(0): ###-111-1111
    postalCode(5)(0): 11111
    SAMAccountName(7)(0): account02
    sn(6)(0): Smith
    telephoneNumber(12)(0): ###-342-6265
    userPrincipalName(16)(0): account02@COMPUTERTEST
```

```

DN: CN=Mike Johnson,CN=Users,DC=COMPUTERTEST
    displayName(10)(0): Mike Johnson
    givenName(4)(0): Mike
    distinguishedName(34)(0): CN=Mike

Johnson,CN=Users,DC=COMPUTERTEST
    objectGUID(12)(0): 312328
    SAMAccountName(7)(0): account03
    sn(5)(0): Johnson
    userPrincipalName(16)(0): account03@COMPUTERTEST

```

Fehlgeschlagene Suche: SEARCH_BASE ungültig

Wenn die Suche aufgrund einer ungültigen SEARCH_BASE fehlschlägt, erhalten Sie eine Ausgabe, die der folgenden ähnelt:

```

Starting pdm_ldap_test...
LDAP service type=edirectory
Service Desk platform=windows
Using search base=o=SmartLabsx
Using filter=(&(objectClass=InetOrgPerson)
ldap_init(155.35.173.110,15389): (Success)

ldap_bind_s() (Success)
LDAP API Verion 3
ldap_search_st() (No Such Object or Referral)

```

Fehlgeschlagene Suche: SIZELIMIT_EXCEEDED, TIMEOUT

Die Suche kann mit einer SIZELIMIT_EXCEEDED- oder TIMEOUT-Meldung fehlschlagen, wenn Sie einen Filter angeben, der die Suche nicht ausreichend einschränkt. Die meisten LDAP-Server begrenzen die Größe der von einer Suchanfrage zurückgegebenen Ergebnismenge. Wenn Sie diese Grenze überschreiten, erhalten Sie eine SIZELIMIT_EXCEEDED-Meldung. Wenn Ihre Suchanfrage länger als die Standardzeitüberschreitung von 20 Sekunden dauert, beendet der LDAP-Server Ihre Anfrage aufgrund der Zeitüberschreitung, und Sie erhalten eine TIMEOUT-Fehlermeldung, die der folgenden ähnelt:

```

Starting pdm_ldap_test...
LDAP service type=edirectory
Service Desk platform=windows
Using search base=o=SmartLabsx
Using filter=(&(objectClass=InetOrgPerson)
ldap_init(155.35.173.110,15389): (Success)
ldap_bind_s() (Success)
LDAP API Verion 3
ldap_search_st() (TIMEOUT or SIZELIMIT_EXCEEDED)

```

Fehlgeschlagene Suche: 0 Datensätze zurückgegeben

Die Suche kann fehlschlagen, weil Ihr Standardfilter nicht korrekt ist. Wenn `ldap_test` null (0) Datensätze zurückgibt, prüfen Sie stets die "Using filter"-Zeile. Diese ist der Basisfilter, der von `LDAP_FILTER_PREFIX` und `LDAP_FILTER_SUFFIX` oder den `LDAP_OBJECT_CLASS`-Optionen generiert wird:

```
Starting pdm_ldap_test...
LDAP service type=edirectory
Service Desk platform=windows
Using search base=o=SmartLabs
Using filter=(&(objectClass=InetOrgPerson)
ldap_init(155.35.173.110,15389): (Success)
ldap_bind_s() (Success)
LDAP API Verion 3
ldap_search_st() 0 records
```

Einschränken der Suche

Benutzen Sie den Parameter `-f` mit dem `pdm_ldap_test`-Befehl, um einen Filter anzugeben, der zum Grundfilter zur Einengung der Suchkriterien hinzugefügt wird. Sie müssen im Filter die entsprechende LDAP-Syntax und die LDAP-Schemaattributnamen verwenden. Setzen Sie den Filter immer in Anführungszeichen und verwenden Sie Klammern, um die Reihenfolge der Operatoren anzugeben.

Verwenden Sie zum Beispiel den folgenden Befehl, um nach allen Datensätzen zu suchen, für die `sn=Account_10001`:

```
pdm_ldap_test -f "(sn=Account_10001)"
```

Das `pdm_ldap_test`-Dienstprogramm unterstützt die folgenden Gleichheits-Operator:

Gleichheits-Operator	Beschreibung
=	ist gleich
<=	kleiner oder gleich
>=	größer oder gleich
~=	gleich

Das `pdm_ldap_test`-Dienstprogramm stützt die folgenden Booleschen Operatoren:

Boolescher Operator	Beschreibung
&	AND
	ODER
!	NOT

Die Operatoren AND und OR wirken sich auf jedes Klammernpaar () im Suchfilter aus. Der Operator NOT wirkt sich nur auf das Klammernpaar aus. Diese Operatoren gehen den Suchfiltern immer *voraus*, um auf diese und nicht zwischen ihnen angewandt zu werden. Sie können auch auf eine beliebige Anzahl von Filtern angewandt werden, wie in den folgenden Beispielen gezeigt:

```
"(&(sn=Brown)(initials=A)) "
```

```
"(|(sn=Brown)(sn=Smith))"
```

```
"(!sn=Brown)"
```

Bestimmen der Attributnamen, die Werte haben

Benutzen Sie den Parameter -a "*" und den Parameter -f mit dem Befehl `pdm_ldap_test`, um zu entscheiden, welche Attribute für LDAP-Benutzer- oder Gruppen-Datensätze definiert werden. Diese Prüfung ist nützlich, um zu bestimmen, ob LDAP-Attribute vorhanden sind, die Kontaktattributen zugeordnet werden sollen. Außerdem können Sie damit prüfen, ob ein bestimmtes Attribut einen Wert hat und verfügbar sein soll, wenn Kontaktdatensätze erstellt oder aktualisiert werden.

Das folgende Beispiel zeigt die Ausgabe aus einem iPlanet-Verzeichnis:

```
pdm_ldap_test -a "*" -f sn=Account_1000001
```

```
2 LDAP records found...
```

```
DN: cn=Account_1000001,ou=200K_Plus,o=SmartLabs
    sn(15)(0): Account_1000001
    objectClass(13)(0): inetOrgPerson
    objectClass(20)(1): organizationalPerson
    objectClass(6)(2): Person
    objectClass(18)(3): ndsLoginProperties
    objectClass(3)(4): Top
```

```
DN: cn=Account_1000001,ou=2_Plus,o=SmartLabs
    mail(28)(0): ThisIsTheMailingAddressField
    uid(13)(0): Login_1000001
    givenName(17)(0): GivenNameOfPerson
    sn(15)(0): Account_1000001
    objectClass(13)(0): inetOrgPerson
    objectClass(20)(1): organizationalPerson
    objectClass(6)(2): Person
    objectClass(18)(3): ndsLoginProperties
    objectClass(3)(4): Top
```

Das folgende Beispiel zeigt die Ausgabe aus Active Directory:

```
Ldap_test -a "*" -f (&(sn=Brown)(initials=A))"
```

1 LDAP records found...

```
DN: CN=John A. Smith,CN=Users,DC=mycontroller,DC=xyz,DC=com
  objectClass(3)(0): top
  objectClass(6)(1): person
  objectClass(20)(2): organizationalPerson
  objectClass(4)(3): user
  cn(16)(0): John A. Smith
  sn(5)(0): Brown
  givenName(7)(0): John
  initials(1)(0): A
  distinguishedName(55)(0): CN=John A.
  Smith,CN=Users,DC=mycontroller,DC=xyz,DC=com
  displayName(16)(0): John A. Smith
  memberOf(52)(0): CN=Domain Admins,CN=Users,DC=mycontroller,DC=xyz,DC=com
  sAMAccountName(7)(0): smijo04
  userPrincipalName(25)(0): smijo04@mydomain.xyz.com
  objectCategory(63)(0):
  CN=Person,CN=Schema,CN=Configuration,DC=mycontroller,DC=xyz,DC=com
```

Einschalten der LDAP-Verfolgung

Mit dem Dienstprogramm "pdm_logstat" können Sie die Ablaufprotokollierung einschalten, um die Verwendung von LDAP innerhalb von CA SDM zu überwachen.

Die Syntax für den Befehl "pdm_logstat" lautet:

```
pdm_logstat -f ldap_virtldb.c 1000
```

Die folgenden stdlog-Meldungen helfen Ihnen, den Status des Verbindungsprozesses zu verstehen.

Bestimmen, ob der Prozess "ldap_virtldb" gestartet wurde

Die erste zu betrachtende Zeile beim Analysieren der stdlogs für LDAP-Meldungen ist der Start des Prozesses "ldap_virtldb". Die LDAP-Fähigkeit von CA SDM beginnt nur, wenn dieser Prozess gestartet wird.

Hinweis: Selbst wenn keine LDAP-Integrationsoptionen installiert oder eingerichtet sind, wird dieser Prozess weiterhin ausgeführt.

```
06/03 17:00:18.27 cpasd1 bopLDAP 1964 SIGNIFICANT ldap_virtldb.c
```

```
680 STARTUP of LDAP_virtldb
```

Bestimmen, ob alle erforderlichen Optionen installiert sind

Wenn eine der erforderlichen LDAP-Optionen nicht definiert wurde, zeigt stdlog die fehlenden Optionen wie folgt an:

```
06/03 17:00:18.72 cpasdl bopLDAP 1964 SEVERE_ERROR ldap_virtddb.c 1023 LDAP Server
port id missing
06/03 17:00:18.78 cpasdl bopLDAP 1964 SEVERE_ERROR ldap_virtddb.c 1023 LDAP Server
distinguished name missing
06/03 17:00:18.78 cpasdl bopLDAP 1964 SEVERE_ERROR ldap_virtddb.c 1023 LDAP Server
distinguished name password missing
```

Bestimmen, ob die LDAP-Verbindung erfolgreich ist

Sie können bestimmen, ob die LDAP-Verbindung erfolgreich ist, indem Sie die Einträge in stdlog prüfen. Aus den Einträgen sollte hervorgehen, dass eine Verbindung mit dem LDAP-Server erfolgreich hergestellt wurde (siehe folgendes Beispiel):

```
06/05 12:35:10.41 cpasdl bopLDAP 1912 SIGNIFICANT ldap_virtddb.c 958 LDAP_SRVR
connecting to host(Francisco.us.danconia.net) port(389)
06/05 12:35:11.01 frisco bopLDAP 1912 SIGNIFICANT ldap_virtddb.c 1002 LDAP_SRVR
binding with username(simon)
```

Bestimmen, ob die LDAP-Verbindung nicht verfügbar ist

Wenn aus irgendeinem Grund keine Verbindung zum LDAP-Server hergestellt werden kann, sind *LDAP-Einträge*, die *Zusammenführung von LDAP* oder andere LDAP-Funktionen nicht verfügbar, und es werden keine Ergebnisse zurückgegeben. In solchen Fällen enthält stdlog ähnliche Meldungen wie die folgenden, wenn Sie auf eine dieser Operationen zugreifen:

```
06/03 17:00:32.25 cpasdl bopLDAP 1964 SIGNIFICANT ldap_virtddb.c 219 LDAP server
not available; 'register_producer' not processed
06/05 10:52:57.63 cpasdl bopLDAP 1896 SIGNIFICANT ldap_virtddb.c 219 LDAP server
not available; 'select_full' not processed
06/05 10:52:57.66 cpasdl web:local 1868 ERROR sel_data_cache. 611 Error in ldap
Select_Cache method got_initial_count: LDAP server not available; 'select_full' not
processed
06/05 10:52:57.66 cpasdl bopLDAP 1896 SIGNIFICANT ldap_virtddb.c 219 LDAP server
not available; 'select_cancel' not processed
```

Bestimmen des tatsächlich verwendeten Filters

CA SDM ruft Datensätze aus dem LDAP-Verzeichnis gemäß der Suchbasis und des Filters ab, die im Optionsmanager definiert wurden, sowie der Suchkriterien, die vom Benutzer eingegeben werden. Prüfen Sie die folgende Meldung, um den in der Suchanforderung tatsächlich generierte Filter zu bestimmen:

```
06/24 14:18:28,32 mcxxx04- bopLDAP 3844 TRACE ldap_virtddb.c 853 Starting select
full: base=DC=kirklandsd,DC=ca,DC=com;
filter=(&(objectCategory=person)(|(sn=Jones)(pZLastName=Jones)));
attributes=(uid,sAMAccountName,pZUserName,distinguishedName)
```

Bestimmen der abgerufenen Attribute

CA SDM ruft Datensätze aus dem LDAP-Verzeichnis gemäß der Suchbasis und des Filters ab, die im Optionsmanager definiert wurden. Prüfen Sie die folgende Meldung, um zu bestimmen, ob die in "ldap.maj</cs>" und "ldap_group.maj</cs>" definierte SEARCH_BASE und Attributzuordnung korrekt ist:

```
06/24 14:18:28,39 mcxxx04- bopLDAP      3844 TRACE    ldap_virtddb.c   766 Starting
select short: base=CN=John D. Jones,CN=Users,DC=kirklandsd,DC=ca,DC=com;
filter=(&(objectCategory=person));
attributes=(modifyTimestamp,sn,pzLastName,givenName,pzFirstName,initials,pzMiddle
Name,uid,sAMAccountName,pzUserName,telephoneNumber,pzWorkPhoneNumber,mobile,pzMob
ilePhoneNumber,department,pzDepartment,facsimileTelephoneNumber,pzFaxPhoneNumber,
pager,mail,pzEmailAddress,streetAddress,pzAddress,l,pzCity,st,pzState,postalCode,
pzPostalCode,c,pzCountry,o,memberOf)
```

Bestimmen der verfügbaren und nicht verfügbaren LDAP-Daten

Angenommen, CA SDM konnte eine erfolgreiche Zuordnung zum ID-Attribut des LDAP-Objekts vornehmen, dann werden die in \$NX_ROOT/bopcfg/majic/ldap.maj definierten Attribute für jeden Eintrag abgerufen, oder es wird eine Meldung protokolliert, die angibt, dass ein Attribut nicht definiert wurde. Es folgt ein Beispiel für solche Meldungen:

```
06/24 14:18:28.41 mclda04- bopLDAP      3844 TRACE    ldap_virtddb.c   1396 Value not
available for 'modifyTimestamp'
```

```
06/24 14:18:28.41 mclda04- bopLDAP      3844 TRACE    ldap_virtddb.c   1396 Value not
available for 'telephoneNumber,pzWorkPhoneNumber'
```

Kapitel 9: Verwalten von Rollen

Hinweis: Weitere Informationen über andere Aspekte der Web-Schnittstelle finden Sie unter Konfigurieren der Web-Schnittstelle.

Dieses Kapitel enthält folgende Themen:

[Rollen](#) (siehe Seite 369)

[Vordefinierte Rollen](#) (siehe Seite 369)

[Role-Based Sicherheit](#) (siehe Seite 371)

[Rollenbasierte Navigation](#) (siehe Seite 381)

[Implementieren einer benutzerdefinierten Menüstruktur](#) (siehe Seite 390)

[Implementieren einer anwenderspezifischen Menüstruktur](#) (siehe Seite 392)

[Erstellen von Rollendatensätzen](#) (siehe Seite 393)

[Erstellen von Registerkartendatensätzen](#) (siehe Seite 394)

[Erstellen von Menüleistendatensätzen](#) (siehe Seite 395)

[Erstellen von Webformular-Datensätzen](#) (siehe Seite 396)

[Kopieren von Menüstrukturen](#) (siehe Seite 397)

[Erstellen und Anpassen von Menüstrukturen](#) (siehe Seite 398)

[Erstellen und Veröffentlichen von Helpsets](#) (siehe Seite 400)

[Wechseln von Rollen](#) (siehe Seite 401)

Rollen

Rollen sind die primären Datensätze, die die CA SDM-Sicherheit und Benutzeroberflächennavigation steuern. Jede Rolle definiert eine Detailansicht des Systems und zeigt nur die Funktionen an, die Anwender zum Ausführen der Aufgaben benötigen, die ihnen Rolle in der Geschäftsorganisation zugewiesen wurden.

Die Standardrolle eines Benutzers bestimmt die Systemansicht, die dem Benutzer nach der Anmeldung angezeigt wird. Benutzer mit mehreren Rollenzuweisungen können von einer Rolle auf andere umschalten, um unterschiedliche Ansichten des Systems zu sehen, ohne sich abmelden und wieder anmelden zu müssen.

Vordefinierte Rollen

Sie können die vordefinierten Rollen in ihrer Standardkonfiguration verwenden, sie entsprechend Ihrer Geschäftsanfrage ändern oder neue Rollen erstellen.

Die folgende Tabelle beschreibt die vordefinierten, mit CA SDM installierten Rollen. Diese Rollen wurden so konzipiert, dass sie mit den Best Practices von ITIL v3 konform sind und so die am Standort erforderliche Anpassung reduzieren, die Ihre IT-Organisation zum Einhalten der ITIL-Standards durchführen muss.

CA SDM unterstützt nur ITIL; außerdem orientiert sich die CA SDM-Dokumentation an ITIL. Weitere Informationen finden Sie unter [ITIL-Konfiguration](#) (siehe Seite 64).

Rollentyp	Rollenname	Beschreibung
Endbenutzer	Konfigurations-Viewer	Führt grundlegende CI Anzeige- und Nachforschungsaufgaben von innerhalb Ihrer Organisation durch.
	Kunde	Führt grundlegende Self-Service-Aufgaben von außerhalb Ihrer Organisation durch.
	Mitarbeiter	Führt grundlegende Self-Service-Aufgaben von innerhalb Ihrer Organisation durch.
Analyst	Konfigurationsanalyst	Führt Aufgaben innerhalb des Lebenszyklus von Configuration Items und Second-Level-CMDB-Support innerhalb Ihrer Organisation durch.
	Kundendienstmitarbeiter	Bietet Support bei organisationsfremden Benutzern, meist Kunden.
	Knowledge-Analyst	Führt Aufgaben innerhalb des Knowledge-Management-Lebenszyklus durch.
	Level 1-Analyst	Bietet First-Level-Support innerhalb Ihrer Organisation.
	Level 2-Analyst	Bietet Second-Level-Support innerhalb Ihrer Organisation, bei dem fortgeschrittenere inhaltliche Sachkenntnisse notwendig sind.
	Support-Automatisierung-Analyst	Bietet First-Level-Support innerhalb Ihrer Live Assistance-Umgebung.
	Analyst des Lieferanten	Bietet Support für ein eingegrenztes Segment Ihrer IT-Umgebung von außerhalb Ihrer Organisation, wie anbieterspezifische Hardware.
Manager	Change Manager	Verwaltet den Change-Prozess, aber in der Regel nicht die Analysten, die Change-Tickets bearbeiten.
	Kundenservicemanager	Verwaltet Kundendienstmitarbeiter und den externen Support-Prozess.
	Incident Manager	Verwaltet den Incident-Prozess, aber in der Regel nicht die Analysten, Incident-Tickets bearbeiten.
	Knowledge-Manager	Beaufsichtigt Knowledge-Analysten, Knowledge-Dokument-Neuzuordnungen und Eskalationen und die alltägliche Knowledge-Administration.
	Problem Manager	Verwaltet den Problemprozess, aber in der Regel nicht die Analysten, die an Problem-Tickets arbeiten.

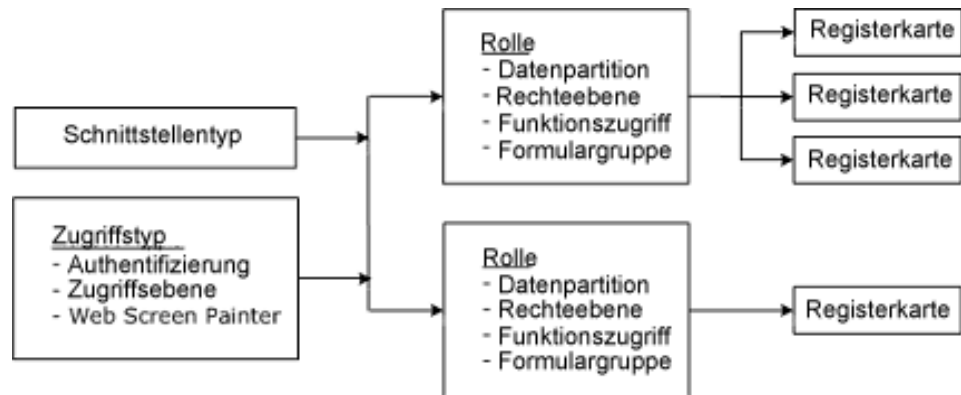
Rollentyp	Rollenname	Beschreibung
Administratoren	CA Service Desk-Manager	Ist für Eskalationen zuständig und beaufsichtigt Level-1-Analysten. Kann auch globale Service-Desk-Operationen verwalten.
	Administrator	Führt administrative Aufgaben während der CA SDM- und Knowledge Management-Implementierung durch. Typischerweise installiert, konfiguriert und integriert diese Rolle die Produkte.
	Konfigurationsadministrator	Führt administrative Aufgaben durch, die mit Ihrer CA CMDB-Implementierung in Verbindung stehen. Diese Rolle verwaltet typischerweise die CMDB- und Configuration-Item-Infrastruktur und Datenstrukturen.
	Knowledge Management-Administrator	Konfiguriert und überwacht Knowledge-Management-Einstellungen.
	Service Desk-Administrator	Führt administrative Aufgaben durch, die mit Daten und Prozessen zusammenhängen, wie beispielsweise das Erstellen und Aktualisieren von Kategorien, Kontakten, Servicetypen, Ursachen und so weiter.
	Support-Automatisierung-Administrator	Führt administrative Aufgaben durch, die mit Ihrer Support-Automatisierung-Umgebung zusammenhängen, wie beispielsweise die Konfiguration von Warteschlangen und Analytiker-Tool-Berechtigungen.
	Systemadministrator	Führt administrative Aufgaben durch, die mit Ihrer CA SDM-Implementierung, -Konfiguration und -Anpassung zusammenhängen, wie beispielsweise das Festlegen von Optionen, das Konfigurieren von Integrationen und die Anpassung von Webformularen.
	Mandantenadministrator	Führt administrative Aufgaben durch, die mit der Mandantenfähigkeit zusammenhängen; diese gelten nur für einen bestimmten Mandanten oder eine Support-Organisation.

Role-Based Sicherheit

Zugriffstypen und Rollen sind die ersten Komponenten, die Sie benutzen, um die CA SDM-Sicherheit zu steuern.

Das folgende Diagramm zeigt eine Übersicht davon, wie Rollen mit anderen Systemobjekten in gegenseitiger Beziehung stehen, um für rollenbasierte Sicherheit zu sorgen.

Hinweis: Weitere Informationen zu weiteren Sicherheitsaspekten finden Sie unter [Sicherheit](#) (siehe Seite 297).



Funktionsweise von Zugriffstypen

Jeder Zugriffstyp für einen Anwender steuert die folgenden Aspekte des Systemverhaltens:

- CA SDM-Web-Authentifizierung beim Einloggen eines Benutzers
- die Zugriffsebene für den Benutzer
- ob der Benutzer Webformulare oder das Datenbankschema mit Web Screen Painter ändern kann
- verfügbare Rollen für den Benutzer

Sie können einen Zugriffstyp mit einem Kontakt verbinden, indem Sie den Zugriffstyp auswählen, während Sie den Kontaktdatensatz erstellen oder aktualisieren.

Die folgende Tabelle listet die vordefinierten Zugriffstypen auf, gibt ihre verknüpften Rollen an und zeigt eine kurze Beschreibung.

Zugriffstyp	Verknüpfte Rollen	Beschreibung
Administration	■ Administrator (Standard) ■ Konfigurationsadministrator ■ Mitarbeiter ■ Level 2-Analyst ■ Service Desk-Administrator ■ Systemadministrator ■ Mandantenadministrator	Bietet die höchste Sicherheitsstufe bei Zugriffen auf alle wichtigen Administratorrollen. Wird während der Implementierung und danach in der Verwaltung benutzt. Hinweis: Der Zugriffstyp "Administration" wird vorkonfiguriert, um Administratoren zu gestatten, auf alle der verknüpften Rollen umzuschalten. Um zum Beispiel eine unterschiedliche Ansicht des Systems anzuzeigen, können Administratoren auf die Mitarbeiter-Rolle umschalten, ohne sich aus- und wieder einloggen zu müssen.
Kunde	■ Kunde	Verschafft sehr beschränkten Zugriff auf <i>externe</i> Kunden, die die Ansicht "Self-Service" verwenden.
Mitarbeiter	■ Mitarbeiter	Verschafft sehr beschränkten Zugriff auf <i>interne</i> Mitarbeiter, die die Ansicht "Self-Service" verwenden. Wird benutzt, um Incident-Seiten neu zu erstellen und zu aktualisieren.
IT-Personal	■ Konfigurationsanalyst ■ Mitarbeiter ■ Level 2-Analyst (Standard) ■ Knowledge-Analyst ■ Knowledge Management-Administrator ■ Knowledge-Manager	Verschafft Analysten-orientierten Zugriff auf Benutzer, die innerhalb Ihrer IT-Organisation arbeiten aber nicht Mitglieder des Support-Teams sind. Dieser Zugriff besteht speziell für Benutzer, die auf Knowledge Management zugreifen müssen.

Zugriffstyp	Verknüpfte Rollen	Beschreibung
Knowledge Management	■ Konfigurationsadministrator ■ Konfigurationsanalyst ■ Konfigurations-Viewer ■ Mitarbeiter ■ Knowledge-Analyst ■ Knowledge Management-Administrator (Standard) ■ Knowledge-Manager ■ Level 2-Analyst	Verschafft administrativen Zugriff für Benutzer, die Knowledge Management-Merkmale verwalten.
Prozess-Management	■ Change Manager ■ Konfigurationsanalyst ■ Mitarbeiter ■ Incident Manager (Standard) ■ Level 2-Analyst ■ Problem Manager ■ CA Service Desk-Manager	Verschafft Zugriff für Benutzer, die wichtige Rollen im Prozessmanagement haben.
Unicenter Service Desk Management	■ Kundenservicemanager ■ Konfigurationsanalyst ■ Mitarbeiter ■ Level 1-Analyst ■ Level 2-Analyst ■ Service Desk-Manager (Standard)	Bietet angepassten Zugriff für Benutzer, die für die Verwaltung der IT-Supportfunktionen oder der externen Kundenservicefunktionen zuständig sind (in der Regel Supervisor des First-Level-Supports).
Service Desk-Mitarbeiter	■ Konfigurationsanalyst ■ Konfigurations-Viewer ■ Kundendienstmitarbeiter ■ Mitarbeiter ■ Level 1-Analyst (Standard) ■ Level 2-Analyst	Verschafft Zugriff für Benutzer, die Support-Aufgaben erfüllen. Der Zugriff besteht speziell für solche Benutzer, die First-Level Support ausführen.
Support-Automatisierung-Admin	■ Support-Automatisierung-Administrator	Verschafft Zugriff für Benutzer, die Support-Automatisierung-Verwaltung ausführen.

Zugriffstyp	Verknüpfte Rollen	Beschreibung
Support-Automatisierung-Analyst	Support-Automatisierung-Analyst	Verschafft Zugriff für Benutzer, die Live-Unterstützung für Endbenutzer ausführen.
Mitarbeiter des Lieferanten	Analyst des Lieferanten	Verschafft sehr beschränkten Zugriff für externe Anbieter, die nur mit Elementen arbeiten, die direkt ihr Produkt betreffen (z. B. eine besondere Hardwaremarke).

Rollendatensätze

Sie können Rollen einem Zugriffstyp oder direkt einem Benutzerkontaktdatensatz zuweisen. Wenn eine Rollenzuweisungskonflikt auftritt, haben die Kontaktrollenzuweisungen Vorrang.

Jeder Rollendatensatz muss mit den folgenden Komponenten konfiguriert werden:

- Eine Formulargruppe
- Ein Web-Schnittstellentyp
- Funktionszugriffs-Einstellungen
- Ein oder mehrere Registerkarten
- Ein Helpset

Folgende optionale Komponenten können ebenfalls zu jeder Rollendefinition beitragen:

- Menüstrukturen
- Scoreboards
- Menüleisten
- Symbolleisten
- Eine Datenpartition
- Zugriff auf Knowledge Management
- Support-Automatisierung-Zugriffsebenen
- Berichts-Webformulare
- Los: Ressourcen

Funktionale Zugriffsbereiche

Funktionelle Zugriffsbereiche definieren den Zugriff auf Ticket-Datensätze und andere Systemkomponenten auf Rollenebene. Die `usp_functional_access_type`-Tabelle definiert den Bereich, und die `usp_functional_access_level`-Tabellen beschreiben den Anwenderzugriff.

Die folgende Tabelle zeigt die standardmäßigen funktionellen Zugriffsebenen:

Name	Codename	Neu
Administration	admin	Nein
Incident/Problem/Request	call_mgr	Nein
Change	change_mgr	Nein
Inventar	inventory	Nein
Issue	issue_mgr	Nein
Knowledge-Dokument	kd	Nein
Benachrichtigung	notify	Nein
Referenz	Referenz	Nein
Sicherheit	security	Nein
Ankündigung	Ankündigung	Ja
Incident-/Problem-/Request-Referenz	call_mgr_reference	Ja
Incident-/Problem-/Request-Vorlage	call_mgr_template	Ja
Change-Vorlage	change_mgr_template	Ja
Change-Referenz	change_reference	Ja
Configuration Item	ci	Ja
Configuration Item-Gemeinsamkeit Readonly	ci_common_ro	Ja
Configuration Item-Referenz	ci_reference	Ja
Kontakt	Kontakt	Ja
Gruppe	Gruppe	Ja
Issue-Vorlage	issue_mgr_template	Ja
Issue-Referenz	issue_reference	Ja
Standort	Standort	Ja
Verwaltung für mehrere Standorte	multisite_admin	Ja
Referenz für mehrere Standorte	multisite_reference	Ja

Benachrichtigungsreferenz	notification_reference	Ja
Organisation	organization	Ja
Priorisierung	Priorisierung	Ja
Service-Ebene	service_level	Ja
Site	Standort	Ja
Gespeicherte Abfrage	stored_queries	Ja
Support-Automatisierung	sa	Ja
Survey	Umfrage	Ja
Mandanten-Admin	tenant_admin	Ja
Zeitzone	timezone	Ja
Workflow-Referenz	workflow_reference	Ja
Schicht	Schichten	Ja

Hinzufügen eines funktionalen Zugriffsbereichs

Wenn Sie einen funktionalen Zugriffsbereich hinzufügen, verfügen die existierenden Rollen automatisch über den Zugriff "Ändern". Sie können die Zugriffsebenen überprüfen und ändern, um die geeignete Autorisierung zu gewähren.

So fügen Sie einen funktionalen Zugriffsbereich hinzu:

1. Wählen Sie auf der Registerkarte "Administration" die Option "Sicherheits- und Rollenmanagement" > "Funktionszugriff" aus.
2. Klicken Sie auf "Neu erstellen".
Die Seite "Neuen Funktionszugriff erstellen" wird angezeigt.
3. Füllen Sie die Felder des funktionalen Zugriffsbereichs nach Bedarf aus.
4. Klicken Sie auf "Speichern".
Die Seite "Funktionaler Zugriff – Detail" wird geöffnet.
5. Weisen Sie [einer](#) (siehe Seite 379) oder [mehreren](#) (siehe Seite 378) Rollen Zugriffsebenen zu.

Hinweis: Ausführliche Informationen zu funktionalen Zugriffsbereichen finden Sie in der *Online-Hilfe*.

Anwenden von Zugriffsebenen auf mehrere Rollen

Bei funktionalen Zugriffsbereichen können Sie die Zugriffsebenen für Rollen festlegen, und auf diese Weise Zugriffsberechtigungen mit geringem Zeitaufwand implementieren. An Stelle des Rollenmanagement aktualisieren Sie den funktionalen Zugriffsbereich mit geeigneten Rollenzugriffsebenen.

So wenden Sie Zugriffsebenen auf mehrere Rollen an:

1. Wählen Sie auf der Registerkarte "Administration" die Option "Sicherheits- und Rollenmanagement" > "Funktionszugriff" aus.
2. Klicken Sie den Namen des Funktionsbereichs.
3. Klicken Sie auf der Registerkarte "Rollen" auf "In Liste bearbeiten".
4. Überprüfen Sie und aktualisieren Sie die Rolle wie gewünscht. Die folgenden Zugriffsebenen sind verfügbar:

Keine

Verweigert der Rolle den Zugriff auf das Funktionsobjekt.

Ansicht

Gewährt dem Funktionsobjekt Lesezugriff.

Ändern

Gewährt dem Funktionsobjekt Lese-/Schreibzugriff.

5. Wählen Sie bei Bedarf weitere Rollen und Zugriffsebenen aus.
6. (Optional) Klicken Sie auf "Alle ändern".
7. Klicken Sie auf "Speichern".

Die Änderungen für die Rollen gelten sofort.

Hinweis: Information zu Rollen und funktionale Zugriffsebenen finden Sie in der *Online-Hilfe*.

Beispiel: Ändern der Einstiegsebenen für die Ankündigung

In diesem Beispiel wird gezeigt, wie Sie die Rollenzugriffsebenen für den funktionalen Zugriffsbereich "Ankündigung" ändern können.

1. Wählen Sie auf der Registerkarte "Administration" die Option "Sicherheits- und Rollenmanagement" > "Funktionszugriff" aus.
Die Seite "Funktionaler Zugriff – Detail" wird geöffnet.
2. Klicken Sie auf "Ankündigung".
3. Klicken Sie auf der Registerkarte "Rollen" auf "In Liste bearbeiten".

4. Wählen Sie die Option "Level 2-Analyst".
5. Wählen Sie unter "Zugriffsebene" die Option "Anzeigen".
Die Zugriffsebene für die Rolle "Level 2-Analyst" wird mit dem Wert "Anzeigen" hervorgehoben.
6. Wählen Sie die Option "Konfigurationsanalyst".
7. Wählen Sie unter "Zugriffsebene" die Option "Anzeigen".
Die Zugriffsebene für den Konfigurationsanalysten wird mit dem Wert "Ändern" hervorgehoben.
8. Klicken Sie auf "Speichern".
Die Änderung wird mit einer Meldung bestätigt.
9. Melden Sie sich mit der Rolle "Level 2-Analyst" an.
10. Wählen Sie "Ankündigungen anzeigen".
Die Seite "Ankündigungen" wird angezeigt.
11. Klicken Sie auf eine Ankündigung.
Es wird eine Meldung angezeigt, dass Sie mit der Rolle "Level 2-Analyst" lediglich über die Berechtigung verfügen, Ankündigungen anzuzeigen.
12. Legen Sie für die Option "Rolle" den Wert "Konfigurationsanalysten" fest.
13. Wählen Sie "Ankündigungen anzeigen".
Die Seite "Ankündigungen" wird angezeigt.
14. Klicken Sie auf eine Ankündigung.
Die Seite "Ankündigung aktualisieren" wird angezeigt. Als ein Konfigurationsanalyst können Sie Ankündigungen ändern.

Anwenden von Zugriffsebenen auf Rollen

Sie können mit dem Rollenmanagement ändern, wie Benutzer auf die Benutzerschnittstelle zugreifen. Wenn Sie die Zugriffsebenen für eine Rolle ändern, werden in der Benutzerschnittstelle nur die Objekte, Seiten und Menüelemente der jeweiligen Zugriffsebene angezeigt. Kann z. B. eine Rolle keine Kontakte mehr einrichten, wird im Menü "Datei" die Option für neue Kontakte nicht angezeigt.

Gehen Sie folgendermaßen vor, um eine Zugriffsebene auf eine Rolle anzuwenden:

1. Wählen Sie auf der Registerkarte "Administration" die Optionen "Sicherheits- und Rollenmanagement" > "Rollenmanagement" > "Rollenliste" aus.
2. Klicken Sie in der Rollenliste mit der rechten Maustaste auf den Rollennamen, und wählen Sie im Kontextmenü "Bearbeiten" aus.

3. Klicken Sie auf der Registerkarte "Funktionszugriff" auf "In Liste bearbeiten".
4. Klicken Sie auf einen Funktionsnamen.
Die Zeile wird hervorgehoben.
5. Aktualisieren Sie die funktionellen Zugriffsbereiche nach Bedarf mit den folgenden Zugriffsebenen:

Keine

Verweigert der Rolle den Zugriff auf das Funktionsobjekt.

Ansicht

Gewährt dem Funktionsobjekt Lesezugriff.

Ändern

Gewährt dem Funktionsobjekt Lese-/Schreibzugriff.

6. Klicken Sie auf "Speichern".
Die Änderung wird mit einer Meldung bestätigt. Die Rolle kann den funktionalen Zugriffsbereich auf der angegebenen Zugriffsebene sofort verwenden.
7. Überprüfen Sie die Zugriffsebene, indem Sie sich mit der Rolle anmelden und sich die Menüs, Seitenoptionen und Schaltflächen ansehen.

Beispiel: Gewähren der Rolle "Level 2-Analyst" zum Ändern des Ticketzugriffs

Dieses Beispiel zeigt, wie sich die Benutzerschnittstelle verändert, wenn Sie den Zugriff "Level 2-Analyst" zur Änderung von Tickets gewähren.

1. Wählen Sie auf der Registerkarte "Administration" die Optionen "Sicherheits- und Rollenmanagement" > "Rollenmanagement" > "Rollenliste" aus.
Die Rollenliste wird angezeigt.
2. Klicken Sie mit der rechten Maustaste auf "Level 2-Analyst", und wählen Sie im Kontextmenü die Option "Bearbeiten" aus.
3. Klicken Sie auf der Registerkarte "Funktionszugriff" auf "In Liste bearbeiten".
4. Wählen Sie "Incident-/Problem-/Anfragereferenz" aus.
5. Wählen Sie "Ändern" auf der Zugriffsebene aus.
Die Zugriffsebene wird auf "Ändern" aktualisiert.
6. Klicken Sie "Speichern", und melden Sie sich ab.
Die Änderung wird mit einer Meldung bestätigt.
7. Melden Sie sich mit der Rolle "Level 2-Analyst" an.
8. Wählen Sie "Suchen" > "Incidents" aus.

9. Klicken Sie auf "Suchen", und öffnen Sie einen Incident.

Die Seite "Incident - Detail" weist die Schaltfläche "In Liste bearbeiten" auf. Als Level 2-Analyst können Sie das Ticket ändern.

Datenaufteilungen

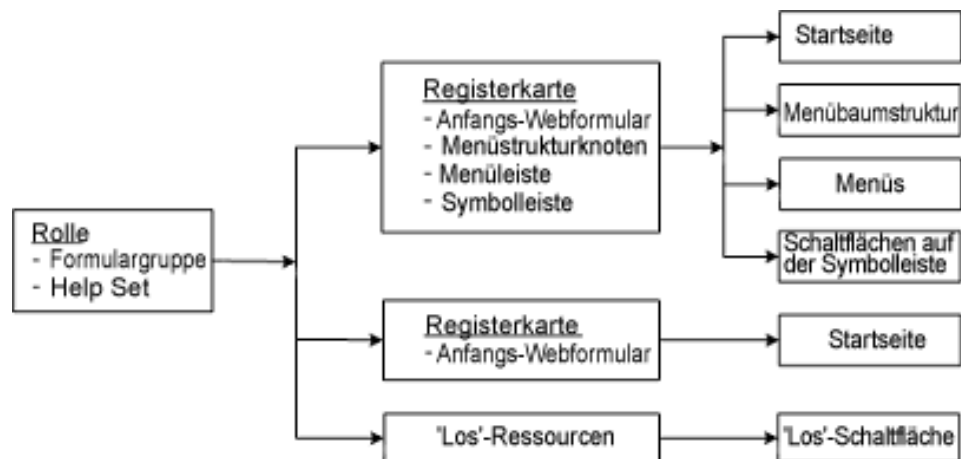
Datenpartitionen sind Untermengen der CA SDM-Datenbank, mit denen Sie den Zugriff auf Datensatzebene steuern können. Sie können eine Datenpartition mit einer Rolle verknüpfen und so den Zugriff auf Tickets und andere Datensätze steuern, die über die Web-Schnittstelle zugänglich sind.

Weitere Informationen zum Arbeiten mit Datenpartitionen finden Sie unter [Datenpartitionszuordnungen](#) (siehe Seite 315).

Rollenbasierte Navigation

Die Ansicht jedes Anwenders der Web-Schnittstelle wird von einer Rolle definiert. Anwender mit mehreren Rollenzuweisungen können auf mehrere Web-Schnittstellen-Ansichten umschalten.

Das folgende Diagramm zeigt, wie Rollen mit anderen Objekten interagieren, um eine rollenbasierte Darstellung der Benutzeroberfläche zu erzeugen.



Registerkarten

Eine Registerkarte ist eine grafische Anzeigeeinheit, die eine Rolle mit den aktuellen Funktionen des Benutzers dieser Rolle verknüpft. Wenn sich ein Benutzer am System anmeldet, werden im Hauptfenster die Registerkarten angezeigt, die der Standardrolle des Benutzers zugewiesen wurden.

Registerkarten definieren die wichtigsten Teilbereiche im Hauptfenster der Web-Schnittstellen. Jede Registerkarte ist so konfiguriert, dass sie einen geeigneten Satz an Benutzeroberflächenfunktionen für die Rolle oder die Rollen bereitstellt, von denen sie verwendet wird.

Alle Rollen müssen mindestens eine Registerkarte haben. Sie können eine oder mehrere Registerkarten mit einer Rolle verknüpfen. Jede Registerkarte hat eine Sequenznummer, die die Anzeigereihenfolge im Hauptfenster steuert. Wenn nur eine Registerkarte mit einer Rolle verknüpft ist, wird nicht die Registerkarte, sondern die Startseite der Registerkarte angezeigt.

Sie können Registerkarten so konfigurieren, dass sie die folgenden Arten von Anzeigefunktionen enthalten:

- Eine Startseite (Standardwebformular), die angezeigt wird, wenn ein Benutzer die Registerkarte auswählt. Die Startseite ist für alle Registerkarten erforderlich. Sie können jeder Registerkarte nur eine Startseite zuweisen.

Hinweis: Sie können eine Startseite so konfigurieren, dass grafische Berichte aus Business Object angezeigt werden, so dass die Benutzer Berichte während der Laufzeit generieren können. Weitere Informationen finden Sie unter [CA Business Intelligence-Berichterstellung](#) (siehe Seite 881).

- Eine Menüleiste, die Dropdown-Listen der Befehle anzeigt, wie z. B. Datei-, Anzeige- und Suchbefehle. Die Menüleiste ist optional. Sie können jeder Registerkarte nur eine Menüleiste zuweisen.
- Eine Symbolleiste, die Tool-Schaltflächen für den einfachen Zugriff auf gebräuchliche Menübefehle enthält. Diese Symbolleiste ist optional.

CA SDM bietet mehrere vordefinierte Registerkarten. Sie können die vordefinierten Registerkarten einer Rolle zuweisen oder ändern sowie anwenderspezifische Registerkarten erstellen.

Wichtig! Weisen Sie nicht mehr Registerkarten zu, als Ihr Browserfenster anzeigen kann; andernfalls reichen Registerkarten mit höheren Sequenznummern über den sichtbaren Anzeigebereich des Fensters hinaus und werden für den Benutzer unerreichbar.

Wichtig! Wählen Sie nur Registerkarten mit Formularen aus, die der Formulargruppe der Rolle angehören, die Sie erstellen oder bearbeiten. Weisen Sie zum Beispiel der Administratorrolle nicht die Registerkarte "Kunde" oder "Mitarbeiter" zu; andernfalls kommt es zu einem Fehler, wenn Benutzer versuchen, auf diese Registerkarte zuzugreifen. Die Formulargruppe der Rolle ist auf der Seite "Rolle - Detail" im Feld "Anpassung der Formulargruppe" angegeben und wird auch auf der Seite "Rolle - Liste" in der Spalte "Formulargruppe" angezeigt. Eine Liste mit den Webformularen in jeder Formulargruppe finden Sie unter [Formulargruppen](#) (siehe Seite 1257).

Vordefinierte Registerkarten

Die folgende Tabelle zeigt die vordefinierten Registerkarten, die jeder Rolle zugewiesen wird. Die Registerkarten sind in Sequenznummerreihenfolge aufgelistet, wobei die Position von links nach rechts im Fenster angegeben wird.

Hinweis: In vielen Fällen gibt es mehrere Version von Registerkarten mit demselben Anzeigenamen. Die Registerkarte "Service Desk" bietet für die Administratorrolle beispielsweise den vollen Zugriff auf die CA SDM-Funktionen, während sich die Registerkarte "Service Desk" für die Change Manager-Rolle stärker auf Changes konzentriert.

Rolle	Registerkarten
Administrator	■ Registerkarte "Service Desk" mit vollständigem Menü und Scoreboard ■ Registerkarte "Knowledge" ■ Registerkarte "Administration" mit vollständiger Menüstruktur ■ Registerkarte "Berichte" - Administrator ■ Registerkarte "Change-Kalender" ■ CA CMDB-Registerkarte ■ Support-Automatisierung-Registerkarte
Change Manager	■ Registerkarte "Berichte" - Change Manager ■ Registerkarte "Service Desk" - Change Manager ■ Registerkarte "Change-Kalender"
Konfigurationsadministrator	■ CA CMDB-Registerkarte ■ Registerkarte "Administration" – Konfigurationsadministrator
Konfigurationsanalyst	■ CA CMDB-Scoreboard - Konfigurationsanalyst
Konfigurations-Viewer	■ CA CMDB-Scoreboard - Konfigurations-Viewer
Kunde	■ Registerkarte "Kunde"
Kundenservicemanager	■ Registerkarte "Service Desk" - Kundenservicemanager ■ Registerkarte "Knowledge" ■ Registerkarte "Berichte" - Kundenservicemanager
Kundendienstmitarbeiter	■ Registerkarte "Service Desk" - Kundenservicemitarbeiter ■ Registerkarte "Schnellprofil" ■ Registerkarte "Knowledge"
Mitarbeiter	■ Registerkarte "Mitarbeiter"

Rolle	Registerkarten
Incident Manager	■ Registerkarte "Berichte" - Incident Manager ■ Registerkarte "Service Desk" - Incident Manager ■ Registerkarte "Knowledge"
Knowledge-Analyst	■ Registerkarte "Service Desk" - Knowledge-Analyst ■ Registerkarte "Knowledge" ■ Knowledge Management-Ablaufplan ■ Registerkarte "Knowledge-Berichtskarte" ■ Registerkarte "Berichte - Knowledge-Analyst"
Knowledge-Manager	■ Registerkarte "Service Desk" - Knowledge Manager ■ Registerkarte "Knowledge" ■ Knowledge Management-Ablaufplan ■ Registerkarte "Administration" - Knowledge Manager ■ Registerkarte "Knowledge-Berichtskarte" ■ Registerkarte "Berichte" - Knowledge Manager
Knowledge Management-Administrator	■ Registerkarte "Administration" - Knowledge-Administrator
Level 1-Analyst	■ Registerkarte "Service Desk" - Analyst auf Ebene 1 ■ Registerkarte "Schnellprofil" ■ Registerkarte "Knowledge"
Level 2-Analyst	■ Registerkarte "Service Desk" - Analyst auf Ebene 2 ■ Registerkarte "Knowledge" ■ Registerkarte "Change-Kalender"
Problem Manager	■ Registerkarte "Berichte" - Problem Manager ■ Registerkarte "Service Desk" - Problem Manager ■ Registerkarte "Knowledge"
Service Desk-Administrator	■ Registerkarte "Administration" - Service Desk-Administrator
CA Service Desk-Manager	■ Registerkarte "Berichte" - Service Desk-Manager ■ Registerkarte "Service Desk" - Service Desk-Manager ■ Registerkarte "Knowledge" ■ Registerkarte "Change-Kalender"

Rolle	Registerkarten
Support-Automatisierung-Administrator	■ Registerkarte "Service Desk" - Analyst auf Ebene 1 ■ Support-Automatisierung-Registerkarte ■ Support-Automatisierung-Admin ■ Registerkarte "Schnellprofil" ■ Registerkarte "Knowledge"
Support-Automatisierung-Analyst	■ Registerkarte "Service Desk" - Analyst auf Ebene 1 ■ Support-Automatisierung-Registerkarte ■ Registerkarte "Schnellprofil" ■ Registerkarte "Knowledge"
Systemadministrator	■ Registerkarte "Administration" - Systemadministrator
Mandantenadministrator	■ Registerkarte "Administration" - Mandantenadministrator
Analyst des Lieferanten	■ Registerkarte "Service Desk" - Anbieteranalyst

Webformulare

Webformulare definieren die Seiten, die in der CA SDM-Web-Schnittstelle erscheinen.

Es gibt vier Webformulartypen:

- Business-Objekt-Berichts-URL
- Seite "HTML"
- GO Ressource
- Benutzerdefiniert (zum Beispiel, eine URL für eine fremde Webseite)

Informationen zur Erstellung von benutzerdefinierten Webformularen finden Sie unter [Webformular-Datensätze erstellen](#) (siehe Seite 396).

Formulargruppen

Formulargruppen definieren die Seitensätze in der CA SDM-Web-Schnittstelle, die für eine Rolle verfügbar sind. Jede Rolle besitzt eine Formulargruppe. Anwender können nur die Webseiten anzeigen, die in der ihrer Rolle zugewiesenen Formulargruppe enthalten sind.

Jeder Schnittstellentyp hat eine zugeordnete Formulargruppe, einen Satz HTML-Dateien, die die Seiten definieren, welche Benutzer mit diesem Schnittstellentyp sehen können.

CA SDM stellt folgende vordefinierte Formulargruppen bereit:

- Analyst
- Kunde
- Mitarbeiter
- ITIL

Sie können die vordefinierten Formulargruppen in ihrer Standardkonfiguration benutzen, die vordefinierten Formulargruppen ändern, und neue Formulargruppen mit Hilfe von Web Screen Painter erstellen. Sie können eine Auflistung der HTML-Dateinamen anzeigen, die in jeder vordefinierten [Formulargruppe](#) (siehe Seite 1257) enthalten sind.

Menüstrukturen

Menüstrukturen sind die hierarchischen Listen der Knoten (Menüstrukturressourcen), die im Navigations-Fensterbereich auf der linken Seite des Hauptfensters der Web-Schnittstelle angezeigt werden.

Eine Rolle kann eine Menüstruktur haben, die Knoten für den Zugriff auf viele Funktionsbereiche des Systems zur Verfügung stellt. Zum Beispiel hat die vordefinierte Administratorrolle eine Menüstruktur, die Knoten zu den System- und Rollenmanagement-Verwaltungsfunktionen, den Service-Desk-Verwaltungsfunktionen und vielen anderen beinhaltet.

Für Rollen, die eine Menüstruktur umfassen, bietet die Menüstruktur Zugriff auf einen spezifischen Satz von Ressourcen, die Zugriff auf Funktionsbereich des Systems bieten.

CA SDM stellt vordefinierte Menüstrukturen für die folgenden Rollen zur Verfügung:

- Administrator (admin_tree)
- CA CMDB-Administrator (cmdb_adm_tree)
- Knowledge Management-Administrator (kt_adm_tree)
- Knowledge Manager ("kt_mgr_tree")
- Support-Automatisierung-Administrator (sa_admin_tree)
- Service Desk-Administrator (sd_adm_tree)
- Systemadministrator (sys_adm_tree)
- Mandantenadministrator (tn_admin_tree)

Sie können die Felder "Name", "Datensatzstatus", und "Beschreibung" der vordefinierten Menüstruktursätze bearbeiten. Es ist aber nicht möglich, sie durch Hinzufügen oder Entfernen der Menüstrukturressourcen anzupassen.

Um eine anwenderspezifische Menüstruktur zu erstellen, können Sie einen neuen Menüstruktur-Datensatz anlegen oder eine der vordefinierten Menüstrukturen kopieren und anpassen.

Hinweis: Das unveränderliche Feld "Intern" jedes Menüstruktur-Datensatzes gibt an, ob die Menüstruktur angepasst werden kann. Wird in diesem Feld "JA" angezeigt, bedeutet dies, dass es sich um eine vordefinierte Menüstruktur handelt, die nicht angepasst werden kann. "NEIN" bedeutet, dass es sich um eine standortdefinierte Menüstruktur handelt, die angepasst werden kann. Die Schaltfläche "Menü anpassen" wird in Menüstrukturdetail-Datensätzen nur angezeigt, wenn der Wert des Feldes "Intern" "NEIN" lautet.

Wenn Sie eine Menüstruktur an eine Registerkarte anhängen, wird sie für alle Rollen, die Zugriff auf diese Registerkarte haben, verfügbar.

Menüstrukturressourcen

Menüstrukturressourcen definieren die Elemente, auf die Benutzer von der Menüstruktur aus zugreifen können.

Eine Menüstrukturressource besteht aus einem Namen, einer Beschreibung und einem URL-Fragment oder dem HTML-Dateinamen, der von einer Web-Engine verwendet wird, welche die angezeigte Webseite steuert.

Menüleisten

Eine Menüleiste ist ein Anwenderschnittstellenelement, das eine horizontale Liste von Menüs im Hauptfenster der Web-Schnittstelle zeigt. Jedes Menü enthält eine Dropdown-Liste mit Optionen oder Befehlen. Sie können benutzerdefinierte Menüleisten für beliebige benutzerdefinierte Rollen definieren, die Sie erstellen.

Menüleisten-Datensätze geben das HTML-Formular an, welches die Menüelemente steuert, auf die die Menüleiste zugreifen kann.

Hinweis: Um die Funktionen der Menüleiste zu definieren, müssen Sie die Web Screen Painter-Anwendung verwenden. Informationen zum Konfigurieren der Funktionen einer vordefinierten oder benutzerdefinierten Menüleiste finden Sie in der *Web Screen Painter-Online-Hilfe*.

Die folgende Tabelle listet die vordefinierten Menüleisten auf und bezeichnet die vordefinierten Registerkarten, die sie verwenden.

Menüleiste	Zugeordnete Registerkarten
Administration	■ Registerkarte "Administration" – Konfigurationsadministrator ■ Registerkarte "Administration" - Knowledge-Administrator ■ Registerkarte "Administration" - Knowledge Manager ■ Registerkarte "Administration" - Service Desk-Administrator ■ Registerkarte "Administration" - Systemadministrator ■ Registerkarte "Administration" - Mandantenadministrator ■ Registerkarte "Administration" mit vollständiger Menüstruktur
CA CMDB	■ Registerkarte CA CMDB mit vollständigem Menü und Scoreboard
Change-Kalender	■ Registerkarte "Change-Kalender"
Wissen	■ Registerkarte "Knowledge" ■ Knowledge Management-Ablaufplan
Service Desk	■ Registerkarte "Service Desk" mit vollständigem Menü und Scoreboard
Service Desk-Change Manager	■ Registerkarte "Service Desk" - Change Manager
Service Desk-Kundenservicemanager	■ Registerkarte "Service Desk" - Kundenservicemanager
Service Desk-Kundenservicemitarbeiter	■ Registerkarte "Service Desk" - Kundenservicemitarbeiter
Service Desk-Incident Manager	■ Registerkarte "Service Desk" - Incident Manager
Service Desk-Knowledge-Analyst	■ Registerkarte "Service Desk" - Knowledge-Analyst
Service Desk-Knowledge Manager	■ Registerkarte "Service Desk" - Knowledge Manager
Service Desk-Analyst auf Ebene 1	■ Registerkarte "Service Desk" - Analyst auf Ebene 1
Service Desk-Analyst auf Ebene 2	■ Registerkarte "Service Desk" - Analyst auf Ebene 2
Service Desk-Problem Manager	■ Registerkarte "Service Desk" - Problem Manager
Service Desk-Service Desk-Manager	■ Registerkarte "Service Desk" - Service Desk-Manager
Service Desk-Anbieteranalyst	■ Registerkarte "Service Desk" - Anbieteranalyst
Support-Automatisierung-Analyst	■ Support-Automatisierung-Registerkarte - Support-Automatisierung-Analyst

Symbolleisten

Werkzeugleisten erweitern die Funktionalität von Menüleisten durch Hinzufügen der Möglichkeit, eine oder mehrere Symbolschaltflächen rechts neben den Menüs anzuzeigen.

Symbolschaltflächen werden als Symbole auf der Symbolleiste angezeigt. Durch Klicken auf eine Symbolschaltfläche hat der Benutzer einfachen Zugriff auf häufig benutzte Menüoptionen oder Befehle.

Hinweis: Sie benutzen die Web-Screen Painter-Anwendung, um die Funktionalität der Symbolleiste zu definieren. Informationen zum Konfigurieren der Funktionen einer vordefinierten oder benutzerdefinierten Symbolleiste finden Sie in der *Web Screen Painter-Online-Hilfe*.

'Los'-Ressourcen

Mit der Schaltfläche *Los* können Sie auf einfache Weise einen bestimmten Datensatz auffinden.

"Los"-Ressourcen sind eine Art Webformular. Falls eine Rolle verknüpfte "Los"-Ressourcen besitzt, erscheint beim Anmelden eines Benutzers mit dieser Rolle die "Los"-Schaltfläche rechts oben im CA SDM-Hauptfenster und in allen Pop-up-Fenstern. Die "Los"-Schaltfläche besitzt zwei zugeordnete Bereiche in der Benutzeroberfläche:

- Eine Dropdown-Liste zum Auswählen des Typs für den gesuchten Datensatz (z. B. Change)
- Ein Textfeld zum Eingeben eines Werts, mit dem ein bestimmter Datensatz ermittelt werden soll (z. B. "135", um den Change 135 zu suchen)

Durch Zuweisen von "Los"-Ressourcen zu einer Rolle können Sie die Arten von Datensätzen angeben, nach denen Benutzer in dieser Rolle suchen können. Zum Beispiel hat die vordefinierte Administratorrolle folgende "Los"-Ressourcen:

- Change
- Dokument nach ID
- Incident (Störung)
- Issue
- Wissen
- Problem
- Request
- Benutzer nach ID

- Benutzer nach Name
- Benutzer nach Telefonnummer

Hilfesätze

Hilfesätze sind Sammlungen von Themen in der Online-Hilfe, die für die Anwender je nach ihren Rollenzuweisungen und der aktuellen Rolleneinstellung verfügbar sind. Wenn Sie sich beispielsweise mit der Administratorrolle anmelden, können Sie die Themen in der Online-Hilfe einsehen, die zum Administrator-Hilfesatz gehören. Wenn Sie zur Mitarbeiterrolle wechseln, sehen Sie die Themen im Mitarbeiter-Hilfesatz.

Für jede vordefinierte Rolle gibt es einen entsprechenden vordefinierten Hilfesatz. Sie können für beliebige, von Ihnen definierte benutzerdefinierte Regeln benutzerdefinierte Helpsets erstellen.

Hinweis: Informationen zum Arbeiten mit Helpsetdefinitionen finden Sie in der *Online-Hilfe*.

Implementieren einer benutzerdefinierten Menüstruktur

Für viele Standorte sind die vordefinierten Rollen ausreichend. Es kann allerdings vorkommen, dass Sie eine benutzerdefinierte Rolle erstellen und diese anpassen wollen, um standortspezifische Anforderungen innerhalb Ihrer Organisation zu erfüllen.

Der folgende Prozess umreißt die Aufgaben, die Sie bei der Implementierung einer neuen Rolle ausführen müssen. Das hier gezeigte Beispiel beschreibt, wie Sie eine Rolle für eine kleine Gruppe von Analysten implementieren, die für das Überprüfen und Autorisieren von Change-Tickets zuständig sind.

Um eine benutzerdefinierte Rolle zu erstellen, führen Sie die im folgenden Beispiel beschriebenen Schritte aus:

1. Erstellen Sie einen neuen Rollendatensatz unter Verwendung der folgenden Feldwerte:

Rollenname

Change-Analyst

Code

chg_anal

Anpassung der Formulargruppe

Analyst

Bevorzugtes Dokument

Incident (Störung)

2. Wählen Sie auf der Registerkarte "Autorisierung" im Feld "Datenpartition" die Option "Service Desk-Analyst" aus.
3. Wählen Sie auf der Registerkarte "Funktionszugriff" das Feld "Changes bearbeiten".
4. Geben Sie die folgenden Werte auf der Registerkarte "Web-Schnittstelle" ein:

Web-Schnittstellentyp

Analyst

Hilfeansicht

Change-Analyst

5. Wählen Sie die folgenden Registerkarten aus:
 - Registerkarte "Berichte" - "Change-Analyst"
 - Registerkarte "Service Desk" - "Change-Analyst"
 - Registerkarte "Change-Kalender"
6. Wählen Sie auf der Registerkarte "Berichts-Webformulare" die folgenden Berichte aus:
 - Bericht über die Alterung aktiver Changes nach Priorität für Status
 - Aktive Changes am Ende der Woche
 - Changes nach fehlgeschlagenem Servicetyp für Change-Kategorien
7. Fügen Sie die Change-Ressource auf der Registerkarte "'Los'-Ressourcen" hinzu.
8. Erstellen Sie einen benutzerdefinierten Hilfesatz mit der Bezeichnung "Change-Analyst", der alle geeigneten Inhalte für die neue Rolle umfasst.

Weitere Informationen finden Sie unter [Erstellen und Veröffentlichen eines Hilfe-Moduls](#) (siehe Seite 400).

9. Erstellen Sie die folgenden benutzerdefinierten Registerkarten mit den entsprechenden Merkmalen für die neue Rolle:
 - Registerkarte "Berichte" - "Change-Analyst"
 - Registerkarte "Service Desk" - "Change-Analyst"
10. Erstellen Sie eine benutzerdefinierte Menüstruktur, die alle entsprechenden Knoten für die neue Rolle einschließt.

Weitere Informationen finden Sie unter [Implementieren einer benutzerdefinierten Menüstruktur](#) (siehe Seite 392).

Implementieren einer anwenderspezifischen Menüstruktur

Für viele Standorte sind die vordefinierten Menüstrukturen hinreichend. Es kann allerdings vorkommen, dass Sie eine Rolle anpassen möchten, indem Sie eine anwenderspezifische Menüstruktur dafür implementieren.

In den meisten Fällen ist es leichter, mit einer Kopie einer vordefinierten Menüstruktur anzufangen und dann Knoten innerhalb der Hierarchie hinzuzufügen, zu entfernen oder neu anzuordnen. Sie können aber auch eine Menüstruktur erstellen und eine völlig neue Hierarchie von Knoten aufbauen.

Sie können mit einer der folgenden Methoden eine anwenderspezifische Menüstruktur für eine Rolle verfügbar machen:

- Ersetzen Sie die Menüstruktur im Webformular (Startseite) für die Registerkarte, die die Originalstruktur "admin_tree" zeigt.
- Erstellen Sie ein Webformular und ordnen Sie das neue Webformular mit der neuen Menüstruktur einer Registerkarte zu.

So implementieren Sie ein anwenderspezifisches Menü:

1. Kopieren Sie eine der vordefinierten Menüstrukturen.

Hinweis: Notieren Sie sich den Wert, den Sie in das Feld "Code" eingeben.

2. Erstellen Sie ein Webformular mit den folgenden Feldwerten:

- **Typ:** HTML

- **Ressource:**

```
$cgi?SID=$SESSION.SID+FID=123+OP=DISPLAY_FORM+HTML=admin_main_role.html  
+KEEP.tree_code=menu_tree_code
```

Hinweis: Geben Sie den Wert des Codes für die Menüstruktur an, die Sie in Schritt 1 für menu_tree_code erstellt haben. Der Code "admin_main_role.html" verwendet den Wert der Variablen KEEP.tree_code als Menüstruktur.

3. Erstellen Sie eine Registerkarte "Bericht" mit den folgenden Feldwerten:

- **Startseite:** Das Webformular, das Sie in Schritt 2 erstellt haben
- **Menüleiste:** Administration

Hinweis: "Administration" ist eine allgemeine, von vielen Rollen benutzte Menüleiste. Sie ist nicht rollenspezifisch.

4. Weisen Sie die in Schritt 3 erstellte Registerkarte der Rolle zu, die Zugriff auf die anwenderspezifische Menüstruktur haben soll.
5. Melden Sie sich bei CA SDM ab und erneut an.

Auf der Registerkarte "Administration" wird Ihre anwenderspezifische Menüstruktur angezeigt.

Weitere Informationen:

[Erstellen von Webformular-Datensätzen](#) (siehe Seite 396)

Erstellen von Rollendatensätzen

Administratoren können für angepasste Rollen erstellen, um Standort-spezifischen speziellen Anforderungen zu entsprechen.

So erstellen Sie Rollen:

1. Wählen Sie auf der Registerkarte "Administration" "Sicherheit und Rollenmanagement", "Rollenverwaltung", "Rollenliste" aus.

Die Seite "Rollenliste" wird angezeigt.

2. Klicken Sie auf "Neu erstellen".

Die Seite "Neue Rolle" wird angezeigt.

3. Füllen Sie die folgenden Felder aus:

Rollenname

Gibt den Namen der auf der Benutzeroberfläche angezeigten Rolle an.

Code

Gibt den Code an, der die Rolle im System identifiziert.

Hinweis: Nachdem Sie den Datensatz gespeichert haben, kann dieser Feldwert nicht geändert werden.

Datensatzstatus

Zeigt an, ob die Rolle aktiv oder inaktiv ist.

Standard?

Zeigt an, ob dies die Standardrolle ist.

Anpassung der Formulargruppe

Gibt eine vordefinierte oder benutzerdefinierte Formulargruppe an.

Bevorzugtes Dokument

Gibt das von dieser Rolle zum Eingeben von Tickets in das System verwendete Dokument an.

Beschreibung

Beschreibt den Rollenzweck. Diese Beschreibung wird auf der Seite "Rollenliste" angezeigt und vereinfacht das Zuweisen von angemessenen Rollen zu Anwendern.

Klicken Sie auf "Speichern".

Die Rollendefinition wird gespeichert und die Seite "Rolle - Detail" angezeigt.

Erstellen von Registerkartendatensätzen

Sie können benutzerdefinierte Registerkarten erstellen, die dann auf der Hauptseite der Web-Schnittstelle angezeigt werden. Wenn Sie einen Registerkartendatensatz mit einem Rollendatensatz verbinden, ist er für alle Benutzer verfügbar, denen diese Rolle zugeordnet ist.

So erstellen Sie Registerkarten:

1. Wählen Sie auf der Registerkarte "Administration" "Sicherheit und Rollenverwaltung", "Rollenverwaltung", "Registerkarten" aus.

Die Seite "Registerkarten - Liste" wird angezeigt.

2. Klicken Sie auf "Neu erstellen".

Die Seite "Neue Registerkarte erstellen" wird angezeigt.

3. Füllen Sie die folgenden Felder aus:

Registerkartenname

Gibt den Namen an, der die Registerkarte innerhalb der Administrator-Schnittstelle kennzeichnet. Der Registerkartenname wird beispielsweise auf der Seite "Registerkarten - Liste" angezeigt.

Code

Gibt den Code an, der diese Registerkarte im System identifiziert.

Hinweis: Nachdem der Code definiert wurde, kann er nicht mehr geändert werden.

Datensatzstatus

Zeigt an, ob der Kontakt aktiv oder inaktiv ist.

Anzeigename

Gibt den Namen an, der in der grafischen Darstellung der Registerkarte in der Benutzeroberfläche angezeigt wird.

Startseite

Gibt das Web-Ausgangsformular an, das im Hauptfenster angezeigt wird, wenn ein Benutzer diese Registerkarte auswählt.

Wichtig! Die Startseite und die Menüleiste müssen der gleichen Formulargruppe angehören. Wenn Sie eine Registerkarte mit einer Startseite und einer Menüleiste definieren, die verschiedenen [Formulargruppen](#) (siehe Seite 1257) angehören, tritt beim Benutzerzugriff auf die Registerkarte ein Fehler auf.

Menüleiste

Gibt die Menüleiste an, die im Hauptfenster angezeigt wird, wenn ein Benutzer diese Registerkarte auswählt.

Klicken Sie auf "Speichern".

Die Registerkarte wird erstellt.

Erstellen von Menüleistendatensätzen

Sie können angepasste Menüleisten erstellen, um den Zugriff auf Systemfunktionen für die benutzerdefinierten Rollen zu steuern.

So erstellen Sie Menüleisten:

1. Von der Registerkarte "Administration" navigieren Sie zu "Sicherheit und Rollenverwaltung", "Rollenverwaltung", "Menüleisten".

Die Seite "Menüleiste - Liste" wird angezeigt.

2. Klicken Sie auf "Neu erstellen".

Die Seite "Neue Menüleiste erstellen" wird angezeigt.

3. Füllen Sie die folgenden Felder aus:

Menüleiste - Name

(Erforderlich) Gibt den Name für die Menüleiste an. Mithilfe dieses Feldes können Sie die in der Menüleiste verfügbaren Funktionen identifizieren.

Code

(Erforderlich) Gibt den Code an, der diese Menüleiste im System identifiziert. Nachdem der Code definiert wurde, kann er nicht mehr geändert werden.

Datensatzstatus

Zeigt an, ob die Menüleiste aktiv oder inaktiv ist.

HTML-Name

Gibt den Namen des HTML-Formulars an, das die Menüleistendefinition enthält. Die Menüleiste unter Verwendung des Web Screen Painter entworfen.

Beschreibung

Beschreibt die Menüleiste. Mit dieser Beschreibung können Sie weitere Angaben zur Menüleiste und zu den Rollen machen, die sie verwenden.

Klicken Sie auf "Speichern".

Die Menüleistendefinition wird gespeichert, und die Seite "Menüleiste - Detail" wird angezeigt.

Erstellen von Webformular-Datensätzen

Administratoren können eigene benutzerdefinierte Webformulare erstellen, die als Startseiten für Registerkarten, auf Registerkarten anzuzeigende Berichte, als "Los"-Schaltflächen oder als ein weiterer URL dienen sollen.

So erstellen Sie Webformulare:

1. Von der Registerkarte "Administration" navigieren Sie zu "Sicherheit und Rollenverwaltung", "Rollenverwaltung", "Webformulare".

Die Seite "Webformularliste" wird angezeigt.

2. Klicken Sie auf "Neu erstellen".

Die Seite "Neues Webformular erstellen" wird angezeigt.

3. Füllen Sie die folgenden Felder aus:

Name des Webformulars

(Erforderlich) Gibt den Namen für das Webformular an.

Datensatzstatus

Zeigt an, ob dieses Formular aktiv oder inaktiv ist.

Code

(Erforderlich) Gibt den Code an, der das Webformular im System identifiziert. Nachdem der Code definiert wurde, kann er nicht mehr geändert werden.

Hinweis: Dieses Feld gibt "web_form_name" auf der Registerkarte "Eigenschaften" eines Multiframe-Formulars in Web Screen Painter an.

Typ

Gibt eine der folgenden Arten von Webformularen an, die Sie erstellen:

- **HTMPL-Seite** - Zeigt eine Webseite an, die als Startseite für eine der von Ihnen erstellten benutzerdefinierten Registerkarten dient.
- **Report** - Gibt einen CA SDM-Bericht an, der auf einer beliebigen Registerkarte angezeigt wird.

- **Los: Ressource** - Gibt als Ressource eine Los-Schaltfläche an.
- **Other** - Greift über URLs auf andere externe Webseiten zu.

Beschreibung

Beschreibt das Webformular. In diesem Feld können Sie weitere Angaben zum Webformular machen, z. B. wo es angezeigt wird und wozu es dient.

Ressource

Gibt den Code an, der das Webformular aufruft. Dies kann Befehlszeilencode oder eine URL sein.

Beispiel: Öffnen Sie das einfache HTML-Formular "menu_tab_dflt.html":
`$cgi?SID=$SESSION.SID+FID=123+OP=DISPLAY_FORM+HTML=menu_tab_dflt.html`

Klicken Sie auf "Speichern".

Kopieren von Menüstrukturen

Sie können eine bestehende Menüstruktur kopieren, um sie als Ausgangspunkt für eine für angepasste Menüstruktur zu verwenden.

So kopieren Sie Menüstrukturen:

1. Wählen Sie "Sicherheit und Rollenverwaltung", "Rollenverwaltung", "Menüstrukturen" auf der Registerkarte "Administration" aus.

Die Seite "Menüstruktur - Liste" wird angezeigt.

2. Klicken Sie die Menüstruktur, die Sie kopieren möchten.

Die Seite "Menüstruktur - Detail" wird angezeigt.

3. Klicken Sie auf "Datei" > "Kopieren".

Die Seite "Neue Menüstruktur erstellen" wird angezeigt.

4. Füllen Sie die folgenden Felder aus:

Menüstruktur - Name

(Erforderlich) Der von Ihnen zugewiesene Name für diese Menüstruktur.

Code

(Erforderlich) Der Code, der die Menüstruktur gegenüber dem System identifiziert. Nachdem der Code definiert wurde, kann er nicht mehr geändert werden.

Datensatzstatus

Zeigt an, ob diese Menüstruktur aktiv oder inaktiv ist.

Beschreibung

Beschreibt die Menüstruktur. In der Beschreibung können Sie zusätzliche Details zu der Menüstruktur und den Rollen angeben, die diese verwenden.

Klicken Sie auf "Speichern".

Die Seite "Menüstruktur - Detail" für die neue Menüstruktur wird angezeigt.

5. Klicken Sie auf "Menü anpassen".

Eine Kopie der ursprünglichen Menüstruktur wird angezeigt.

6. Passen Sie die Menüstruktur nach Wunsch an.

Hinweis: Weitere Informationen zum Hinzufügen, Entfernen und Bearbeiten von Menüstrukturressourcen finden Sie in der *Online-Hilfe*.

Erstellen und Anpassen von Menüstrukturen

Sie können Menüstrukturen auf der Basis einer der vorgegebenen Standardmenüstrukturen erstellen und für spezielle Bedürfnisse anpassen.

So erstellen Sie Menüstrukturen and passen sie an:

1. Wählen Sie "Sicherheit und Rollenverwaltung", "Rollenverwaltung", "Menüstrukturen" auf der Registerkarte "Administration" aus.

Die Seite "Menüstruktur - Liste" wird angezeigt.

2. Klicken Sie auf "Neu erstellen".

Die Seite "Neue Menüstruktur erstellen" wird angezeigt.

3. Füllen Sie die folgenden Felder aus:

Menüstruktur - Name

(Erforderlich) Der von Ihnen zugewiesene Name für diese Menüstruktur.

Code

(Erforderlich) Der Code, der die Menüstruktur gegenüber dem System identifiziert. Nachdem der Code definiert wurde, kann er nicht mehr geändert werden.

Datensatzstatus

Zeigt an, ob diese Menüstruktur aktiv oder inaktiv ist.

Beschreibung

Eine Beschreibung der Menüstruktur. In der Beschreibung können Sie zusätzliche Details zu der Menüstruktur und den Rollen angeben, die diese verwenden.

4. Klicken Sie auf "Speichern".

5. Klicken Sie auf "Menü anpassen".

Es wird ein Formular angezeigt, über das Sie die Menüstruktur anpassen können. Diese Menüstruktur enthält zunächst lediglich einen obersten Knoten mit dem Text, den Sie als Menüstrukturname eingegeben haben.

6. Klicken mit der rechten Maustaste auf den Knoten in der Menüstruktur und wählen Sie aus dem Kontextmenü den Befehl "Neuen Knoten erstellen".

Die Seite "Neuen Knoten erstellen" wird angezeigt.

7. Füllen Sie die folgenden Felder aus:

Knotenname

Geben Sie einen Namen für den Knoten ein. Dies ist der Name, der in der Menüstruktur angezeigt wird.

Beschreibung

Geben Sie eine Beschreibung für den Knoten ein. Mit dieser Beschreibung können Sie den Zweck des Knotens definieren.

Ressource

Geben Sie die Ressource direkt in das Feld ein, oder klicken Sie auf das Suchsymbol, um die Ressource aus einer Liste auszuwählen. Die Menüstrukturressource legt die Aktion fest, die ausgeführt werden soll, wenn der Benutzer den Knoten aus der Menüstruktur auswählt.

8. Wiederholen Sie Schritte 6 und 7 für alle Knoten, die in der Menüstruktur angezeigt werden sollen.

Hinweis: Weitere Informationen zum Hinzufügen, Entfernen und Bearbeiten von Menüstrukturressourcen finden Sie in der *Online-Hilfe*.

9. Klicken Sie auf "Speichern".

Die Menüstrukturdefinition wird gespeichert, und die Seite "Menüstruktur - Detail" wird angezeigt.

Erstellen und Veröffentlichen von Helpsets

Sie können für beliebige, von Ihnen definierte benutzerdefinierte Regeln benutzerdefinierte Helpsets erstellen.

So erstellen Sie ein Helpset, fügen ihm Daten hinzu und veröffentlichen es:

1. Wählen Sie auf der Registerkarte "Administration" "Sicherheit und Rollenverwaltung", "Rollenverwaltung", "Hilfesätze" aus.

Die Seite "Hilfesatz - Liste" wird angezeigt.

2. Klicken Sie auf "Neu erstellen".

Die Seite "Neuen Hilfesatz erstellen" wird geöffnet.

3. Füllen Sie die folgenden Felder aus:

Name des Helpsets

Der einmalige Name dieses Hilfesatzes.

Schnittstellentyp

Der Schnittstellentyp des Hilfesatzes (wie z. B. Analyst, Mitarbeiter oder Kunde).

Datensatzstatus

Zeigt an, ob der Hilfesatz aktiv oder inaktiv ist.

Dateinamenpräfix

Das Präfix, das an die Hilfedateien angehängt werden soll, die für diesen Hilfesatz generiert werden. Verwenden Sie in den Namen keine Leerzeichen.

Hinweis: Weisen Sie ein Präfix zu, mit dem Sie die Dateien, die zu diesem Helpset gehören, problemlos erkennen. Verwenden Sie beispielsweise ANAL als Präfix für den Hilfesatz für Analysten.

Intern

Für benutzerdefinierte Helpsets ist diese Option auf NEIN gesetzt. Der Wert für dieses Feld kann nicht geändert werden.

4. Klicken Sie auf "Speichern".

Die Registerkarte "Inhalt" wird angezeigt.

5. Klicken Sie auf "Inhalt definieren".

Das Fenster "Ausgewählte Hilfe aktualisieren" wird geöffnet.

6. Wählen Sie den Inhalt aus, der in dem Helpset enthalten sein soll.

Wichtig! Einige Themen sind obligatorisch und werden in jedem Fall in Ihren neuen Hilfesatz aufgenommen, unabhängig davon, ob Sie sie markieren oder nicht. Hierzu gehören beispielsweise die CA SDM-Startseite und andere Titelthemen. Verschachtelte Themen sind zudem abhängig von ihren Containerthemen. Containerthemen werden automatisch berücksichtigt, wenn Sie eines der verschachtelten Themen aufnehmen. Wenn Sie beispielsweise das Thema über die Verwendung des Scoreboard markieren, wird auch das Containerthema "Navigieren in CA SDM" eingebunden, wenn Sie den Hilfesatz veröffentlichen.

7. Klicken Sie auf "OK".

Das Fenster "Ausgewählte Hilfe aktualisieren" wird geschlossen und der Inhalt auf der Registerkarte "Inhalt" aufgeführt.

8. Klicken Sie auf "Veröffentlichen".

Daraufhin wird der Hilfesatz durch Packen der ausgewählten Themen in ein Hilfesystem, das Sie in einem Webbrowser anzeigen können, generiert.

9. Warten Sie einen Augenblick, bis das Veröffentlichungsverfahren abgeschlossen ist, und wählen Sie dann in der Menüleiste "Ansicht" und "Aktualisieren" aus.

Die Schaltfläche "Hilfe anzeigen" ist nun verfügbar.

10. Klicken Sie auf "Hilfe anzeigen".

Das benutzerdefinierte Helpset wird in Ihrem Standardwebbrowser angezeigt.

Wechseln von Rollen

Benutzer mit entsprechend zugewiesenen Rollen können zwischen Rollen wechseln, ohne sich erneut am System anmelden zu müssen. Rollen können Benutzern über den Zugriffstyp oder den Kontaktdatensatz zugewiesen werden.

Hinweis: Weitere Informationen finden Sie unter [Konfigurieren von Benutzerkonten](#) (siehe Seite 337).

So wechseln Sie Ihre Rolle:

1. Wählen Sie die gewünschte Rolle aus der Dropdown-Liste "Rolle" oben rechts in der Hauptseite der CA SDM-Web-Schnittstelle.
2. Klicken Sie auf "Rolle festlegen".

Die Web-Schnittstelle und die verfügbare Funktionalität werden entsprechend der neu angenommenen Rolle angepasst.

Kapitel 10: Einrichten einer Support-Struktur

Dieses Kapitel enthält folgende Themen:

[Modelle](#) (siehe Seite 403)
[CA Workflow](#) (siehe Seite 407)
[CA Process Automation-Workflow-Integration](#) (siehe Seite 410)
[Freigegebene Codes](#) (siehe Seite 417)
[Statuscodes](#) (siehe Seite 419)
[Aufgabentypen](#) (siehe Seite 424)
[Request-/Incident-/Problembereiche](#) (siehe Seite 427)
[Change- und Issue-Kategorien](#) (siehe Seite 430)
[Automatisches Schließen von Tickets](#) (siehe Seite 436)
[Aktivitäten zugehöriger Tickets](#) (siehe Seite 438)
[Prioritätsberechnung](#) (siehe Seite 440)
[Statusübergänge und abhängige Attributsteuerungen](#) (siehe Seite 458)
[Statusübergänge für Self-Service](#) (siehe Seite 469)
[Timer](#) (siehe Seite 474)
[Zeitzone](#) (siehe Seite 475)
[So richten Sie die Anhangsbibliothek ein](#) (siehe Seite 478)
[Ankündigungen](#) (siehe Seite 488)
[Einrichten von gespeicherten Abfragen](#) (siehe Seite 490)
[Sequenznummern](#) (siehe Seite 491)
[Verwenden des Audit-Protokolls](#) (siehe Seite 492)
[Integration in das CA-Netzwerk und Systemverwaltung](#) (siehe Seite 493)
[Drucken von CA SDM-Webseiten](#) (siehe Seite 493)
[Verhalten für die Anzeige von Datensätzen in der Web-Schnittstelle](#) (siehe Seite 494)
[Support-Struktur](#) (siehe Seite 495)
[Aktivieren der CAPA-Hilfe](#) (siehe Seite 495)

Modelle

CA SDM unterstützt die folgenden Service Desk-Modelle:

- Internes Modell
- Externes Modell
- Kombiniertes Modell

Hinweis: Einzelheiten zur Verwendung der Web-Schnittstelle zum Implementieren des ausgewählten Modells finden Sie in der *Online-Hilfe*.

Internes Modell

Ein interner Service Desk unterstützt Mitarbeiter, die für eine Firma arbeiten und Fragen oder Probleme hinsichtlich der Produkte und Dienste haben, die ihnen von der Firma zur Verfügung gestellt werden. In CA SDM ist die Anfrage die grundlegende Support-Einheit bei einem internen Service Desk.

- Anfragen sind Tickets, die sich um die Fragen oder die Probleme der Mitarbeiter kümmern. Ihre Aufgabe ist die Unterstützung einer Infrastruktur, die Bestandteil der Supportorganisation ist und von dieser verwaltet wird.
- Changes sind Tickets, die Changes an der unterstützten Unternehmensinfrastruktur verwalten. Interne Service Desks verwenden häufig Anfragen als primäres Ticket und hängen Changes an, wenn die Anfrage eine Änderung der Infrastruktur zur Folge hat.

Wenn Sie einen internen Service Desk betreiben, gehen Sie wie folgt vor:

- Überprüfen Sie die Mitarbeiter-Kontakttypen mit der Verwaltungsfunktion der Web-Schnittstelle, um herauszufinden, ob sie Ihre Anforderungen erfüllen. Wenn die meisten Ihrer Kontakte Mitarbeiter sind, die den Service Desk für Support verwenden, können Sie „Mitarbeiter“ als Standardzugriffstyp festlegen. Auf diese Weise müssen Sie den Zugriffstyp nicht für jeden Mitarbeiterkontakt festlegen, der von Ihrem Service Desk unterstützt wird.
- Überprüfen Sie die Mitarbeiter-Kontakttypen mit der Verwaltungsfunktion der Web-Schnittstelle, um herauszufinden, ob sie Ihre Anforderungen erfüllen.
- Stellen Sie sicher, dass Ihre Kontakte so festgelegt sind, dass sie über den entsprechenden Zugriffstyp und Kontakttyp verfügen. Wenn Sie zum Beispiel „Mitarbeiter“ als Standardzugriffstyp festlegen, müssen Sie auch für die Analytikerkontakte den Zugriffstyp „Analytiker“ festlegen.

Der Kontakttyp wird normalerweise abhängig davon zugewiesen, wie Sie den Kontakt erstellen. In einigen Fällen wurde der Kontakttyp jedoch nicht definiert. Mitarbeiter, die den Service Desk für Support verwenden, sollten den Kontakttyp „Mitarbeiter“ haben, während Mitarbeiter, die als Support Desk-Analytiker arbeiten, den Kontakttyp „Analytiker“ haben sollen.

Sie können unter Verwendung der administrativen Funktion der Web-Schnittstelle mit Kontakten arbeiten.

Wenn Sie einen internen Service Desk betreiben, in dem Sie Mitarbeiter unterstützen, besteht Ihre Support-Struktur aus den Anfragen und Changes, die die Mitarbeiter erstellen, und den zugrunde liegenden Unterstützungsfunktionen für diese Anfragen und Changes. Als Administrator richten Sie die Support-Struktur ein.

Externes Modell

Ein externer Service Desk unterstützt Kunden, die Produkte oder Dienste von Ihrer Firma kaufen und Fragen oder Probleme hinsichtlich der Produkte oder Dienste haben. In CA SDM ist der Issue die grundlegende Support-Einheit bei einem externen Service Desk. Issues sind Tickets zur Abwicklung von Kundenfragen oder -problemen und sind auf die Unterstützung der von den Kunden erworbenen Produkte und Dienste ausgerichtet.

Wenn Sie einen externen Service Desk betreiben, sollten Sie folgende Punkte beachten:

- Überprüfen Sie den Kundenzugriffstyp mit der Verwaltungsfunktion der Web-Schnittstelle, um herauszufinden, ob er Ihre Anforderungen erfüllt. Wenn es sich bei den meisten Ihrer Kontakte um Kunden handelt, können Sie „Kunde“ als Standardzugriffstyp festlegen.
- Überprüfen Sie den Kundenkontakttyp mit der Verwaltungsfunktion der Web-Schnittstelle, um herauszufinden, ob sie Ihre Anforderungen erfüllen.
- Stellen Sie sicher, dass Ihre Kontakte so festgelegt sind, dass sie über den entsprechenden Zugriffstyp und Kontakttyp verfügen. Wenn Sie zum Beispiel „Kunde“ als Standardzugriffstyp festlegen, müssen Sie auch für die Analytikerkontakte den Zugriffstyp „Analytiker“ festlegen.

Der Kontakttyp wird normalerweise abhängig davon zugewiesen, wie Sie den Kontakt erstellen. In einigen Fällen wurde der Kontakttyp jedoch nicht definiert. Kunden, die den Service Desk für Support verwenden, sollten den Kontakttyp „Kunde“ haben, und Analytiker, die im Support Desk arbeiten, sollten den Kontakttyp „Analytiker“ haben.

Sie können unter Verwendung der administrativen Funktion der Web-Schnittstelle mit Kontakten arbeiten.

Wenn Sie einen externen Service Desk betreiben, in dem Sie Kunden unterstützen, besteht Ihre Support-Struktur meistens aus den Issues, die die Kunden erstellen, und den zugrunde liegenden Unterstützungsfunktionen für diese Issues. Als Administrator müssen Sie die Support-Struktur mithilfe der in diesem Kapitel folgenden Informationen einrichten. Jedes Thema gibt an, ob die Informationen auf Ihr Modell zutreffen.

Kombiniertes Modell

Einige Firmen müssen sowohl einen internen als auch einen externen Service Desk betreiben. In diesem Fall haben Sie folgende Möglichkeiten:

- Trennen Sie das interne und externe Service Desk-Modell durch separate Service Desk-Installationen.
- Richten Sie CA SDM zur Unterstützung beider Modelle ein.

Letztere Methode ist nützlich, wenn Ihre Service Desk-Analysten sowohl für die Unterstützung von Mitarbeitern als auch von Kunden geschult sind und wenn die Unterscheidung zwischen internem und externem Support nicht immer klar ist. Zum Beispiel können Mitarbeiter Produkte von Ihrer Firma kaufen oder Kunden können Probleme und Fragen hinsichtlich der Infrastruktur Ihrer Firma haben.

Als Administrator müssen Sie die Support-Struktur für einen kombinierten internen/externen Service Desk, der aus Issues, Requests und Changes besteht, und die zugrunde liegenden Support-Funktionen einrichten. Wenn Sie sich für einen kombinierten internen/externen Service Desk entscheiden, führen Sie folgende Schritte aus, bevor Sie eine Struktur einrichten:

- Überprüfen Sie die Zugriffstypen "Mitarbeiter" und "Kunde" mit der Verwaltungsfunktion der Web-Schnittstelle, um herauszufinden, ob sie Ihre Anforderungen erfüllen. Wenn es sich bei den meisten Ihrer Kontakte um Kunden handelt, können Sie „Kunde“ als Standardzugriffstyp festlegen. Wenn die meisten Ihrer Kontakte Mitarbeiter sind, die den Service Desk für Support verwenden, können Sie „Mitarbeiter“ als Standardzugriffstyp festlegen.
- Überprüfen Sie die Kontakttypen "Mitarbeiter" und "Kunde" mit der Verwaltungsfunktion der Web-Schnittstelle, um herauszufinden, ob sie Ihre Anforderungen erfüllen.
- Stellen Sie sicher, dass Ihre Kontakte so festgelegt sind, dass sie über den entsprechenden Zugriffstyp und Kontakttyp verfügen. Wenn Sie zum Beispiel "Kunde" als Standardzugriffstyp festlegen, müssen Sie auch für die Analystenkontakte den Zugriffstyp "Analyst" und für die Mitarbeiterkontakte den Zugriffstyp "Mitarbeiter" festlegen

Der Kontakttyp wird normalerweise abhängig davon zugewiesen, wie Sie den Kontakt erstellen. In einigen Fällen kann es jedoch sein, dass der Kontakttyp nicht definiert wird.

- Der Kontakttyp von Kunden, die den Service Desk für Support nutzen, sollte "Kunde" sein.
- Der Kontakttyp von Mitarbeitern, die den Service Desk für Support nutzen, sollte "Mitarbeiter" sein.
- Der Kontakttyp von Mitarbeitern, die beim Service Desk als Support-Desk-Analysten arbeiten, sollte "Analyst" sein.

Sie können unter Verwendung der administrativen Funktion der Web-Schnittstelle mit Kontakten arbeiten.

Weitere Informationen:

[Kontakttypen](#) (siehe Seite 340)

[Funktionsweise von Zugriffstypen](#) (siehe Seite 372)

CA Workflow

Eine CA Workflow-Prozessdefinition kann mit jedem CA SDM-Tickettyp (siehe Seite 64) verknüpft werden. Die Prozessdefinition, die auf einzelne Tickets angewendet wird, wird von der Change-Kategorie, der Issue-Kategorie oder vom Request-/Incident-/Problembereich bestimmt, dem das Ticket zugewiesen ist.

Wenn eine CA Workflow-Prozessdefinition mit einer Kategorie oder einem Bereich verknüpft wird und ein Ticket dieser Kategorie oder diesem Bereich zugeordnet ist, erstellt CA Workflow eine Prozessinstanz aus der Definition. Der Fortschritt der Prozessinstanz wird auf der Registerkarte "Workflow-Aufgaben" des Tickets angezeigt.

Sie können während der CA SDM-Installation optional CA Workflow installieren oder CA SDM anweisen, eine andere Instanz von CA Workflow durch Aktualisieren mehrerer Optionen Optionsmanager zu verwenden, einschließlich:

CAWF_USERNAME

Gibt den CA EEM-Anwender an, der vollen Zugriff auf CA Workflow hat (Berechtigungen für IDE- und Process-Ressourcen)

CAWF_PASSWORD

Gibt das Kennwort für den cawf_username an.

CAWF_PM_LOCATION

Gibt als Lokation `http://<server>:8090/pm/` an.

CAWF_PM_URL

Gibt die folgende URL an:

`http://<wf_hostname>:<wf_tomcat_port>/pm/services/pmService2`

CAWF_WL_LOCATION

Gibt als Lokation `http://<server>:8090/wl/` an.

CAWF_WL_URL

Gibt als URL `http://<server>:8090/wl/services/wlService` an.

Diese Optionen bestimmen verschiedene Endpunkte für CA Workflow. In den meisten Fällen müssen Sie einfach den Server und den Anschluss aktualisieren, damit diese der Position von CA Workflow entsprechen.

Wichtig! Nach einer Änderung des CA Workflow-Servers funktionieren vorhandene Kategorien, Bereiche oder Tickets, die mit Definitionen und Prozessinstanzen auf dem alten Server verknüpft sind, nicht mehr.

Workflow zur Laufzeit

Wenn ein Ticket mit einer Kategorie oder einem Bereich gespeichert werden, der mit einer CA Workflow-Prozessdefinition verknüpft ist, wird eine Instanz der Definition erstellt. Der Fortschritt der Instanz wird auf der Registerkarte "Workflow-Aufgaben" des Tickets angezeigt. Da CA Workflow Verzweigungen enthalten kann, werden nur abgeschlossene und ausstehende Arbeitselemente angezeigt.

Auf der Registerkarte "Workflow-Aufgaben" werden alle abgeschlossenen und ausstehenden Arbeitselemente sowie der Status des gesamten Workflows angezeigt. Wenn Sie auf den Link "Aktivitätsname" klicken, wird die Web-Anwendung "CA Workflow Worklist" angezeigt, in der Sie einzelne Arbeitselemente abschließen können.

Die Daten für die Registerkarte "Workflow" werden direkt aus dem CA Workflow-Server abgerufen. Wenn der CA Workflow-Server nicht verfügbar ist, wird eine Fehlermeldung auf der Registerkarte angezeigt.

Auswählen einer Workflow-Prozessdefinition

Eine CA Workflow-Prozessdefinition muss über das Zeichenfolgenattribut *usd_persid* verfügen, das mit einer Change- oder Issue-Kategorie oder einem Request-/Incident-/Problembereich verknüpft ist. Dieses Attribut muss als Eingabeparameter gekennzeichnet werden. Wenn CA SDM die CA Workflow-Instanz startet, setzt sie "usd_persid" auf den eindeutigen Bezeichner ("persistent_id") des Tickets. Ein Verwendungszweck für "usd_persid" besteht darin, Webservice-Aufrufe von CA Workflow zu CA SDM zu ermöglichen.

Wichtig! Change- und Issue-Kategorien können entweder das interne (klassische) Workflow-System oder die CA Workflow-Anwendung von CA SDM verwenden, nicht aber beide gleichzeitig. Request-/Incident-/Problembereiche können nur die CA Workflow-Anwendung verwenden. Das klassische interne Workflowsystem wird nicht für Request-, Incident- oder Problemtickets unterstützt.

So wählen Sie eine CA Workflow-Prozessdefinition aus:

1. Wählen Sie eine Change- oder Issue-Kategorie aus. Um z. B. eine Change-Kategorie auszuwählen, wählen Sie auf der Registerkarte "Administration" die Optionen "Service Desk" > "Changes" > "Kategorien" aus.

Die Seite "Change-Kategorien - Liste" wird angezeigt.

2. Klicken Sie auf das Symbol der Change-Kategorie, die Sie bearbeiten wollen.

Die Seite "Change-Kategorie – Detail" wird angezeigt.

3. Klicken Sie auf der Registerkarte "Workflow" auf die Schaltfläche "CA Workflow verwenden".

Hinweis: Wenn Sie diesen Vorgang fortsetzen und die Kategorie speichern, wird ein mit der Kategorie verbundener Workflow im Stil von CA SDM gelöscht.

Eine Auswahlseite, auf der die verfügbaren CA Workflow-Bearbeitungsdefinitionen ausgeführt sind, wird angezeigt.

4. Wählen Sie eine CA Workflow-Prozessdefinition.

Die Auswahl wird in die Kategorie eingetragen.

5. Klicken Sie auf "Speichern".

Die Kategorie wird mit der ausgewählten Prozessdefinition aktualisiert.

6. (Optional) Ändern Sie die verknüpfte CA Workflow-Prozessdefinition durch Bearbeiten der Kategorie, und klicken Sie auf den Hyperlink der CA Workflow-Definition.

Die Seite zum Auswählen von Prozessdefinitionen wird angezeigt.

Hinweis: CA Workflow-Prozessdefinitionen werden nur auf der Auswahlseite angezeigt, wenn die Definition das Zeichenfolgenattribut "usd_persid" besitzt. Wenn die Definition gestartet wird, wird dieses Attribut auf den Wert von persistent_id des Tickets eingestellt. Die CA Workflow-Prozessdefinition kann optional den Zeichenfolge-Eingabeparameter "label" enthalten. Wenn dieser Parameter definiert ist, stellt CA SDM für seinen Wert die Ticketnummer ein. Die Ticketnummer wird in der CA Workflow-Worklist angezeigt und bietet Kontext zum Arbeitselement.

Workflow-Aufgaben

Workflow-Aufgaben geben die Aktivitäten an, die für Tickets abgeschlossen werden müssen, die einer bestimmten Kategorie oder einem bestimmten Bereich zugeordnet sind. Wie Eigenschaften und andere Aspekte von Kategorien oder Bereichen werden bei Auswahl der Kategorie die betreffenden Aufgaben automatisch zum Ticket hinzugefügt. Die Definition von Workflow-Aufgaben bietet folgende Möglichkeiten:

- Angeben und Beschreiben der Art der durchzuführenden Aufgabe
- Zuweisen einer Sequenznummer zu jeder Aufgabe
- Angeben des Benutzers, der die Aufgabe durchführt
- Identifizieren des Fortschritts bei der Lösung von Aufgaben durch Zuweisen bestimmter Status, die für die einzelnen Aufgaben gelten

Wenn sich der Status einer Aufgaben ändert, können bestimmte Verhaltensweisen ausgelöst werden. Mit Verhalten können Sie spezielle Aufgaben oder Prozesse definieren, die durchgeführt werden, wenn die Workflow-Aufgabe einen bestimmten Status erreicht. Durch die Definition von Verhalten können Sie zum Beispiel einem bestimmten Manager eine E-Mail-Benachrichtigung senden, wenn eine Genehmigungsaufgabe in den Status „In Bearbeitung“ wechselt.

Hinweis: Weitere Informationen zum Erstellen von Workflow-Aufgaben und Definieren von Verhaltensweisen für diese finden Sie in der *Online-Hilfe*.

CA Process Automation-Workflow-Integration

CA Process Automation ist ein eigenständiges CA-Produkt mit Funktionen zur Automatisierung und Verfolgung von Hardware- und Softwareverwaltungsaufgaben in IT-Umgebungen von Unternehmen. CA Process Automation dient zur Automatisierung von Aufgaben und Verwaltung von Anwenderinteraktionen, wie Genehmigungen und Benachrichtigungen, um Compliance und Genauigkeit in Produktionsumgebungen zu gewährleisten.

Wenn Sie CA SDM und CA Process Automation integrieren, dann können Sie die Vorteile der CA Process Automation-Workflowfunktionen von wichtigen Punkten in CA SDM nutzen. Eine wirksame Integration von CA SDM und CA Process Automation erfordert, dass Sie beide Produkte kennen.

Weitere Informationen:

[CA Process Automation-Komponenten](#) (siehe Seite 411)

[CA Process Automation Integration mit CA SDM zur Laufzeit](#) (siehe Seite 412)

[Erstellen einer Prozessdefinition](#) (siehe Seite 413)

[Erstellen von Startauftragsformularen](#) (siehe Seite 414)

[Anhängen von CA Process Automation-Prozessdefinitionen](#) (siehe Seite 416)

CA Process Automation-Komponenten

CA Process Automation bietet viele Möglichkeiten und Strukturen, die eine breite Palette von Aktivitäten als Teile des CA Process Automation-Prozessmanagement erleichtern. Für die Integration in CA SDM sind allerdings nur die folgenden CA Process Automation-Komponenten für die CA Process Automation-Integration kritisch:

- **Prozessdefinition** - Identifiziert eine kollektive Reihe von Aufgaben, Schritten und Bedingungen, die in einer bestimmten Start-Reihenfolge strukturiert und von verschiedenen Personen oder Beteiligten abgeschlossen werden. Diese Komponente ist der zentrale Baustein aller CA Process Automation-Inhalte.
- **Startauftragsformular** - Objekt, welche beschreibende Informationen für Endbenutzer enthält. Das Startauftragsformular bietet Benutzern eine Prozessdefinition und blendet die technischen Details der Prozessdefinition aus.
- **Schlüsselwörter** - Liste mit vordefinierten Wörtern oder Phrasen, die an Startauftragsformularen angehängt werden müssen.
- **Automations-Bibliothek** - Bereich innerhalb von CA Process Automation, der Prozessdefinitionen und Startauftragsformulare speichert und anzeigt
- **Bibliothekspfad oder Referenzpfad** - Ordnerstruktur, die Prozessdefinitionen und Startauftragsformulare innerhalb der Automations-Bibliothek organisiert und beschreibt
- **Prozessinstanz** - Aktive Entität, die die Regeln ausführt, welche in einer Prozessdefinition definiert sind. Die Prozessinstanz schreitet fort, bis der Prozessdefinitionsstatus vollständig ist.
- **Meldungen zum Prozessinstanzprotokoll** - Konfigurierbarer, laufender Datensatz, der das Fortschreiten von Aktivitäten der Prozessinstanz detailliert angibt. Protokollmeldungskategorien sind bei der CA SDM-Integration in CA Process Automation nützlich.

Hinweis: Der Anwendungsbereich der Definitionen von CA Process Automation-Komponenten ist auf die Verwendung innerhalb von CA SDM beschränkt. Informationen zu CA Process Automation-Komponenten und -Funktionen finden Sie in der CA Process Automation-Dokumentation.

CA Process Automation Integration mit CA SDM zur Laufzeit

Wenn Sie die Integration durchführen, sind für CA SDM-Benutzer folgende Funktionen verfügbar:

- Bei einer neuen Anfrage, Change oder Issue wird eine auf der Ticketkategorie oder dem Ticketbereich basierende CA Process Automation-Prozessinstanz ausgelöst. Daraufhin werden sofort Zusammenfassung-Informationen auf der Registerkarte "Workflow-Aufgaben" angezeigt.
- Wenn sich ein Anfragebereich, eine Change-Kategorie, oder eine Issue-Kategorie ändert, dann wird eine angehängte CA Process Automation-Prozessinstanz beendet und eine neue Prozessinstanz ausgelöst.
- Wenn Sie als CA SDM-Benutzer versuchen, eine Anfrage, einen Change oder ein Issue mit einer unvollständigen CA Process Automation-Prozessinstanz zu schließen, dann können Sie das Ticket nicht schließen. Statt dessen müssen Sie zuerst das Ticket annullieren. Der Status "Annullieren" beendet die CA Process Automation-Prozessinstanz, bevor das Ticket geschlossen wird.
- Wenn Sie den Status der Prozessinstanz abfragen möchte, ohne außerhalb des Tickets zu navigieren, dann klicken Sie auf die Registerkarte "Workflow-Aufgaben" des Tickets. Die Registerkarte "Workflow-Aufgaben" zeigt das Startdatum, das Enddatum und den aktuellen Status der Prozessinstanz sowie einen aktuellen Audit-Pfad von Nachrichten an, wo der Pfad der Prozessinstanz angegeben wird.
- Wenn Sie den aktuellen Pfad der Prozessinstanz innerhalb des gesamten Prozesses sehen möchten, dann wählen Sie auf der Registerkarte "Workflow-Aufgaben" die Schaltfläche "Vorgang anzeigen". Die Schaltfläche "Vorgang anzeigen" löst einen graphischen Snapshot der gesamten Prozessinstanz aus und zeigt den aktuellen Pfad an.
- Wenn Sie die CA Process Automation-Interaktions-Anfrageformulare anzeigen möchten, für die eine Benutzeraktion anhängig ist, dann wählen Sie auf der Registerkarte "Workflow-Aufgaben" einen beliebigen Eintrag. Die Registerkarte "Workflow-Aufgaben" enthält einen Audit-Pfad von Prozessinstanz-Nachrichten, die in der CA Process Automation-Aufgabenliste aufgeführt sind.

Hinweis: Wenn Sie die CA SDM-Schaltfläche "Vorgang anzeigen" oder CA Process Automation-Prozessinstanz-Nachrichten auswählen, dann fordert Sie das System zur Eingabe eines CA Process Automation-Benutzernamens und eines Kennworts für eine einzelne Browsersitzung auf. Nach der ersten Eingabeaufforderung werden Sie kein weiteres Mal aufgefordert, bis der CA SDM-Browser beendet wird.

Erstellen einer Prozessdefinition

Wenn Sie die Prozessdefinition erstellen, füllen Sie CA Process Automation mit Inhalt aus, der in CA SDM angezeigt werden soll. Sie verwenden den grafischen Prozessentwickler CA Process Automation zum Erstellen, Testen und Einchecken einer Prozessdefinition. Über CA SDM können Sie auch Makros zum Initiieren des CA Process Automation-Vorgangs erstellen.

Hinweis: Weitere Informationen zum Erstellen von CA Process Automation-Makros finden Sie in der *Online-Hilfe*.

So erstellen Sie eine Prozessdefinition in CA Process Automation:

1. Melden Sie sich beim CA Process Automation-Client als Administrator an.
2. Verwenden Sie den grafischen Prozessentwickler CA Process Automation zum Erstellen, Testen und Einchecken einer Prozessdefinition. Wenn Sie mit der Prozessdefinition arbeiten, benutzen Sie die Anweisungen in der CA Process Automation-Benutzerdokumentation.

Hinweis: Wenn Sie versäumen, die Prozessdefinition einzuchecken, bevor Sie versuchen, sie zu benutzen, kann der Workflow nicht richtig in CA SDM funktionieren.

Die folgenden Elemente der Prozessdefinition sind in CA SDM verfügbar:

Prozessname

Wird auf den Seiten "Anfragebereich", "Change-Kategorie" und "Issue - Detail" angezeigt. Der Prozessname wird auch auf der Registerkarte "Workflow-Aufgaben" eines Tickets angezeigt. Der Prozessname beschreibt die Prozessdefinition zu CA SDM für Analysten und andere Benutzer, die Tickets verwalten.

Referenzpfad des Vorgangs

Wird auf den Seiten "Anfragebereich", "Change-Kategorie" und "Issue - Detail" angezeigt. Der Referenzpfad des Vorgangs wird auch auf der Registerkarte "Ticket-Workflow-Aufgabe" angezeigt. Der Referenzpfad des Vorgangs kann nützlich sein, um den Zweck des Prozesses Endbenutzern zu beschreiben. Zum Beispiel ist "/Prozesse/Genehmigung" nicht hilfreich. Stattdessen beschreibt ein Referenzpfad wie "/Bürobedarf/ Genehmigungen/Über-200-Euro" den Workflow zum Verwalten von Bestellungen, die 200 Euro übersteigen.

Prozessprotokollmeldungen

Wird auf der CA SDM-Registerkarte "Ticket-Workflow-Aufgabe" angezeigt. Standardmäßig wird ein Datensatz von Aktivitäten mit der Prozessinstanz gespeichert. Prozessprotokollmeldungen weisen die Kategorie "Prozess" auf. Ein Prozessentwickler kann benutzerdefinierte Meldungen erstellen, die auf der Registerkarte "Workflow-Aufgaben" eines CA SDM-Tickets angezeigt werden sollen.

Hinweis: Informationen zum Konfigurieren der Option "caextwf_log_categories" zum Verwalten von Protokollmeldungen finden Sie im *Implementierungshandbuch*.

Erstellen von Startauftragsformularen

Wenn Sie ein Startauftragsformular erstellen, verknüpfen Sie es mit der Prozessdefinition und checken es ein. Sie nehmen die entsprechenden Schlüsselwörter in die Eigenschaften des Startauftragsformulars auf. Wenn das entsprechende Schlüsselwort in den Eigenschaften des Startauftragsformulars fehlt, werden das Startauftragsformular und die zugehörige Prozessdefinition in CA SDM nicht angezeigt.

So erstellen Sie ein Startauftragsformular:

1. Melden Sie sich beim CA Process Automation-Client als Administrator an.
2. Öffnen Sie die CA Process Automation-Bibliothek, und navigieren Sie zum Pfad des Startauftragsformulars.

Das Startauftragsformular wird im rechten Fenster der CA Process Automation-Bibliothek angezeigt.
3. Wählen Sie das Startauftragsformular in der Liste aus.

Es wird ein Kontextmenü angezeigt.
4. Wählen Sie "Eigenschaften" aus.

Die Seite "Bibliothek-Objekteigenschaften" wird angezeigt.
5. (Optional) Klicken Sie auf die Registerkarte "Allgemein", und ändern Sie die Beschreibung für das Startauftragsformular. Fügen Sie eine Beschreibung hinzu, die dem CA SDM-Administrator Aufschluss über die genaue Verwendungsweise des Startauftragsformulars und der zugehörigen Prozessdefinition gibt.
6. Klicken Sie auf die Registerkarte "Schlüsselwörter".

Die Registerkarte "Schlüsselwörter" ist nun aktiv.
7. Klicken Sie auf das Symbol "ab+".

Es wird eine Zeile zur leeren Liste hinzugefügt.

8. Klicken Sie auf die Zeile.

Ein blinkender Cursor hebt die Zeile hervor und zeigt an, dass die Zeile für Eingaben bereit ist.

9. Geben Sie einen der folgenden Werte ein, um ein Schlüsselwort mit dem entsprechenden Ticketbereich bzw. der Kategorie zu verknüpfen. Um z. B. ein Startauftragsformular für den CA SDM-Request-Bereich verfügbar zu machen, geben Sie das Schlüsselwort "pcat" ein.

Ticket	Zu verwendendes Schlüsselwort
Request-Bereich	pcat
Änderungskategorie	chgcat
Issue-Kategorie	isscat

10. Fügen Sie für jedes anwendbare Schlüsselwort eine Zeile zur Liste hinzu. Damit z. B. das Startauftragsformular sowohl in Request-Bereichen als auch in Change-Kategorien angezeigt wird, fügen Sie eine Zeile für das Schlüsselwort "chgcat" und eine andere Zeile für das Schlüsselwort "pcat" ein.

11. Klicken Sie auf "OK".

CA Process Automation speichert die Schlüsselwörter und Beschreibung und schließt das Dialogfeld "Bibliothek-Objekteigenschaften".

12. Checken Sie das Startauftragsformular ein.

Hinweis: Wenn Sie das Startauftragsformular nicht einchecken, wird es nicht in CA SDM angezeigt.

Die CA Process Automation-Startauftragsformularinformationen werden in der CA SDM-Startauftragsformular-Liste angezeigt. Der CA SDM-Administrator kann das CA SDM-Startauftragsformular mit der Prozessdefinition auf der Seite "Request-Bereich", "Change-Kategorie" oder "Issue-Kategorie - Detail" verknüpfen.

Die folgenden Startauftragsformularelemente werden in CA SDM angezeigt:

Startauftragsformular-Name

Wird auf den Seiten "Request-Bereiche", "Change-Kategorien" und "Issue-Kategorien" angezeigt.

Startauftragsformular-Referenzpfad

Wird auf den Seiten "Request-Bereiche", "Change-Kategorien" und "Issue-Kategorien" angezeigt.

Startauftragsformular-Beschreibung

Wird auf den Seiten "Request-Bereiche", "Change-Kategorien" und "Issue-Kategorien" angezeigt. Der Text in diesem Feld beschreibt, inwieweit das Startauftragsformular für die Auswahl für einen bestimmten Request-Bereich, eine Change-Kategorie oder eine Issue-Kategorie geeignet ist.

Anhängen von CA Process Automation-Prozessdefinitionen

Wenn Sie eine CA Process Automation-Prozessdefinition an einen CA SDM-Ticketbereich oder eine Kategorie anhängen, erstellen Sie eine statische Verbindung zwischen einem CA SDM-Ticketbereich oder einer Kategorie und einer CA Process Automation-Prozessdefinition.

Wenn ein CA SDM-Anwender ein Ticket erstellt oder bearbeitet und eine Ticket-Kategorie auswählt, wird die verknüpfte CA Process Automation-Prozessdefinition als eine Prozessinstanz gestartet. Relevante Informationen zur Prozessinstanz werden auf der Registerkarte "Workflow-Aufgaben" im Ticket angezeigt.

So hängen Sie eine Prozessdefinition an:

1. Wählen Sie auf der Registerkarte "Administration" die Option "Service Desk" aus.
2. Navigieren Sie zu den Ticketbereichen oder Kategorien.

Die entsprechende Bereichs- bzw. Kategorielliste wird angezeigt.

3. Erstellen oder bearbeiten Sie einen Ticketbereich oder eine Kategorie.

Die Seite "Aktualisierung" wird angezeigt.

4. Klicken Sie auf die Registerkarte "Workflow".

Sind die CA Process Automation-Optionen im CA SDM-Optionsmanager installiert, ist die Schaltfläche "CA IT-PAM verwenden" auf der Registerkarte "Workflow" verfügbar.

5. Klicken Sie auf "CA IT-PAM verwenden".

Die Liste der CA IT PAM-Startauftragsformulare wird angezeigt. Jede Zeile in der Liste stellt ein CA Process Automation-Startauftragsformular dar.

Hinweis: Sie können CA Process Automation, CA Workflow oder den internen Workflow von CA SDM zur Verwaltung verschiedener Ticketbereiche oder Kategorien verwenden. Allerdings kann für eine einzelne Kategorie nur jeweils ein Workflow-Tool verwendet werden.

6. Klicken Sie auf den Wert in der Spalte "Name", um die mit diesem Startauftragsformular verknüpfte Prozessdefinition auszuwählen.

Die Liste der CA IT PAM-Startauftragsformulare wird geschlossen. Der Name und der Referenzpfad der Prozessdefinition werden auf der Registerkarte "Workflow" angezeigt.

7. Klicken Sie auf "Speichern".

Das System speichert die Prozesseinstellungen. Das nächste Ticket, das ein Anwender im festgelegten Ticketbereich oder in der festgelegten Kategorie erstellt, hängt den Workflow automatisch an und erstellt eine Prozessinstanz. Die Registerkarte "Workflow-Aufgaben" des Tickets enthält eine Zusammenfassung der Prozessinstanzinformationen. Ein Anwender kann durch Klicken auf "Prozess anzeigen" auf der Registerkarte "Workflow-Aufgaben" auf weitere Informationen zur Prozessinstanz zugreifen.

Freigegebene Codes

In CA SDM benutzen verschiedene Arten von Tickets bestimmte zugrunde liegende Codes gemeinsam, wie zum Beispiel Codes für Priorität, Schweregrad, Auswirkung und Dringlichkeit. Requests und Changes haben einige Codes gemeinsam, und alle Arten von Tickets haben andere Codes gemeinsam.

Betrachten Sie die folgenden Informationen zu freigegebenen Codes:

- Sie werden standardmäßig numerisch angeordnet.
- Sie können die Codes anpassen.
- Sie können keine freigegebenen Codes hinzufügen oder löschen.
- Sie können Codes für Auswirkung, Priorität, Schweregrad und Dringlichkeit verwenden.

Richten Sie nach Service Desk-Modell die folgenden Codes ein:

Freigegebene Codes	Beschreibung
Priorität	Muss für alle Service Desk-Modelle eingerichtet sein.
Relevanz	Muss für alle internen und kombinierten Service Desk-Modelle eingerichtet sein.
Impact	Muss für alle internen und kombinierten Service Desk-Modelle eingerichtet sein.
Urgency	Muss für alle internen und kombinierten Service Desk-Modelle eingerichtet sein.

Hinweis: Ausführliche Informationen zum Anpassen dieser Codes mit Hilfe der Verwaltungsfunktion der Web-Schnittstelle finden Sie in der *Online-Hilfe*.

Weitere Informationen:

[Prioritätscodes](#) (siehe Seite 418)

[Schweregrad-Codes](#) (siehe Seite 418)

[Auswirkungscodes](#) (siehe Seite 419)

[Dringlichkeitscodes](#) (siehe Seite 419)

Prioritätscodes

Prioritätscodes geben die Rangfolge an, in der der Service Desk auf Tickets antworten soll (d. h., sie geben den Grad der Aufmerksamkeit an, den ein Ticket erhalten soll). Auf Prioritätscodes wird in Anfragen, Changes und Issues verwiesen. Daher gelten sie für alle Service Desk-Modelle.

Sie können Prioritäten benutzen, um Tickets manuell oder automatisch durch Überwachen von Ereignissen zu eskalieren. In vielen Service Desk-Installationen werden Prioritätscodes im Scoreboard verwendet, um Analysten den Echtzeitstatus ihrer Anfragen und Changes anzuzeigen.

Sie können einem Prioritätscode einen Dienstyp zuweisen, der anschließend bei Angabe des Prioritätscodes Tickets automatisch zugewiesen wird. Auf diese Weise können Sie einem Ticket eine bestimmte Dienstebene auf der Basis der zugewiesenen Priorität zuordnen. Zum Beispiel wird der systemdefinierte Servicetyp, eine Lösung in 4 Stunden, automatisch der Priorität 1 zugeordnet. Tickets, denen eine Priorität von 1 zugeordnet ist, wird automatisch dieser Servicetyp zugeordnet, einschließlich aller Servicetypereignisse, die dem Servicetyp zur Lösung in 4 Stunden zugeordnet sind.

Weitere Informationen:

[Service Level Agreements \(Dienstverträge\)](#) (siehe Seite 266)

Schweregrad-Codes

Schweregradcodes geben den Umfang des Schadens an Ausrüstungen an, die von einem Request betroffen sind. Auf Schweregradcodes wird nur in Requests verwiesen. Daher gelten sie nur für das interne und das kombinierte Service Desk-Modell.

Hinweis: Schweregrad wird häufig als Synonym für Priorität verwendet. Einige Standorte verwenden nur die Priorität und ignorieren den Schweregrad gänzlich. Wenn Sie unterscheiden möchten, wie ernst ein Problem auf einer technischen Ebene (Schweregrad) ist und wie schnell es gelöst werden soll (Priorität), können Sie Codes für Schweregrad und Priorität verwenden.

Auswirkungscodes helfen dabei, die Incident-Priorität zu berechnen.

Auswirkungscodes

Auswirkungscodes messen die Wichtigkeit eines Tickets für den Betrieb des Systems. Wenn zum Beispiel ein Change den Betrieb des gesamten Systems beeinflussen kann, wird ihm eine hohe Auswirkung zugewiesen. Auf Auswirkungscodes wird nur in Anfragen und Changes verwiesen. Daher gelten sie nur für das interne und das kombinierte Service Desk-Modell.

Hinweis: Auswirkungs- und [Dringlichkeitscodes](#) (siehe Seite 419) sind einander ähnlich, dienen aber spezifischen Zwecken.

Dringlichkeitscodes

Dringlichkeitscodes messen die Wichtigkeit der Anfrage für die Benutzer des Systems (d. h., sie geben die Wichtigkeit der Anfrage für die gesamte Produktionsumgebung an). Wenn eine Anfrage den Auftrag des Unternehmens gefährden könnte, kann der Dringlichkeits-Code zum Beispiel ein Wert von 5-Sofort sein. Auf Dringlichkeitscodes wird nur in Anfragen verwiesen. Daher gelten sie nur für das interne und das kombinierte Service Desk-Modell.

Dringlichkeitscodes und Auswirkungscodes dienen speziellen Zwecken, werden aber oft verwechselt, weil sie zusammenfallen. Zum Beispiel kann eine Anfrage zur Meldung eines Feuers in einer kritischen Datenzentrale eine Auswirkung auf 3-Einzelne-Gruppe und eine Dringlichkeit von 5-Sofort haben. Diese Codes gelten, weil sich das Feuer auf mehr als eine Gruppe auswirkt, aber nicht notwendigerweise auf die ganze Organisation. Da die Datenzentrale für Operationen kritisch ist, macht die Dringlichkeit ein sofortiges Eingreifen notwendig.

Statuscodes

Statuscodes werden zur Verfolgung des Status eines Elements verwendet. Trennen Sie Anfragen zum Verfolgen von Statuscodes, Changes, Issues und Workflow-Aufgaben. Für jeden Fall gibt es vordefinierte Statuscodes, die Sie verwenden können, wenn sie Ihren Bedürfnissen entsprechen. Andernfalls können Sie die vordefinierten Statuscodes ändern oder neue Statuscodes definieren, die für Ihren Standort spezifisch sind. Je nach Service Desk-Modell müssen Sie die folgenden Codes einrichten:

Statuscodes	Beschreibung
Request	Muss für alle internen und kombinierten Service Desk-Modelle eingerichtet sein.
Change	Muss für alle internen und kombinierten Service Desk-Modelle eingerichtet sein.

Statuscodes	Beschreibung
Issue	Muss für alle externen und kombinierten Service Desk-Modelle eingerichtet sein.
Aufgabe	Muss für alle Service Desk-Modelle eingerichtet sein.

Mit Statuscodes können Analysten Informationen auf der Basis des Status sortieren und auswählen und somit den Fortschritt genau verfolgen. Wie sorgfältig Sie die Statuscodes definieren, bestimmt, wie genau die Analysten den tatsächlichen Status eines Elements beschreiben können.

Sie können einen Statuscode als aktiv oder inaktiv kennzeichnen. Wenn Sie einen Statuscode als inaktiv kennzeichnen, steht er den Analysten nicht mehr für die Verwendung zur Verfügung, bleibt aber für die spätere Verwendung verfügbar (d. h., er wird nicht aus der Datenbank gelöscht). Wenn Sie später entscheiden, den Statuscode zu verwenden, müssen Sie ihn nur aufrufen und als aktiv kennzeichnen.

Hinweis: Dieselben Bereichsdefinitionen stehen für Anfrage-, Incident- und Problem-Tickets zur Verfügung. Auf der Registerkarte "Administration" werden diese Bereiche als Anfrage-/Incident-/Problembereiche bezeichnet. Sie werden hier einfach kurz als "Anfragebereiche" bezeichnet.

Anfragestatuscodes

Die folgende Tabelle beschreibt die vordefinierten Statuscodes für Anfrage-Tickets.

Anfragestatuscode	Beschreibung
Bestätigt	Der Empfang einer Anfrage wurde bestätigt.
Geschlossen	Eine Anfrage wurde vollständig gelöst.
Geschlossen - Ungelöst	Eine Anfrage wurde geschlossen, muss aber noch gelöst werden.
Behebung in Arbeit	Eine Anfrage ist offen, und die Behebung steht aus.
Halten	Die Servicetypereignisse für die Anfrage sind im Haltezustand.
Öffnen	Eine Anfrage wurde definiert und dient zur Überwachung und Verwaltung ihres Abschlusses.
Problem geschlossen	Ein Issue ist vollständig geschlossen.
Problem behoben	Eine Problemanfrage wurde behoben, aber noch nicht geschlossen.
Offene Probleme	Eine Anfrage wurde als Problem identifiziert.

Anfragestatuscode	Beschreibung
Nachforschen	Eine Anfrage ist offen, und zusätzliche Nachforschungen und Analysen stehen aus.
Vorgang wird bearbeitet	Die Problembehebung einer Anfrage wird durchgeführt.

Wenn Ihr Standort eine andere Terminologie zur Identifikation des Anfragestatus verwendet, sollten Sie Statuscodes definieren, die Ihren Anfragen entsprechen, und die vordefinierten Statuscodes ignorieren oder die Definitionen entsprechend ändern. Sie können zum Beispiel folgende zusätzliche Anfragestatuscodes definieren:

Anfragestatuscode	Beschreibung
Duplikat	Anfragen, die geöffnet wurden, jedoch ein Duplikat einer vorhandenen Anfrage für einen anderen Benutzer sein können.
Notfall	Kritische Anfragen, die sofort bearbeitet werden müssen.
Bericht	Anfragen, die gelöst und geschlossen sind, über die jedoch auf Managementebene berichtet werden soll.
Test	Anfragen, die gelöst sind, jedoch vor Abschluss eine Woche lang getestet werden sollen.

Statuscodes von Changes

Die folgende Tabelle beschreibt die vordefinierten Statuscodes für Change-Tickets.

Statuscode von Changes	Beschreibung
Genehmigung in Arbeit	Ein Change ist offen und die Genehmigung steht aus.
Genehmigt	Ein Change wurde geschlossen.
Abgebrochen	Ein Change wurde abgebrochen.
Geschlossen	Ein Change wurde geschlossen.
Halten	Die Servicetypereignisse für den Change sind im Haltezustand.
Implementierung in Arbeit	Ein Change wird implementiert.
Öffnen	Ein Dienstauftrag wurde in einem Change definiert, und der Change wird zur Überwachung und Verwaltung seiner Fertigstellung verwendet.
Abgelehnt	Ein Change wurde abgelehnt.
Gelöst	Ein Change wurde geschlossen.

Statuscode von Changes	Beschreibung
RFC	Eine Change-Anfrage wurde gesendet.
Unterbrochen	Beendet Workflow-Aufgaben für einen Change.
Überprüfung in Arbeit	Ein Change wird überprüft.
Rückgängig gemacht	Ein bereits implementierter Change wurde rückgängig gemacht.
Implementiert	Ein Change wurde implementiert.

Wenn Ihr Standort eine andere Terminologie zur Identifikation des Status eines Change verwendet, sollten Sie Statuscodes definieren, die Ihren Bedürfnissen entsprechen, und die vordefinierten Statuscodes ignorieren oder die Definitionen entsprechend ändern. Sie können zusätzliche Statuscodes von Changes definieren, zum Beispiel ähnliche wie die in der folgenden Tabelle aufgeführten:

Benutzerdefinierter Anfragestatuscode	Beschreibung
Duplikat	Changes, die geöffnet wurden, jedoch ein Duplikat eines vorhandenen Change für einen anderen Benutzer sein können.
Notfall	Kritische Changes, die sofort bearbeitet werden müssen.
Bericht	Changes, die abgeschlossen und geschlossen sind, über die jedoch auf Managementebene berichtet werden soll.

Schließungscodes

Mit Schließungscodes definieren Sie das Endergebnis von Changes, z. B. erfolgreich oder erfolglos. Schließungscodes können Sie auf einem Change manuell bzw. als Teil der Aktivität "Status aktualisieren" festlegen, wenn der Status geschlossen, fertig oder gelöst lautet.

Hinweis: Weitere Informationen zum Erstellen oder Definieren von Schließungscodes und Details zu den Optionen *require_closure_code* und *den force_closure_code* finden Sie in der *Online-Hilfe*.

Statuscodes von Issues

Die folgende Tabelle beschreibt die vordefinierten Statuscodes für Issue-Tickets.

Statuscode von Issues	Beschreibung
Genehmigung in Bearbeitungsstatus	Ein Issue ist offen und die Genehmigung steht aus.

Statuscode von Issues	Beschreibung
Abgebrochen	Ein Issue wurde abgebrochen.
Geschlossen	Ein Issue wurde abgeschlossen.
Halten	Die Servicetypereignisse für das Issue sind im Haltezustand.
Implementierung in Arbeit	Ein Issue wird implementiert.
Öffnen	Ein Issue wurde definiert und ist offen, so dass sie bis zu ihrer Lösung überwacht und verwaltet werden kann.
Unterbrochen	Beendet Workflow-Aufgaben für ein Issue.
Verhandlung im Gange	Eine Verhandlung mit einem Kunden zu diese Issue ist im Gange.
Überprüfung in Bearbeitungsstatus	Ein Issue wird überprüft.

Wenn Ihr Standort eine andere Terminologie zur Identifikation des Status eines Issue verwendet, sollten Sie Statuscodes definieren, die Ihren Bedürfnissen entsprechen, und die vordefinierten Statuscodes ignorieren oder die Definitionen entsprechend ändern. Sie möchten zum Beispiel zusätzliche Issue-Statuscodes wie folgende definieren:

Benutzerdefinierter Issue-Statuscode	Beschreibung
Duplikat	Issues, die geöffnet wurden, jedoch ein Duplikat eines vorhandenen Issue für einen anderen Benutzer sein können.
Notfall	Kritische Issues, die sofort bearbeitet werden müssen.
Bericht	Issues, die abgeschlossen und geschlossen sind, über die jedoch auf Managementebene berichtet werden soll.

Aufgabenstatuscodes

Aufgabenstatuscodes beschreiben die verschiedenen möglichen Status einer Workflow-Aufgabe. Jede Aufgabe in einem Issue- oder Change-Workflow hat ihren eigenen Status, separat vom Ticketstatus. Mit Hilfe von Workflow-Aufgaben kann der Analyst verfolgen, wie lange es dauert, um einzelne Aufgaben innerhalb eines Tickets abzuschließen.

Die folgende Tabelle beschreibt die vordefinierten Statuscodes für Workflow-Aufgaben.

Aufgabenstatuscode	Beschreibung
Genehmigen	Die Aufgabe wurde genehmigt.

Aufgabenstatuscode	Beschreibung
Abgebrochen	Die Aufgabe wurde abgebrochen, und keine weiteren Aktualisierungen sind möglich.
Abgeschlossen	Aufgabe ist abgeschlossen.
Ausstehend	Die Aufgabe wurde gestartet.
Ablehnen	Die Aufgabe wurde abgelehnt.
Erneut öffnen	Die Aufgabe wurde erneut-geöffnet.
Erneut geöffnet – Warten	Eine vorherige Aufgabe wurde erneut geöffnet.
Überspringen	Die Aufgabe wird übersprungen.
Warten	Die Aufgabe wurde nicht gestartet.

Wenn Ihr Standort eine andere Terminologie zur Identifikation des Status einer Workflow-Aufgabe verwendet, sollten Sie Statuscodes definieren, die Ihren Bedürfnissen entsprechen, und die vordefinierten Statuscodes ignorieren oder die Definitionen entsprechend ändern.

Sie können jedem Aufgabenstatuscode ein bestimmtes Verhalten zuweisen, das stattfindet, wenn die Aufgabe diesen Status erreicht. Dadurch können Sie wesentlich mehr Informationen über den Fortschritt einer Aufgabe liefern. Sie können außerdem die Akkumulierungsfunktion verwenden, um die Zeit und die Kosten zur Vollendung des Tickets zu verfolgen.

Aufgabentypen

Aufgabentypen helfen, zusammen mit Aufgabenstatuscodes, das Verhalten bestimmter Workflow-Aufgaben zu bestimmen. Um kennzeichnende Eigenschaften für jeden Aufgabentyp zu erstellen, können Sie Aufgabenstatuscodes angeben oder bestimmte Status verwenden.

Da sowohl Changes als auch Issues Workflow-Aufgaben verwenden, müssen Sie Aufgabentypen für alle Service Desk-Modelle einrichten. Mit Hilfe der Aufgabenstatuscodes wird das mit jeder Aufgabe verbundene Verhalten identifiziert. Zum Beispiel kann der Aufgabentyp "Genehmigung" so eingerichtet werden, dass er "Genehmigen", "Ablehnen", "In Bearbeitung" und "Warten" als verfügbare Status zulässt. Wenn der Aufgabentyp "Genehmigung" dann den Status "In Bearbeitung" annimmt, können Sie einem bestimmten Manager, Analysten usw. eine Benachrichtigung senden.

Sie können einen Aufgabentyp als aktiv oder inaktiv kennzeichnen. Wenn Sie einen Aufgabentyp als inaktiv kennzeichnen, steht er den Analysten nicht mehr für die Verwendung zur Verfügung, bleibt aber für die spätere Verwendung verfügbar (d. h. er wird nicht aus der Datenbank gelöscht). Wenn Sie später entscheiden, den Aufgabentyp zu verwenden, markieren Sie ihn wieder als aktiv.

Hinweis: Sie können die vordefinierten Aufgabentypen auf der Seite "Aufgabentyp - Liste" der administrativen Funktion der Web-Schnittstelle anzeigen.

Beispiel: Aufgabenstatuscodes

Die folgende Tabelle enthält einige Beispielstatuscodes:

Aufgabenstatuscode	Beschreibung
Genehmigung	Ticket genehmigen oder ablehnen
Ende der Gruppenaufgaben	Ende der Gruppenaufgaben
Beginn der Gruppenaufgaben	Beginn der Gruppenaufgaben
Startgenehmigung	Genehmigung zum Starten des Tickets

In diesem Beispiel definieren "Gruppenaufgabe - Start" und "Gruppenaufgabe - Ende" eine Gruppe von Aufgaben in einer Issue- oder Change-Kategorie, die abgeschlossen werden müssen. Aufgaben in der Gruppe können in einer beliebigen Reihenfolge ausgeführt werden. Nachdem die Gruppenstartaufgabe den Status "In Bearbeitung" (gestartet) hat, werden alle Aufgaben innerhalb der Gruppe ebenfalls in diesen Status versetzt.

Hinweis: Weitere Informationen zum Verwenden von Aufgabentypen finden Sie in der *Online-Hilfe*.

Durch Auswahl einer oder mehrerer Incident-Flags können Analysten den betreffenden Incident verfolgen. Die von Analysten angegebenen Informationen liefern Ihrer Organisation die Metriken zu Incidents für Berichte. Analysten können z. B. angeben, dass ein Incident falsch zugewiesen wurde. Wenn ein Bericht eine große Anzahl von falsch zugewiesenen Tickets enthält, weiß Ihre Organisation, dass Zuweisungen angepasst werden müssen.

Analysten können z. B. Informationen angeben, die Ihre Organisation bei folgenden Vorgängen unterstützen:

- Verbessern der Reaktionsfähigkeit im Rahmen des SLA und Abschluss auf niedrigerer Ebene innerhalb der Support-Organisation

- Identifizieren Sie Tickets, die falsch zugewiesen sind.
- Angeben der Verwendung eines Remote Control-Tools zur Lösung des Tickets

Installieren Sie die Optionsmanager-Option `efficiency_tracking`, so dass Analysten die Nachverfolgungsoptionen verwenden können, die auf der Effizienznachverfolgungs-Registerkarte auf Incident-Detailseiten angezeigt werden.

Hinweis: Weitere Informationen über die Incident-Nachverfolgung finden Sie in der *Online-Hilfe*.

Installieren der Incident-Nachverfolgung

Sie können eine Option installieren, mit der Analysten einen Incident durch das Setzen bestimmter Flags nachverfolgen können. Die von Analysten angegebenen Informationen liefern Ihrer Organisation die Metriken zu Incidents für Berichte. Nachdem Sie die Option installiert haben, werden die Flags zur Nachverfolgung auf der Registerkarte "Effizienznachverfolgung" auf den Detailseiten von Incidents angezeigt.

So installieren Sie die Incident-Nachverfolgung:

1. Wählen Sie auf der Registerkarte "Administration" die Option "Optionsmanager" > "Anfragemanager".

Das Fenster "Optionen - Liste" wird angezeigt.

2. Klicken Sie auf "efficiency_tracking".

Die Seite "Optionen - Details" für "efficiency_tracking" wird mit den jeweiligen Standardwerten angezeigt.

3. Klicken Sie auf "Bearbeiten".

Die Seite "Optionen aktualisieren" für "efficiency_tracking" wird mit den jeweiligen Standardwerten angezeigt. Sie können die Beschreibung bearbeiten.

4. Klicken Sie auf „Installieren“.

Die Seite mit den Optionsdetails zu "efficiency_tracking" wird angezeigt.

5. Klicken Sie auf "Fenster schließen".

Die Incident-Nachverfolgung ist installiert. Die Registerkarte "Effizienznachverfolgung" wird jedoch nicht auf den Incident-Detailseiten angezeigt.

6. Starten Sie CA SDM neu.

Die Registerkarte "Effizienznachverfolgung" wird auf den Detailseiten für Incidents angezeigt.

Request-/Incident-/Problembereiche

Anfragebereiche definieren die logischen Gruppen, in denen Anfrage-, Incident- und Problem-Tickets kategorisiert werden können. Zum Beispiel können Tickets, die zu einer Anwendung gehören, einem vordefinierten Anwendungsbereich zugeordnet werden. Wenn ein Analyst einem Anfragebereich ein Ticket zuweist, werden alle Informationen, die Sie mit dem Anfragebereich verknüpft haben, automatisch auf dem Ticket eingegeben. Wenn Sie zum Beispiel einen Servicetyp angeben, wird er mit dem Ticket und allen zugehörigen Servicetypereignissen verbunden.

Hinweis: Dieselben Bereichsdefinitionen stehen für Anfrage-, Incident- und Problem-Tickets zur Verfügung. Auf der Registerkarte "Administration" der CA SDM-Web-Schnittstelle werden diese Bereiche als Anfrage-/Incident-/Problembereiche bezeichnet. Sie werden hier einfach kurz als "Anfragebereiche" bezeichnet.

Sie können den Status eines beliebigen Anfragebereichs auf aktiv oder inaktiv setzen. Wenn Sie einen Anfragebereich auf inaktiv setzen, steht er Analysten nicht mehr zur Verfügung, wird aber nicht aus der Datenbank gelöscht. Wenn Sie später beschließen, den Anfragebereich zu verwenden, müssen Sie den Status nur zurück auf aktiv setzen.

Anfragebereiche ermöglichen Folgendes:

- Angeben von Standardwerten für die Gruppe und die Felder für Zuständige auf Tickets
- Automatisches Verknüpfen von Tickets mit einer Serviceebene, indem Sie dem Anfragebereich einen Standardservicetyp zuweisen
- Verknüpfen einer Umfrage mit einem Anfragebereich
- Auswählen und Melden von Tickets nach Bereichen durch Definieren Ihrer eigenen benutzerdefinierten Anfragebereiche Studieren von Anfragetrends und Analysieren von Problemursachen Isolieren bestimmter Anfragebereiche, um aussagekräftigere Untersuchungen und Analysen zu erzielen

Folgende vordefinierte Anfragebereiche werden mit CA SDM installiert:

- Anwendungen
- E-Mail
- Hardware

- Netzwerke
- Drucker
- Software

Software ist in mehrere verschiedene Anfragebereiche unterteilt.

Hinweis: Informationen zur Definition und Bearbeitung von Anfragebereichen finden Sie in der *Online-Hilfe*.

Weitere Informationen:

[Anfrage-/Incident-/Problembereich - Eigenschaften](#) (siehe Seite 428)

[Definieren von Anfrage/Zwischenfall-/Problembereichen für Self-Service](#) (siehe Seite 430)

Anfrage-/Incident-/Problembereich - Eigenschaften

Eigenschaften dienen zum Hinzufügen benutzerdefinierter Attribute oder Qualitäten zu einem bestimmten Anfragebereich. Wenn Sie zu einem Anfragebereich Eigenschaften hinzugefügt haben und ein Analyst diesem Kategorie ein Ticket zuweist, werden die verknüpften Eigenschaften automatisch auf der Registerkarte "Eigenschaften" des Tickets angezeigt. So können Sie zum Beispiel dem vordefinierten E-Mail-Anfragebereich Eigenschaften hinzufügen, um den E-Mail-Server oder die Postfachgröße anzugeben.

Beim Definieren von Eigenschaften können Sie angeben, ob ein Wert erforderlich oder optional ist. Für [Eigenschaften mit einem obligatorischen Wert](#) (siehe Seite 429) müssen Benutzer einen Wert eingeben (oder den Standardwert akzeptieren), bevor sie das Ticket speichern können.

Die Option "keep_tasks" legt fest, was geschieht, wenn Sie ein vorhandenes Ticket einem anderen Anfragebereich zuweisen:

- Wenn "keep_tasks" nicht installiert ist, werden bestehende Eigenschaften (und Workflow-Aufgaben) aus dem Ticket entfernt und mit dem neuen Anfragebereich verknüpfte Eigenschaften oder Aufgaben hinzugefügt.
- Wenn "keep_tasks" installiert ist, werden bestehende Eigenschaften und Aufgaben auf dem Ticket behalten, und alle Eigenschaften oder Aufgaben, die mit einem neuen Anfragebereich in Zusammenhang stehen, werden hinzugefügt.

Hinweis: Ausführliche Anweisungen zum Hinzufügen von Eigenschaften zu einem Anfragebereich und zum Definieren von Eigenschaftsvalidierungsregeln finden Sie in der *Online-Hilfe*.

Eigenschaftsvalidierungsregeln

Sie können Validierungsregeln definieren, um die Eigenschaftswerte zu beschränken, die Benutzer in einen vordefinierten Satz von auswählbaren Werten eingeben können. Wenn Sie zum Beispiel eine Eigenschaft namens "Betriebssystem" definiert haben, können Sie die Validierungsregel als Dropdownliste definieren, die die Optionen "Windows", "UNIX" und "Linux" enthält.

Ohne Validierungsregeln definierte Eigenschaften werden dem Benutzer als formatfreie Textfelder dargeboten, in die eine beliebige Textzeichenfolge eingegeben werden kann. Durch Validierungsregeln werden die Berichterstellung zu Bereichs- und Kategoriewerten vereinfacht und sind weniger fehleranfällig.

Hinweis: Eigenschaftsvalidierungsregeln sind wieder verwendbar. Sie sind nicht für eine bestimmte Eigenschaft vorgesehen. Sie können vorhandene Validierungsregeln auf Eigenschaften für Change-Kategorien, Issue-Kategorien oder Anfrage-/Incident-/Problembereiche anwenden.

Je nach der Art von Validierungsregel, die Sie für eine Eigenschaft konfiguriert haben, wird auf der Registerkarte "Eigenschaften" des Tickets eine der folgenden Steuerungen angezeigt, wenn der Benutzer der Kategorie oder dem Bereich, an der bzw. an dem diese Eigenschaft angehängt wurde, ein Ticket zuweist:

- **Textbearbeitungsfeld** - Es wurde keine Validierungsregel definiert, und kein Standardwert kann angegeben werden. Benutzer sollen Werte eingeben, die den von Ihnen bereitgestellten Beispielen folgen.
- **Kontrollkästchen** - Ein Kontrollkästchen mit zwei Zuständen wird auf der Registerkarte "Eigenschaften" angezeigt. Standardmäßig enthält das Kontrollkästchen kein Häkchen. Der Benutzer kann den Standardwert annehmen oder das Kontrollkästchen aktivieren. Für Kontrollkästchen, die ein Häkchen enthalten, wird auf der Detailseite des Tickets in der Wertspalte "Ja" angezeigt. Bei deaktivierten Kästchen wird in der Wertespalte "Nein" angezeigt.
- **Dropdown-Liste** - Auf der Registerkarte "Eigenschaften" wird eine Dropdown-Liste mit einem vordefinierten Satz Optionen angezeigt. Sofern Sie einen Standardwert definiert haben, wird dieser ausgewählt, wenn die Dropdown-Liste zum ersten Mal geöffnet wird. Die Option, die der Benutzer auswählt, wird in der Wertspalte auf der Detailseite des Tickets angezeigt.

Definieren von Anfrage/Zwischenfall-/Problembereichen für Self-Service

Mit der Option "Self-Service einschließen" können Sie festlegen, welche Anfragen-/Incident-/Problembereiche für Self-Service-Tickets eingeschlossen werden sollen. Sie können auch andere Self-Service-Symbole definieren als die, die für den Analysten angezeigt werden. Wenn das Ticket gespeichert wird, wird im Anfrage/Incident/Problembereichs-Feld das Self-Service-Symbol angezeigt. Wenn das Ticket in der Analystenschnittstelle angezeigt wird, wird für das Feld das normale Symbol angezeigt. Der Self-Service-Benutzer kann die Anfragebereiche nicht bearbeiten. Sie sind schreibgeschützt.

So legen Sie einen Self-Service-Bereich für Anfragen/Incidents/Probleme fest:

1. Wählen Sie auf der Registerkarte "Administration" die Option "Service Desk" > "Anfragen/Incidents/Probleme" > "Bereiche" aus.

Die Liste "Anfragen/Incidents/Problembereiche" wird angezeigt.

2. Wählen Sie "In Liste bearbeiten" aus.

Im oberen Teil der Seite werden die bearbeitbaren Felder angezeigt.

3. Öffnen Sie den gewünschten Anfrage-/Incident-/Problembereich zur Bearbeitung auf der Symbol-Liste (z. B. Hardware.pc.install).

4. Füllen Sie die folgenden Felder aus:

Self-Service einschließen

Definiert, ob dieser Anfrage-/Incident-/Problembereich in der Self-Service-Schnittstelle angezeigt wird.

Self-Service-Symbol

Definiert eine eindeutige Kennung für diesen Anfrage-/Incident-/Problembereich in der Self-Service-Schnittstelle.

Aktiv

Definiert, ob dieser Anfrage-/Incident-/Problembereich aktiv oder inaktiv ist.

Der Anfrage-/Incident-/Problembereich ist für Self-Service definiert.

5. Klicken Sie auf "Speichern".

Der aktualisierte Anfrage-/Incident-/Problembereich wird in der Liste der Anfrage-/Incident-/Problembereiche aufgeführt, sobald Sie diese Liste erneut öffnen.

Change- und Issue-Kategorien

Change-Kategorien und Issue-Kategorien definieren die logischen Einteilungen, in die Changes und Issues organisiert werden können.

Hinweis: Im Unterschied zu Anfrage-/Incident-/Problembereichen werden Change- und Issue-Kategorien separat verwaltet:

- Sie müssen Change-Kategorien für interne und kombinierte CA SDM-Modelle einrichten.
- Sie müssen Issue-Kategorien für externe und kombinierte CA SDM-Modelle einrichten.

Mithilfe von Kategorien können Sie Standardwerte für bestimmte Felder in Tickets angeben. Sie können Tickets automatisch mit einer Dienstebene verbinden, indem Sie Kategorien einen Standarddiensttyp zuweisen. Außerdem können Sie eine Umfrage mit einer Kategorie verbinden.

Für jede Kategorie können Sie Attribute oder Qualitäten angeben, die dem Ticket zugeordnet werden sollen. Außerdem können Sie einen Workflow erstellen, der alle einzelnen Aufgaben identifiziert, die zur Erfüllung des Tickets erforderlich sind. Durch Definieren von Verhalten, die mit den Workflow-Aufgaben verbunden sind, können Sie Mitarbeiter in Schlüsselpositionen benachrichtigen, wenn sich der Status von Aufgaben ändert oder wenn Aktivitäten zum Schließen des Tickets durchgeführt werden.

Wenn ein Analyst einer Kategorie ein Ticket zuweist, werden alle Informationen, die Sie mit der Kategorie verknüpft haben, automatisch auf dem Ticket eingegeben. Wenn Sie zum Beispiel einen Servicetyp angeben, wird er zusammen mit den zugehörigen Servicetypereignissen mit dem Ticket verbunden.

Hinweis: Weitere Informationen zur Definition und Bearbeitung von Kategorien finden Sie in der *Online-Hilfe*.

Weitere Informationen:

[Vordefinierte Change-Kategorien](#) (siehe Seite 432)

[Vordefinierte Issue-Kategorien](#) (siehe Seite 432)

[Regeln zum Ändern von Kategorien in einem Ticket](#) (siehe Seite 432)

[Kategorieeigenschaften](#) (siehe Seite 433)

[Definieren von Change-Kategorien und Issue-Kategorien für Self-Service](#) (siehe Seite 435)

Vordefinierte Change-Kategorien

Die folgenden Gruppen von vordefinierten Change-Kategorien werden mit CA SDM installiert:

- Hinzufügen
- Ändern
- Verschieben
- Retire

Hinweis: All diese Kategoriesätze sind in mehrere spezifische Kategorien unterteilt. Beispielsweise umfasst die Gruppe der Change-Kategorie Kategorien für die Änderung von Servern und Workstations.

Vordefinierte Issue-Kategorien

Die folgenden vordefinierten Issue-Kategorien werden mit CA SDM installiert:

- Hardware.pc.install
- Software.pc.install

Sie können den Status jeder beliebigen Kategorie auf "Aktiv" oder "Inaktiv" setzen. Wenn Sie eine Kategorie inaktiv machen, steht sie den Analysten zwar nicht mehr zur Verwendung zur Verfügung, wird aber nicht aus der Datenbank gelöscht. Wenn Sie später entscheiden, die Kategorie zu verwenden, ändern Sie ihren Status wieder in aktiv.

Regeln zum Ändern von Kategorien in einem Ticket

Die folgenden Regeln wirken sich nur auf Workflow-Aufgaben aus.

- Wenn die vorherige Kategorie CA Workflow oder Klassischer Workflow benutzt hat, und die neue Kategorie CA Process Automation benutzt, wird eine Verknüpfung der CA Process Automation-Prozessdefinition mit einem Workflow auf einem CA Process Automation-Server hergestellt.
- Wenn sowohl die alte als auch die neue Kategorie den CA SDM-Workflow verwendet, gelten die Regeln von früheren Versionen.

- Wenn die neue Kategorie CA Workflow oder CA Process Automation und die alte den CA SDM-Workflow benutzt, tritt Folgendes ein:
 - Alle unvollständigen und ausstehenden (Aufgaben, die aktualisiert werden können) Workflow-Aufgaben im Stil von CA SDM 6.0 erhalten unabhängig von der Option "KEEP_TASKS" den Status "Abgebrochen". Alle abgeschlossenen Workflow-Aufgaben bleiben bestehen, können aber nicht erneut geöffnet werden.
 - Alle unvollständigen und inaktiven Aufgaben (z. B. Aufgaben mit Wartestatus) werden gelöscht.
 - Die CA Workflow- oder CA Process Automation-Definition wird instanziiert.
- Wenn die neue Kategorie den CA SDM-Workflow und die alte Kategorie den CA Workflow-Workflow verwendet, tritt Folgendes ein:
 - Die CA Workflow- oder CA Process Automation-Instanz wird zwangsweise auf den Status "Beendet" gesetzt.
 - Die Workflow-Aufgaben der neuen Kategorie werden wie üblich hinzugefügt.
- Wenn sowohl die alte als auch die neue Kategorie CA Workflow benutzen, tritt Folgendes ein:
 - Wenn die alte und die neue Kategorie auf dieselbe Prozessdefinition verweisen, wird die aktive Instanz der vorherigen Kategorie fortgesetzt.
 - Wenn die alte und die neue Kategorie auf verschiedene Prozessdefinitionen verweisen, wird die alte Instanz auf "Beendet" gesetzt, und die Definition der neuen Kategorie wird instanziiert.

In einem CA SDM-Workflow kann ein Ticket mit einer aktiven CA Workflow-Instanz nicht geschlossen werden. Die Funktionen "Akkumulieren", "Beschleunigen" und "Aufgabe einfügen" sind für Tickets, die CA Workflow verwenden, deaktiviert.

Kategorieeigenschaften

Eigenschaften werden benutzt, um einer bestimmten Kategorie benutzerdefinierte Attribute oder Qualitäten hinzuzufügen. Wenn Sie einer Kategorie Eigenschaften hinzugefügt haben und ein Analyst dieser Kategorie ein Ticket zuweist, werden die verknüpften Eigenschaften automatisch auf der Registerkarte "Eigenschaften" des Tickets angezeigt.

Sie können zum Beispiel der vordefinierten Issue-Kategorie "Software.pc.install" Eigenschaften hinzufügen, um die Speichergröße, den Verarbeitertyp usw. anzugeben.

Beim Definieren von Eigenschaften können Sie angeben, ob ein Wert erforderlich oder optional ist. Für Eigenschaften mit einem obligatorischen Wert müssen Benutzer einen Wert eingeben (oder den Standardwert akzeptieren), bevor sie das Ticket speichern können.

Beibehalten von Kategorie-Eigenschaften

Die Option "keep_tasks" legt fest, was geschieht, wenn Sie ein vorhandenes Ticket einer anderen Kategorie zuweisen:

- Wenn "keep_tasks" nicht installiert ist, werden bestehende Eigenschaften und Workflow-Aufgaben aus dem Ticket entfernt und mit der neuen Kategorie verknüpfte Eigenschaften oder Aufgaben hinzugefügt.
- Wenn keep_tasks installiert ist, werden bestehende Eigenschaften und Aufgaben auf dem Ticket beibehalten. Die mit der neuen Kategorie verknüpften Eigenschaften oder Aufgaben werden hinzugefügt.

Hinweis: Ausführliche Anweisungen zum Hinzufügen von Eigenschaften zu einer Change- oder Issue-Kategorie und zum Definieren von Eigenschaftsvalidierungsregeln finden Sie in der *Online-Hilfe*.

Eigenschaftsvalidierungsregeln

Sie können Validierungsregeln definieren, um die Eigenschaftswerte zu beschränken, die Benutzer in einen vordefinierten Satz von auswählbaren Werten eingeben können. Wenn Sie zum Beispiel eine Eigenschaft namens "Betriebssystem" definiert haben, können Sie die Validierungsregel als Dropdownliste definieren, die die Optionen "Windows", "UNIX" und "Linux" enthält.

Ohne Validierungsregeln definierte Eigenschaften werden dem Benutzer als formatfreie Textfelder dargeboten, in die eine beliebige Textzeichenfolge eingegeben werden kann. Durch Validierungsregeln werden die Berichterstellung zu Bereichs- und Kategoriewerten vereinfacht und sind weniger fehleranfällig.

Hinweis: Eigenschaftsvalidierungsregeln sind wieder verwendbar. Sie sind nicht für ein bestimmte Eigenschaft vorgesehen. Sie können vorhandene Validierungsregeln auf Eigenschaften für Change-Kategorien, Issue-Kategorien oder Anfrage-/Incident-/Problembereiche anwenden.

Je nach der Art von Validierungsregel, die Sie für eine Eigenschaft konfiguriert haben, wird auf der Registerkarte "Eigenschaften" des Tickets eine der folgenden Steuerungen angezeigt, wenn der Benutzer der Kategorie oder dem Bereich, an der bzw. an dem diese Eigenschaft angehängt wurde, ein Ticket zuweist:

- Textbearbeitungsfeld - Es wurde keine Validierungsregel definiert, und kein Standardwert kann angegeben werden. Benutzer sollen Werte eingeben, die den von Ihnen bereitgestellten Beispielen folgen.
- Kontrollkästchen - Ein Kontrollkästchen mit zwei Zuständen wird auf der Registerkarte "Eigenschaften" angezeigt. Standardmäßig enthält das Kontrollkästchen kein Häkchen. Der Benutzer kann den Standardwert annehmen oder das Kontrollkästchen aktivieren. Für Kontrollkästchen, die ein Häkchen enthalten, wird auf der Detailseite des Tickets in der Wertspalte "Ja" angezeigt. Bei deaktivierten Kästchen wird in der Wertespalte "Nein" angezeigt.

- Dropdown-Liste - Auf der Registerkarte "Eigenschaften" wird eine Dropdown-Liste mit einem vordefinierten Satz Optionen angezeigt. Sofern Sie einen Standardwert definiert haben, wird dieser ausgewählt, wenn die Dropdown-Liste zum ersten Mal geöffnet wird. Die Option, die der Benutzer auswählt, wird in der Wertspalte auf der Detailseite des Tickets angezeigt.

Definieren von Change-Kategorien und Issue-Kategorien für Self-Service

Sie können die Option "Einschließen" in Self-Service zur Festlegung verwenden, welche Change- und Issue-Kategorien in Tickets für Self-Service einzuschließen sind. Sie können auch andere Self-Service-Symbole definieren als die, die für den Analysten angezeigt werden. Wird das Ticket gespeichert, wird das Self-Service-Symbol im Feld "Change-Kategorie" (bzw. "Issue-Kategorie") angezeigt. Wird das Ticket in der Analystenschnittstelle angezeigt, wird das normale Symbol für die Kategorie dargestellt.

So definieren Sie eine Change-Kategorie (bzw. Issue-Kategorie) für Self-Service:

1. Wählen Sie auf der Registerkarte "Administration" die Optionen "Service Desk" > "Changes" (oder "Issues") > "Kategorien" aus.

Die Seite "Kategorien - Liste" wird angezeigt.

2. Wählen Sie "In Liste bearbeiten" aus.

Im oberen Teil der Seite werden die bearbeitbaren Felder angezeigt.

3. Wählen Sie die gewünschte Kategorie aus der Symbolliste aus.

4. Füllen Sie die folgenden Felder aus:

Self-Service einschließen

Legt fest, ob diese Kategorie in der Self-Service-Schnittstelle angezeigt wird.

Standard: Yes (Ja)

Self-Service-Symbol

Definiert eine eindeutige Kennung für diese Kategorie in der Self-Service-Schnittstelle.

Aktiv

Gibt an, ob die Kategorie aktiv oder inaktiv ist.

Die Kategorie wird für Self-Service definiert.

5. Klicken Sie auf "Speichern".

Die aktualisierte Kategorie wird beim erneuten Anzeigen der Liste "Change-Kategorien - Liste" (bzw. "Issue-Kategorien - Liste") aufgeführt.

Automatisches Schließen von Tickets

Sie können Tickets so konfigurieren, dass diese automatisch geschlossen werden können. Dies betrifft Anfragen/Incidents/Probleme, Änderungsaufträge und Issues. Wenn ein Ticket auf den Status "Gelöst" gesetzt wird, wird es automatisch nach der angegebenen Anzahl von Arbeitsstunden geschlossen. Die Aktivitätsbenachrichtigung über die automatische Schließung, die an den Endanwender gesendet wird, zeigt die Anzahl der Arbeitsstunden vor dem Schließen des Tickets an. Die Anzahl der Stunden ist konfigurierbar und mandantenspezifisch. Wird der Status geändert, bevor die konfigurierbare Anzahl von Stunden vergangen ist, wird das Schließen des Tickets abgebrochen.

Als Administrator können Sie die folgenden Aktionen ausführen:

- Sie können eine Ticket-Einstellung für die automatische Schließung definieren, um zu steuern, wie viele Arbeitsstunden für den Endanwender vergehen sollen, bevor das Ticket automatisch geschlossen wird.
- Sie können eine Aktivitätsbenachrichtigung für die automatische Schließung einrichten, um die entsprechenden Kontakte über die geplante automatische Schließung eines Tickets zu informieren.

Hinweis: Wenn Sie die Mandantenfähigkeit verwenden, gehen Sie wie folgt vor:

- Das System verwendet standardmäßig die öffentliche Einstellung zum automatischen Schließen, wenn keine mandantenspezifische Einstellung gefunden wird.
- Für jeden Mandanten ist genau eine Einstellung für das automatische Schließen festlegbar.

Hinweis: Ausführlichere Informationen zum Durchführen dieser Verfahren finden Sie unter "Automatisches Schließen" in der *Online-Hilfe*.

Weitere Informationen:

[Definieren von Einstellungen zur automatischen Schließung von Tickets](#) (siehe Seite 437)
[Definieren einer Aktivitätsbenachrichtigung für die automatische Schließung](#) (siehe Seite 438)

Definieren von Einstellungen zur automatischen Schließung von Tickets

Sie können folgendermaßen die Anzahl von Geschäftsstunden definieren, bevor ein Ticket (alle Ticket-Typen) geschlossen wird:

1. Wählen Sie auf der Registerkarte "Administration" die Option "Service Desk" > "Anwendungsdaten" > "Codes" > "Automatische Schließung" aus.
2. Klicken Sie auf der Listenseite auf "Neu erstellen".
3. Füllen Sie auf der Detailseite die folgenden Felder aus:

Symbol

Definiert den Systemeinstellungsnamen.

Anfrage/Incident/Problem/Change/Issue

Definiert die Anzahl von Geschäftsstunden, bevor das Ticket geschlossen wird, nachdem es in den Status "Gelöst" gesetzt wurde. Wenn der Status vor Ablauf der Anzahl von Stunden geändert wird, wird das Schließen des Tickets abgebrochen. 0 (Null) Stunden gibt an, dass automatische Schließung für den Ticket-Typ nicht implementiert ist.

Beschreibung

Bietet eine kurze Beschreibung des Datensatzes.

Status

Zeigt an, ob der Datensatz aktiv oder inaktiv ist.

Die Einstellung für automatisches Schließen ist definiert.

4. Klicken Sie auf "Speichern" und "Fenster schließen".

Die neue Einstellung wird beim nächsten Öffnen der Liste "Automatische Schließung" angezeigt.

Definieren einer Aktivitätsbenachrichtigung für die automatische Schließung

Sie können die Einstellungen in der standardmäßigen Aktivitätsbenachrichtigung für die automatische Schließung ändern, um die entsprechenden Kontakte über die geplante automatische Schließung eines Tickets zu informieren. Die Aktivität ist gültig für alle CA SDM-Ticket-Typen und schließt eine Standardbenachrichtigungsregel für Anfragen/Incidents/Probleme, Changes und Issues mit ein.

So definieren Sie eine Aktivitätsbenachrichtigung für die automatische Schließung:

1. Wählen Sie auf der Registerkarte "Administration" die Option "Benachrichtigungen" > "Aktivitätsbenachrichtigungen" aus.
2. Wählen Sie die Aktivitätsbenachrichtigung für die automatische Schließung auf der Listenseite aus, um sie zu öffnen.
3. Aktualisieren Sie die standardmäßige Benachrichtigungsregel für die automatische Schließung, und geben Sie Kontakte an, die Benachrichtigungen empfangen sollen.
4. Klicken Sie auf "Speichern" und "Fenster schließen".

Die aktualisierte Aktivitätsbenachrichtigung über die automatische Schließung wird in der Liste der Aktivitätsbenachrichtigungen aufgeführt, wenn Sie die Liste erneut anzeigen.

Aktivitäten zugehöriger Tickets

Wenn eine Aktivität für ein CA SDM-Ticket erstellt wird, können Sie diese Aktivität für zugehörige Tickets übernehmen. Beispielsweise kann ein aus einem Incident erstellter Problemdatensatz den Incident-Datensatz aktualisieren, wenn das Problem gelöst wird. Wenn die Aktivität auftritt, wird für das zugehörige Ticket ein Aktivitätsprotokoll mit den folgenden Informationen erstellt:

- Aktivitätstyp des zugehörigen Tickets, beispielsweise "Aktualisierungsstatus"
- Kontaktname
- Typ des übergeordneten Tickets mit dessen Referenznummer
- -Beschreibung des Aktivitätsprotokolls, beispielsweise "Status aktualisiert von In Bearbeitung nach Offen"

Aktivitätsprotokolle werden in Abhängigkeit von den Eigenschaften, die innerhalb der einzelnen Aktivitätsbenachrichtigung festgelegt sind, an zugehörige Tickets weitergeleitet. Die Attribute zugehöriger Tickets werden nicht geändert. Die folgenden Beziehungen werden weitergeleitet:

- Probleme werden an alle aktiven Zwischenfälle weitergeleitet.
- Changes werden an alle aktiven Probleme und Zwischenfälle weitergeleitet.

Als Systemadministrator können Sie folgende Aktionen ausführen:

- Richten Sie Aktivitätsbenachrichtigungen ein, um zugehörige Ticket-Aktivitäten weiterzuleiten.
- Konfigurieren Sie eine Benachrichtigung über eine Ticket-Aktivität, um geeignete Kontakte zu benachrichtigen, wenn die Aktivität an zugehörige Tickets weitergeleitet wird.

Hinweis: Ausführlichere Informationen zum Durchführen dieser Verfahren finden Sie unter "Aktivitätsbenachrichtigung" in der *Online-Hilfe*.

Weitere Informationen:

[Aktivitätsprotokoll](#) (siehe Seite 519)

[Definieren von Aktivitätsbenachrichtigungen für zugehörige Tickets](#) (siehe Seite 439)

[Definieren von Benachrichtigungen über die Aktivität zugehöriger Tickets](#) (siehe Seite 440)

Definieren von Aktivitätsbenachrichtigungen für zugehörige Tickets

Sie können Aktivitätsprotokolle auf Grundlage der in den einzelnen Aktivitätsbenachrichtigungen festgelegten Eigenschaften auf zugehörige Tickets übertragen. Die Attribute zugehöriger Tickets werden nicht geändert.

So definieren Sie eine Aktivitätsbenachrichtigung für Aktivitäten zugehöriger Tickets:

1. Wählen Sie auf der Registerkarte "Administration" die Option "Benachrichtigungen" > "Aktivitätsbenachrichtigungen" aus.
2. Öffnen Sie die entsprechende Aktivitätsbenachrichtigung, um sie zu bearbeiten.
3. Klicken Sie auf der Detailseite auf das Kontrollkästchen "Aktivität der zugehörigen Tickets", um es zu aktivieren.

Hinweis: Wenn Sie mehrere Mandanten verwenden, gehen Sie wie folgt vor:

- Geben Sie in der Dropdown-Liste "Aktivität der zugehörigen Tickets" den entsprechenden Mandantentyp an.
 - Geben Sie im Mandantenfeld den Namen des Mandanten ein, oder klicken Sie auf das Suchsymbol, um einen Mandanten zu suchen.
4. (Optional) Aktualisieren Sie die standardmäßige Benachrichtigungsregel, und geben Sie Kontakte an, die Benachrichtigungen empfangen sollen.
 5. Klicken Sie auf "Speichern" und "Fenster schließen".

Die aktualisierte Aktivitätsbenachrichtigung wird in der Liste der Aktivitätsbenachrichtigungen aufgeführt, wenn Sie die Liste erneut anzeigen.

Definieren von Benachrichtigungen über die Aktivität zugehöriger Tickets

Sie können die Standardeinstellungen in der Benachrichtigung über die Aktivität der zugehörigen Tickets ändern, um die entsprechenden Kontakte zu benachrichtigen, wenn die Aktivitätsprotokolle auf die zugehörigen Tickets (Anfragen/Incidents/Probleme, Changes und Issues) übertragen werden.

So definieren Sie eine Benachrichtigung über die Aktivität der zugehörigen Tickets:

1. Öffnen Sie auf der Seite "Aktivitätsbenachrichtigungen - Liste" die Benachrichtigung über die Aktivität der zugehörigen Tickets.
2. Klicken Sie auf "Bearbeiten", und ändern Sie nach Bedarf ein oder mehrere Felder auf der Detailseite.
3. (Optional) Aktualisieren Sie die standardmäßige Benachrichtigungsregel, und geben Sie Kontakte an, die Benachrichtigungen empfangen sollen.
4. Klicken Sie auf "Speichern" und "Fenster schließen".

Die aktualisierte Benachrichtigung über die Aktivität der zugehörigen Tickets wird in der Liste der Aktivitätsbenachrichtigungen aufgeführt, wenn Sie die Liste erneut anzeigen.

Prioritätsberechnung

Eine *Prioritätsberechnung* ist eine vordefinierte Wertemenge, die automatisch Prioritäts-, Dringlichkeits- und Auswirkungsfelder bei Problemen und Incidents setzt. Die Prioritätsberechnung hilft Ihnen dabei, Incidents und Probleme für Ihre Geschäftsanforderungen und IT-Möglichkeiten zu verwalten. ITIL empfiehlt, dass Sie Tickets priorisieren, indem Sie eine Datenberechnung verwenden, die auf Dringlichkeits- und Auswirkungswerten basiert. Support-Organisationen definieren diese Berechnungen basierend auf ihren spezifischen Prozessen, darauf, wie diese Berechnung Service Level Agreements (SLAs) beeinflusst, sowie Schlüssel-Events im System. Diese Berechnung kann auch die Kritikalität des CI einschließen, das mit dem Incident und Problem verbunden ist. Das Priorisieren von Tickets unterstützt Sie effektiv in folgenden Punkten:

- Zuweisen von IT-Ressourcen für Tickets
- Verbessern des Kundenservice
- Reduzieren von Kosten

Die CA SDM-Lösung für Prioritätsberechnung umfasst die folgenden Komponenten:

- Eine auf die Dringlichkeits- und Auswirkungswerten basierte Prioritätsberechnungsmatrix
- Standardwerte für Dringlichkeit und Auswirkung

- Anpassungsoptionen für Dringlichkeit und Auswirkung basierend auf betroffenem Service, Öffnungsdatum, betroffenem Endanwender und Incident- oder Problembereich
- Option "Grund der Erfassung" für das manuelle Ändern von Dringlichkeit oder Auswirkung
- Option "Für Vorlagen aktivieren" für das Erstellen eines Tickets auf Basis einer Vorlage

Wenn Sie CA SDM installieren, verwaltet eine standardmäßige Prioritätsberechnung die Ticketwerte automatisch. Sie können die Einstellungen der Standard-Prioritätsberechnung ändern oder zusätzliche Prioritätsberechnungen erstellen, um Incidents oder Probleme zu verwalten. In der Prioritätsberechnung definieren Sie das Ergebnis auf Basis von Business-Szenarien, um die Bedeutungsstufe und Ticketverarbeitung konsequenter zu machen. Anwender können einige Einstellungen überschreiben, aber sie können die Priorität nicht im Ticket festlegen, da dieser Wert datengesteuert ist. Für mehrere Mandanten können Sie oder die Mandanten zusätzliche Prioritätsberechnungen mit bestimmten Einstellungen für jeden Mandanten erstellen.

Wenn ein Analyst einen Incident oder ein Problem öffnet, verwendet das System automatisch eine aktive Prioritätsberechnung und Ticketwerte, um Prioritäts-, Dringlichkeits- und Auswirkungs-Einstellungen zu erzeugen. Die Einstellungen basieren auf einem oder mehreren der folgenden Felder:

- Urgency
- Impact
- Betroffener Endanwender
- Incident- oder Problembereich
- Geöffnet am
- Betroffener Service

Analysten können Dringlichkeits- und Auswirkungswerte bei Bedarf überschreiben. Je nachdem, wie Sie den Optionsmanager konfigurieren, können Mitarbeiter nur Dringlichkeitswerte von Incidents überschreiben, wenn die Option *urgency_on_employee* installiert ist. Wenn die Markierung "Grund der Erfassung" aktiviert ist und die Anwender Dringlichkeits- oder Auswirkungswerte überschreiben und auf "Speichern" klicken, wird die Detailseite für "Eskalieren" angezeigt, auf der die Anwender einen Grund für die Änderung angeben können.

Alle Ticket-Prioritätsberechnungen, manuelle Überschreibungen und Informationen zum Grund werden im neuen Aktivitätsprotokoll angezeigt. Wenn keine Prioritätsanpassungen stattfinden, erstellt das System keinen Aktivitätsprotokolleintrag.

Hinweis: Bei einer Migration von einer Vorgängerversion ist die Prioritätsberechnung standardmäßig deaktiviert. Informationen zum Aktivieren der Prioritätsberechnung oder Beibehalten von Anpassungen finden Sie im *Implementierungshandbuch*.

Verwaltung von Ticketwerten durch Prioritätsberechnung

Das System passt Problem- und Incident-Werte auf der Basis von aktiven Einstellungen der Prioritätsberechnung an, um Analysten bei der effizienteren Verarbeitung von Tickets zu unterstützen. Die folgende Tabelle fasst zusammen, wie die Prioritätsberechnung Felder auf Basis der Prioritätsberechnung und Anwenderaktionen für Probleme, Incidents, Webservice, E-Mail und der Text-API ändert:

Aktion	Automatische Feldänderungen	Beschreibung
Anwender ändert betroffenen Service	Impact Priorität	Das System analysiert den Wert der Service-Auswirkung auf das CI des Typs "Service", um den neuen Auswirkungswert zu berechnen. Die CIs des Typs "Service" sind als CIs definiert, deren Klasse in der Unternehmensservice-Familie definiert ist. Falls das Datum "Geöffnet am" des Tickets innerhalb des Zeitrahmens des Sperrfensters liegt, erhöht das System einen neuen Auswirkungswert auf der Basis des Feldes "Auswirkungszuwachs". Das System ersetzt den Auswirkungswert nur dann, wenn der neue Wert größer als der Ausgangswert der Auswirkung ist.
Anwender ändert Incident-Bereich	Urgency	Der Dringlichkeitswert ändert sich nur, wenn der neue Wert größer als der Standardwert ist.
Anwender ändert Incident-Bereich <i>und</i> betroffenen Endanwender	Urgency Priorität	Wenn der Anwender das Feld "Incident-Bereich" zuerst festlegt, ändert sich der Dringlichkeitswert, nachdem der Anwender den Wert für "Betroffener Endanwender" festlegt. Die Prioritätsberechnung legt die Priorität fest.

Aktion	Automatische Feldänderungen	Beschreibung
Anwender ändert Dringlichkeit und Auswirkung	Priorität Impact	Das System analysiert den Wert der Service-Auswirkung auf das CI des Typs "Service", um den neuen Auswirkungswert zu berechnen. Wenn das Datum "Geöffnet am" des Tickets innerhalb einer Zeit liegt, die von einem Sperrfenster definiert wird, erhöht das System einen neuen Auswirkungswert auf Basis des Feldes "Auswirkungszuwachs". Das System ersetzt den Auswirkungswert nur dann, wenn der neue Wert größer als der Ausgangswert der Auswirkung ist. Wenn der Administrator "Grund der Erfassung" festlegt, muss der Anwender einen Grund für die Änderung angeben. Wenn der Anwender die Dringlichkeits- oder Auswirkungswerte ändert, bleiben diese Werte während der gesamten Ticket-Erstellung oder während der Ticket-Aktualisierung gleich, es sei denn, der Anwender ändert sie erneut. Allerdings kann das System die überschriebenen Werte für Dringlichkeit oder Auswirkung aktualisieren, wenn der Anwender das nächste Mal das Ticket aktualisiert. Nachdem das System die Dringlichkeit und Auswirkung eingestellt hat, legt die Prioritätsberechnung den Prioritätswert fest.
Anwender wählt neuen Incident aus Basis des Knowledge-Dokument, und System hat Überschreibungen für Knowledge-Dokumente (siehe Seite 452)	Impact Urgency	Das System benutzt das Knowledge-Dokument oder Knowledge-Lösungswerte immer, unabhängig davon, ob die Werte größer oder kleiner als die standardmäßigen Prioritätsberechnungswerte sind. Wenn zum Beispiel eine Prioritätsberechnung einen Auswirkungswert von "3-Einzelne Gruppe" und einen Dringlichkeitswert von "3-Schnell" hat, und Knowledge-Dokumente einen Auswirkungswert von "2-Mehrere Gruppen" und einen Dringlichkeitswert von "4-Sehr schnell" haben, wendet das System die Werte vom Knowledge-Dokument auf den Incident an. Der Prioritätswert stammt immer aus der Prioritätsberechnung.
Anwender akzeptiert Knowledge-Dokument als Lösung des Problems oder Incident	Impact Urgency	Das System benutzt die Werte vom Knowledge-Dokument für Auswirkung und Dringlichkeit. Das System verwendet die Prioritätsberechnung auch, um den Prioritätswert zu setzen.

Aktion	Automatische Feldänderungen	Beschreibung
Anwender leitet Incident aus Knowledge-Dokument durch Auswählen einen neuen Incidents ab	Impact Urgency Priorität	Das System benutzt die Prioritätsberechnungswerte.
Anwender leitet Incident aus Knowledge-Dokument ohne System- Überschreibungen für Knowledge-Dokumente (siehe Seite 452) ab	Impact Urgency Priorität	Das System verwendet die Prioritätsberechnungswerte unabhängig davon, wie der Anwender den Incident für das Knowledge-Dokument oder die Knowledge-Lösung erstellte.
Ticket akzeptiert Knowledge-Dokument als Lösung des Problems oder Incidents, und das System überschreibt nicht für Knowledge-Dokumente	Impact Urgency Priorität	Das System verwendet Werte von Problem oder Incident. Der Prioritätswert stammt aus der Prioritätsberechnung.
Ticket im schreibgeschützten Modus akzeptiert Knowledge-Dokument als Lösung des Problems oder Incidents, und System überschreibt für Knowledge-Dokumente	Impact Urgency Priorität	Das System verwendet Auswirkungs- und Dringlichkeitswerte aus dem Knowledge-Dokument, wenn die Werte nicht leer sind. Wenn der Auswirkungs- oder Dringlichkeitswert im Knowledge-Dokument leer ist, verwendet das System Werte des Problems oder Incident. Der Prioritätswert stammt aus der Prioritätsberechnung.
Ticket im Bearbeitungsmodus akzeptiert Knowledge-Dokument als Lösung des Problems oder Incidents, und System überschreibt für Knowledge-Dokumente.	Impact Urgency Priorität	Das System verwendet Werte von Problem oder Incident. Der Prioritätswert stammt aus der Prioritätsberechnung.

Prioritätsberechnung generiert nach dem Speichern von Self-Service-Tickets einen Dringlichkeitswert

Designbedingt werden Dringlichkeitswerte von der Prioritätsberechnung erst nach dem Speichern von Incidents durch Self-Service-Anwender generiert. Self-Service-Anwender, wie VIP-Mitarbeiter, Mitarbeiter und anonyme Anwender, können den generierten Wert nach dem Speichern eines Tickets anzeigen.

Für Self-Service-Anwender werden von der Prioritätsberechnung die folgenden Einstellungen und Werte zum Generieren von Dringlichkeitswerten verwendet:

- Im Optionsmanager ist "Urgency_On_Employee" auf "Ja" gesetzt
- In der aktiven Prioritätsberechnung für Incidents ist der Wert "Dringlichkeit überschreiben" aktiviert
- *Web.cfg*-Dringlichkeitseinstellungen, wie "AnonymousUrg" für anonyme Anwender, "ESCEmpUrg" für VIP-Mitarbeiter und "EmpUrg" für alle anderen Mitarbeiter
- Bereichsdringlichkeitswerte
- Manuelle Überschreibungen durch den Anwender

In der folgenden Tabelle wird zusammengefasst, wie der Dringlichkeitswert für Self-Service-Incidents von der Prioritätsberechnung festgelegt wird:

Self-Service-Anwenderaktion	Dringlichkeitswert
Der Anwender speichert einen Incident mit der Standarddringlichkeit und einem leeren Incident-Bereich.	Das Ticket zeigt den Standarddringlichkeitswert aus <i>web.cfg</i> an.
Der Anwender speichert einen Incident nach Überschreiben des Dringlichkeitswerts.	Das Ticket zeigt unabhängig von der Bereichsdringlichkeit, der Datei <i>web.cfg</i> oder den Einstellungen für die Prioritätsberechnung den vom Anwender ausgewählten Dringlichkeitswert an.
Der Anwender speichert einen Incident nach Auswahl eines Incident-Bereichs. Der Incident-Bereich hat keinen vordefinierten Bereichsdringlichkeitswert.	Das Ticket zeigt den Standarddringlichkeitswert aus <i>web.cfg</i> an.
Der Anwender speichert einen Incident nach Auswahl eines Incident-Bereichs mit vordefiniertem Bereichsdringlichkeitswert. Die Option "Dringlichkeit überschreiben" ist auch bei der aktiven Prioritätsberechnung für Incidents aktiviert.	Wenn der Bereichsdringlichkeitswert größer als die Dringlichkeit in <i>web.cfg</i> ist, zeigt das Ticket den Bereichsdringlichkeitswert an. Das aktualisierte Dringlichkeitsfeld ist jedoch nicht sichtbar, während der Anwender das Ticket erstellt oder bearbeitet. Wenn der Anwender den Incident speichert und erneut öffnet, wird der aktualisierte Dringlichkeitswert für den Incident angezeigt.

Self-Service-Anwenderaktion	Dringlichkeitswert
Der Anwender speichert einen Incident nach Auswahl eines Incident-Bereichs mit vordefiniertem Bereichsdringlichkeitswert. Die Option "Dringlichkeit überschreiben" ist jedoch bei der aktiven Prioritätsberechnung für Incidents deaktiviert.	Das Ticket zeigt einen Dringlichkeitswert aus <i>web.cfg</i> an.
Der Anwender bearbeitet einen vorhandenen Incident, der einen Incident-Bereich mit vordefiniertem Bereichsdringlichkeitswert hat.	Die Drop-down-Liste "Dringlichkeit" zeigt den Bereichsdringlichkeitswert sowie alle geltenden <i>web.cfg</i> -Werte an.

Hinweis: Informationen zum Festlegen von Dringlichkeitswerten für Self-Service-Anwender finden Sie im *Implementierungshandbuch*.

Einstellen der Prioritätsberechnung

Standardmäßig basieren Ticketwerte wie z. B. Priorität auf einer Prioritätsberechnung. Sie können die Anfangswerte für Priorität und Dringlichkeit in der Datei "web.cfg" finden und einstellen. Die Datei "web.cfg" enthält verschiedene Einstellungen für verschiedene Benutzer wie Gast, VIP-Benutzer und Mitarbeiter.

Hinweis: Bei einer Migration von einer älteren Version ist die Prioritätsberechnung standardmäßig deaktiviert. Die ordnungsgemäße Funktion der Detailseiten für benutzerdefinierte Incidents und Probleme setzt weitere Konfiguration voraus. Informationen zum Aktivieren der Prioritätsberechnung oder Beibehalten von Anpassungen finden Sie im *Implementierungshandbuch*.

So legen Sie die Prioritätsberechnung fest:

1. Wählen Sie auf der Registerkarte "Administration" die Optionen "Service Desk" > "Anfragen/Incidents/Probleme" > "Prioritätsberechnung".

Die Prioritätsberechnungsliste wird angezeigt.

2. Klicken Sie mit der rechten Maustaste auf die Standard-Prioritätsberechnung, und wählen Sie im Kontextmenü die Option "Bearbeiten".

Die Standarddetailseite "Prioritätsberechnung" zeigt Standardeinstellungen für Incident- und Problem-Tickets.

3. Prüfen Sie die Standardprioritätsberechnung und ändern Sie die Werte entsprechend. Wenn Sie Prioritätsberechnungswerte festlegen, berücksichtigen Sie die folgenden Gesichtspunkte für Ihre Arbeitsumgebung:
 - **Issue-Eskalation** – Wenn Tickets eine Eskalation zu einem bestimmten VIP erfordern, können Sie den Wert für "Dringlichkeit" erhöhen.
 - **Kritische CIs** – Bei kritischen CIs können Sie eine Service-Auswirkung für jedes CI konfigurieren.
 - **Kritische Service-Betriebszeit** – Wenn für CIs eine hohe Verfügbarkeit erforderlich ist, fügen Sie ein Ausfallfenster hinzu.
 - **Ausfallfenster** – Wenn für CI-bezogene Tickets ein bestimmtes Ausfallfenster verwendet wird, können Sie den Service-Auswirkungswert bei der Prioritätsberechnung erhöhen.
4. Verwenden Sie die Einstellung zum manuellen Überschreiben, um Benutzern zu erlauben, Ticket-Einstellungen soweit erforderlich zu ändern.
5. Wenn Sie eine andere Prioritätsberechnung zum Verwalten von Problemen oder Incidents möchten, [konfigurieren Sie den Ticket-Typ](#) (siehe Seite 450).
6. Klicken Sie auf "Speichern".

Die Felder werden im nächsten neuen oder aktualisierten Ticket bzw. Knowledge-Dokument gemäß den Werten in der aktiven Prioritätsberechnung aktualisiert.
7. Sie können zusätzliche Prioritätsberechnungen für jeden Ticket-Typ erstellen. Erstellen und aktivieren Sie bei mehreren Mandanten zusätzliche Prioritätsberechnungen, um Tickets für die einzelnen Mandanten zu verwalten.

Hinweis: Informationen zur Prioritätsberechnung finden Sie in der *Online-Hilfe*.

Mehrfache Prioritätsberechnungen

Sie können mehr als eine Prioritätsberechnung einrichten. Allerdings verarbeitet nur eine aktive Prioritätsberechnung Probleme oder Incidents bzw. beide. Zum Beispiel können Sie eine aktive Prioritätsberechnung für Probleme und eine andere für Incidents haben. Sie können für künftige Anwendungen auch mehrere inaktive Prioritätsberechnungen speichern.

Zuweisung der Prioritätsberechnung für mehrere Mandanten

Sie oder Ihre Mandanten können mandantenspezifische Prioritätsberechnungen erstellen, um Incidents und Probleme zu verwalten. Wenn Sie Prioritätsberechnungen für mehrere Mandanten zuweisen, beachten Sie Folgendes:

- Wenn eine Prioritätsberechnung keinen zugewiesenen Mandanten hat, wird sie als öffentlich betrachtet. Der Status einer öffentlichen Prioritätsberechnung ist entweder "Aktiv" oder "Inaktiv". Eine Prioritätsberechnung wird nicht mehr als öffentlich betrachtet, wenn sie einem Mandanten zugewiesen wurde.
- Wenn ein Mandant keine Prioritätsberechnungszuweisung hat, werden die Probleme und Incidents automatisch von der Standard-Prioritätsberechnung oder einer anderen aktiven öffentlichen Prioritätsberechnung verwaltet.
- Eine Prioritätsberechnung verwaltet Probleme und Incidents für einen Mandanten. Es können jedoch getrennte mandantenspezifische Prioritätsberechnungen für jeden Ticket-Typ festgelegt werden. Zum Beispiel hat Unternehmen X eine Prioritätsberechnung, um Incidents zu verwalten, und eine zweite Berechnung zum Verwalten von Problemen.
- Wenn Mandanten ihre eigenen Prioritätsberechnungen erstellen, während öffentliche Prioritätsberechnungen aktiv sind, gilt die mandantenspezifische Prioritätsberechnung nur für Tickets des betreffenden Mandanten.

Wenn zum Beispiel die Standard-Prioritätsberechnung aktiv ist, kann das Unternehmens X eine mandantenspezifische Prioritätsberechnung mit dem Namen "new_priority_calculation" erstellen. Die Einstellungen und Konfigurationen von "new_priority_calculation" gelten nur für Incidents und Probleme des Unternehmens X.

- Wenn der Mandant eine Prioritätsberechnung deaktiviert, verwendet das System eine aktive öffentliche Prioritätsberechnung, um Mandantenprobleme und -Incidents zu verwalten.

Beispiel. Das Unternehmen X deaktiviert die mandantenspezifische Prioritätsberechnung, während noch eine aktive Standard-Prioritätsberechnung vorhanden ist. Die Prioritätsberechnung bleibt für das Unternehmen X aktiviert, weil das System die Standard-Prioritätsberechnung verwendet, um Incidents und Probleme für das Unternehmen X zu bearbeiten.

Anmerkung: Weil Mandanten ihre eigenen Prioritätsberechnungsdatensätze löschen können, wird empfohlen, die öffentlichen Prioritätsberechnungen zu deaktivieren, die Incidents und Probleme verwalten. Statt dessen können Sie oder die Mandanten mandantenspezifische Prioritätsberechnungen erstellen.

- Wenn Sie die Funktion für mehrere Mandanten deaktivieren und mehr als eine aktive Prioritätsberechnung vorhanden ist, die Mandanten verwaltet, belassen Sie *nur eine* Prioritätsberechnung, um Incidents und Probleme zu verwalten. Zum Beispiel können Sie alle Prioritätsberechnungen deaktivieren, mit Ausnahme einer Berechnung zum Verwalten von Incidents und einer zweiten zum Bearbeiten von Problemen.

Hinweis: Detaillierte Informationen zu mehreren Mandanten finden Sie im *Implementierungshandbuch*.

Zuweisen von Mandanten zu einer Prioritätsberechnung

Bei einem System mit mehreren Mandanten können Sie einer Prioritätsberechnung einen Mandanten zuweisen. Zunächst deaktivieren Sie die öffentlichen Prioritätsberechnungen. Dann weisen Sie den Mandanten einer Prioritätsberechnung zu und aktivieren diese.

Um einen Mandanten einer Prioritätsberechnung zuzuweisen, gehen Sie wie folgt vor:

1. Wählen Sie auf der Registerkarte "Administration" die Optionen "Service Desk" > "Anfragen/Incidents/Probleme" > "Prioritätsberechnung".

Die Prioritätsberechnungsliste wird angezeigt.

2. Bearbeiten Sie die einzelnen öffentlichen Prioritätsberechnungen, z. B. "Standard". Setzen Sie den Status auf "Inaktiv", und klicken Sie auf "Speichern".

Das System deaktiviert die öffentlichen Prioritätsberechnungen.

3. Erstellen oder bearbeiten Sie für jeden Mandanten eine Prioritätsberechnung mit mandantenspezifischen Einstellungen für "Auswirkung", "Dringlichkeit" und "Priorität".

Die Seite zum Erstellen oder Aktualisieren einer Prioritätsberechnung wird angezeigt.

4. Geben Sie im Feld "Name" den Mandanten an.
5. Wählen Sie im Feld "Status" die Option "Aktiv".
6. Klicken Sie auf "Speichern".

Das System wendet auf neue Incidents und Probleme mandantenspezifische Werte für "Auswirkung", "Dringlichkeit" und "Priorität" an.

Hinweis: Informationen zum Erstellen und Bearbeiten von Prioritätsberechnungen finden Sie in der *Online-Hilfe*.

Ticket-Typ-Überlegungen für Prioritätsberechnung

Wenn Sie Ticket-Typen für eine Prioritätsberechnung konfigurieren, berücksichtigen Sie Folgendes:

- Mit Hilfe der Standard-Prioritätsberechnung können Sie sowohl Incident- als auch Problem-Ticket-Typen verwalten.
- Wenn Sie von einer früheren Version migrieren, dann aktivieren Sie die Standard-Prioritätsberechnung oder erstellen eine Prioritätsberechnung, um Probleme und Incidents zu verwalten.
- Obwohl Sie viele Prioritätsberechnungen haben können, kann nur jeweils eine aktive Prioritätsberechnung einen bestimmten Ticket-Typ verarbeiten. Beispielsweise kann eine aktive Prioritätsberechnung Probleme verwalten, während die andere Incidents verwaltet.
- Wenn Sie eine Prioritätsberechnung erstellen möchten und eine aktive Prioritätsberechnung bereits einen bestimmten Ticket-Typ verarbeitet, dann deaktivieren Sie zuerst den Ticket-Typ der aktiven Prioritätsberechnung. Wenn Sie beispielsweise mit einer Prioritätsberechnung Probleme verwalten möchten, dann deaktivieren Sie den Problem-Ticket-Typ der aktiven Prioritätsberechnung und erstellen Sie eine aktive Prioritätsberechnung, die Probleme verwaltet.

Hinweis: Weitere Informationen zum Aktivieren von Prioritätsberechnungen und Einrichten von Ticket-Typen während der Migration finden Sie im *Implementierungshandbuch*.

Konfigurieren von Ticket-Typen für eine Prioritätsberechnung

Sie können die Ticket-Typen angeben, die von der Prioritätsberechnung verwaltet werden sollen. Wenn die Prioritätsberechnung aktiv ist, verwaltet sie Priorität, Auswirkung und Dringlichkeitswerte für neue Tickets.

So konfigurieren Sie Ticket-Typen für eine Prioritätsberechnung

1. Wählen Sie auf der Registerkarte "Administration" die Optionen "Service Desk" > "Anfragen/Incidents/Probleme" > "Prioritätsberechnung".

Die Prioritätsberechnungsliste wird angezeigt.

2. Klicken Sie mit der rechten Maustaste auf eine Prioritätsberechnung und wählen Sie dann aus dem Kontextmenü den Befehl "Bearbeiten".

Die Seite "Prioritätsberechnung aktualisieren" wird angezeigt.

3. Wählen Sie unter den folgenden Optionen aus:

Vorfälle

Aktiviert bzw. deaktiviert die Prioritätsberechnung für die Verwaltung neuer Incidents.

Probleme

Aktiviert bzw. deaktiviert die Prioritätsberechnung für die Verwaltung neuer Problem-Tickets.

4. Klicken Sie auf "Speichern".

CA SDM verwendet die Einstellungen in der Prioritätsberechnung, um Ticketwerte für neue Incidents, Probleme oder beides zu verwalten.

So verwenden Sie Ticket-Vorlagen, um Werte für Prioritäten zu berechnen:

Wenn Sie die Priorität mit Hilfe von Ticket-Vorlagen berechnen möchten, konfigurieren Sie die Prioritätsberechnung mit der Option *Für Vorlagen aktivieren*. Wenn Sie diese Option aktivieren, werden die Werte für "Dringlichkeit" und "Auswirkung" aus der Vorlage übernommen, der Wert für das Feld "Priorität" wird jedoch aus dem Datensatz für die Prioritätsberechnung entnommen. Der Prioritätswert wird mit Schreibschutz angezeigt.

Wenn Sie diese Option nicht aktivieren, werden die Werte für "Dringlichkeit", "Auswirkung" und "Priorität" aus der Vorlage übernommen. Während Sie das Feld "Priorität" bearbeiten. Die Prioritätsberechnung für das Ticket wird erst durchgeführt, wenn es gespeichert wird.

So verwenden Sie Ticket-Vorlagen, um Werte für Prioritäten zu berechnen:

1. Wählen Sie auf der Registerkarte "Administration" die Optionen "Service Desk" > "Requests/Incidents/Probleme" > "Prioritätsberechnung".

Die Prioritätsberechnungsliste wird angezeigt.

2. Wählen Sie die Prioritätsberechnung aus, die Sie für die Prioritätsberechnung durch Vorlagen verwenden möchten.

Sie können auch Prioritätsberechnungen erstellen, die Ticket-Vorlagen verwenden, um die Prioritätsberechnung durchzuführen.

3. Wählen Sie aus der Liste "Prioritätsberechnung - Optionen" die Option *Für Vorlagen aktivieren* aus.

4. Klicken Sie auf "Speichern".

Die Option ist aktiviert.

Verwenden von Knowledge-Dokumenten zur Berechnung von Prioritätswerten

Soll die Priorität anhand von Knowledge-Dokumenten berechnet werden, können Sie die Feldzuordnung aktualisieren. Nach der Konfiguration der Feldzuordnung kann der Analyst Incident- oder Problem-Tickets aus den Knowledge-Dokumenten erstellen. Das Knowledge-Dokument berechnet Auswirkungs- und Dringlichkeitswerte in den Tickets. Fehlt der Auswirkungs- oder Dringlichkeitswert, stammen die Werte aus der Prioritätsberechnung.

Wichtig! Wenn Sie ein Ticket ändern und speichern, das bereits von einem Knowledge-Dokument berechnete Auswirkungs- und Dringlichkeitswerte enthält, überschreibt die Prioritätsberechnung die von Knowledge Management eingestellten Werte. Das Audit-Protokoll zeigt diese Aktivitäten an.

So verwenden Sie Knowledge-Dokumente zur Berechnung von Prioritätswerten:

1. Wählen Sie auf der Registerkarte "Administration" die Optionen "Service Desk" > "Service Desk-Integration" aus.
2. Wählen Sie "Feldzuordnung" aus.
Die Seite "Feldzuordnung" wird angezeigt.
3. Aktivieren Sie die folgenden Kontrollkästchen nach Bedarf, um die Auswirkung und Dringlichkeit festzulegen:

Leere Service Desk-Werte auffüllen

Legt fest, ob Informationen aus Knowledge Management zum Ausfüllen von Feldern bei Issues oder Anfragen zu verwenden sind.

Service Desk-Werte überschreiben

Bezeichnet die Felder in Issues oder Anfragen, die den in der Spalte "Knowledge Management" aufgeführten Feldern entsprechen.

Hinweis: Wenn für "Auswirkung" und "Dringlichkeit" das Feld "Service Desk-Werte überschreiben" deaktiviert und das Feld "Leere Service Desk-Werte ausfüllen" aktiviert ist, setzen die Knowledge-Werte für "Auswirkung" und "Dringlichkeit" die Incident-Werte außer Kraft.

4. Klicken Sie auf "Speichern".
Beim Erstellen von Incidents und Problemen werden die Auswirkungs- und Dringlichkeitswerte aus dem Knowledge-Dokument erstellt zur Prioritätsberechnung verwendet. Fehlen die Werte, erhält das Ticket die Werte aus einer aktiven Prioritätsberechnung. Ist für den Ticket-Typ keine Prioritätsberechnung aktiv, löscht das System den Inhalt der Felder "Priorität", "Dringlichkeit" und "Auswirkung".

Manuelles Außerkraftsetzen des Auswirkungswerts

Wenn Sie den Auswirkungswert eines Problems oder Incidents außer Kraft setzen möchten, passt die aktive Prioritätsberechnung, die den Ticket-Typ automatisch verwaltet, den Wert für die Priorität an.

So setzen Sie den Auswirkungswerts manuell außer Kraft:

1. Öffnen Sie die Detailseite für das Problem oder den Incident, das bzw. den Sie ändern möchten.

2. Ändern Sie den Auswirkungswert wie gewünscht.

Wenn gerade eine Prioritätsberechnung zur Verwaltung des Ticket-Typs durchgeführt wird, ändert sich der Prioritätswert automatisch entsprechend den Einstellungen in der Prioritätsberechnung.

3. Speichern Sie den Incident.

Das Aktivitätsprotokoll auf der Detailseite des Incidents zeigt nun ebenfalls die Änderungen des Auswirkungswerts an.

Beispiel: Manuelles Außerkraftsetzen des Auswirkungswerts bei einem neuen Incident

1. Erstellen Sie eine Störung.

Der Standard-Dringlichkeitswert ist "3 - Schnell". Der Auswirkungswert ist "3 - Einzelne Gruppe". Der Prioritätswert ist 3.

2. Überschreiben Sie den Auswirkungswert mit "1 - Ganze Organisation".

Der Prioritätswert ändert sich automatisch entsprechend den Werten in der aktiven Prioritätsberechnung zur Verwaltung der Incidents.

3. Speichern Sie den Incident.

Das Aktivitätsprotokoll auf der Detailseite des Incidents zeigt nun ebenfalls die Änderungen des Auswirkungswerts an.

Manuelles Überschreiben von Dringlichkeitswerten

Wenn Sie den Dringlichkeitswert in einem Ticket manuell überschreiben, passt die aktive Prioritätsberechnung, die das Ticket verwaltet, automatisch den Prioritätswert an.

So überschreiben Sie den Dringlichkeitswert manuell:

1. Öffnen Sie die Detailseite für den Incident, den Sie ändern möchten.
2. Ändern Sie den Dringlichkeitswert.

Wenn gerade eine Prioritätsberechnung zur Verwaltung des Ticket-Typs durchgeführt wird, ändert sich der Prioritätswert automatisch entsprechend den Einstellungen in der Prioritätsberechnung.

3. Speichern Sie den Incident.

Das Aktivitätsprotokoll auf der Seite "Incident - Detail" gibt die Dringlichkeitswertänderungen an.

Beispiel: Manuelles Überschreiben des Dringlichkeitswerts in einem neuen Incident

1. Erstellen Sie eine Störung.

Der standardmäßige Dringlichkeitswert ist "3-Schnell". Der Auswirkungswert ist "3-Einzelne Gruppe". Der Prioritätswert ist "3".

2. Überschreiben Sie den Dringlichkeitswert mit "5-Sofort".

Der Prioritätswert ändert sich automatisch entsprechend den Werten in der aktiven Prioritätsberechnung zur Verwaltung der Incidents.

3. Speichern Sie den Incident.

Das Aktivitätsprotokoll auf der Seite "Incident - Detail" gibt die Änderungen der Dringlichkeitswerte an.

Automatisches Anpassen der Auswirkung eines Problems bzw. Incidents

Für zusammen mit einer Familie von Unternehmensservices definierte Configuration Items können Sie den Auswirkungswert für Probleme und Incidents automatisch einstellen. Wenn Sie den Problem- bzw. Incident-Bereich auswählen und einen betroffenen Service auswählen, wird die Auswirkung entsprechend den Einstellungen der Service-Auswirkung des CI für Unternehmensservice-CIs und der Prioritätsberechnung angepasst.

So passen Sie die Auswirkung für ein Problem oder einen Zwischenfall automatisch an:

1. Erstellen Sie ein Problem oder einen Incident für ein Unternehmensservice-CI.
2. Wählen Sie einen betroffenen Service aus.
3. Wählen Sie einen Problem- oder Incident-Bereich aus.

Wenn eine aktive Prioritätsberechnung verfügbar ist, die den Ticket-Typ verwaltet, ändern sich die Werte auf der Basis des Wertes für die Erhöhung der Auswirkung (dieser wird für die Prüfung der Auswirkung im Blackout-Fenster verwendet) in der Prioritätsberechnung und des Wertes "Service-Auswirkung" des betroffenen Service.

Wenn Sie die Standardprioritätsberechnung verwenden, der Wert für "Service-Auswirkung" ist auf "1 - Ganze Organisation" festgelegt, und das Problem bzw. der Incident in keinem Blackout-Fenster geöffnet ist, wird der Wert von "Auswirkung" für das Problem bzw. die Priorität auf 1 festgelegt und der Wert für "Priorität" auf dem Ticket wird auf 2 erhöht.

4. Speichern Sie das Ticket.

Das Aktivitätsprotokoll auf der Detailseite des Incidents zeigt nun ebenfalls die Änderungen des Auswirkungswerts an.

Anpassen der Auswirkung auf ein Problem oder einen Incident – Beispiel

Das folgende Beispiel zeigt auf, wie die Auswirkung auf ein Problem oder einen Incident angepasst wird.

1. Erstellen Sie ein Unternehmensservice-CI mit der Bezeichnung "CI-APC", und platzieren Sie die Klasse unterhalb der Familie "Unternehmensservice".

Sie können die Klasse z. B. als "Anderer Service", "Business-Service" oder "Infrastrukturservice" einrichten.
2. Setzen Sie das Feld "Service-Auswirkung" auf der Registerkarte "Service" im CI-Detailformular auf "2-Mehrere Gruppen".
3. Erstellen Sie auf der Registerkarte "Service Desk" einen Incident, und setzen Sie "Betroffener Service" auf "CI-APC".
4. Speichern Sie das Ticket.

Das Feld "Auswirkung" im Incident gibt den Wert der Service-Auswirkung des ausgewählten betroffenen Services (CI-APC) an. In diesem Fall wird der Auswirkungswert auf "2-Mehrere Gruppen" gesetzt.

Hinweis: Wenn Sie die standardmäßige Prioritätsberechnung verwenden und das aktuelle Ticket während eines Ausfallfensterzeitraums erstellt wird, wird der Auswirkungswert um 1 erhöht. Im obigen Fall wird der Auswirkungswert auf "1-Gesamte Organisation" gesetzt.

Hinweis: Weitere Informationen zur Erstellung von CIs finden Sie in der Online-Hilfe.

Automatisches Anpassen der Dringlichkeit für ein Problem oder Incident

Für Probleme und Incidents können Sie automatisch die Dringlichkeit und Priorität anpassen, indem Sie einen betroffenen Endbenutzer festlegen, für den spezielle Verarbeitung erforderlich ist, oder indem Sie einen Problem-/Incident-Bereich angeben, der einen Bereichsdringlichkeitswert aufweist.

Bei der Zuweisung spezieller Verarbeitung für einen Kontakt bei aktivierter Dringlichkeits Eskalation oder bei der Angabe eines Bereichsdringlichkeitswerts für einen Problem-/Incident-Bereich wird der Dringlichkeitswert innerhalb des Problems/Incidents automatisch an die Werte in der Prioritätsberechnung und den Bereichsdringlichkeitswert für den betroffenen Endbenutzer angepasst.

So passen Sie die Dringlichkeit für ein Problem oder einen Incident automatisch an:

1. Erstellen Sie ein Problem oder einen Incident.
2. Wählen Sie einen betroffenen Endbenutzer aus. Wählen Sie für eine höhere Dringlichkeit einen betroffenen Endbenutzer aus, für den spezielle Verarbeitung erforderlich und die Dringlichkeits Eskalation aktiviert ist.

Wenn gerade eine Prioritätsberechnung zur Verwaltung des Ticket-Typs durchgeführt wird, ändert sich der Dringlichkeitswert entsprechend dem Dringlichkeitserhöhungswert in der aktiven Prioritätsberechnung.

3. Wählen Sie einen Problem- oder Incident-Bereich aus.

Wenn gerade eine Prioritätsberechnung zur Verwaltung des Ticket-Typs durchgeführt wird, ändert sich der Dringlichkeitswert entsprechend dem Bereichsdringlichkeitswert in der Problem-/Incident-Bereichsdefinition.

4. Speichern Sie das Ticket.

Eine Bestätigungsmeldung erinnert Sie daran, dass das Ticket eine spezielle Verarbeitung benötigt. Das Aktivitätsprotokoll auf der Detailseite des Problems/Incident gibt die Änderungen des Dringlichkeitswerts an.

Anpassen der Dringlichkeit eines Problems oder eines Incidents – Beispiel

Das folgende Beispiel zeigt Ihnen, wie die Dringlichkeit eines Problems oder Incidents angepasst wird:

1. Erstellen Sie auf der Registerkarte "Administrator" einen Kontakt mit der Bezeichnung "Nicht-VIP".
2. Erstellen Sie einen speziellen Verarbeitungskontakt mit der Bezeichnung "VIP", und legen Sie den Wert "Dringlichkeit eskalieren" fest.
3. Erstellen Sie einen Bereich mit der Bezeichnung "Testbereich", und setzen Sie die Bereichsdringlichkeit auf "2-Sehr schnell".
4. Erstellen Sie auf der Registerkarte "Service Desk" einen Incident.
5. Wählen Sie für den betroffenen Endbenutzer "Nicht-VIP" aus.
6. Wählen Sie im Incident-Bereich "Testbereich" aus, und speichern Sie das Ticket.

Das Feld "Dringlichkeit" gibt den Wert der Bereichsdringlichkeit aus der Incident-Bereichsdefinition wieder. In diesem Fall wird die Dringlichkeit auf "2-Sehr schnell" gesetzt.

7. Ändern Sie den betroffenen Endbenutzer in "VIP", und speichern Sie das Ticket.

Bei Verwendung der standardmäßigen Prioritätsberechnungsmatrix erhöht sich der Dringlichkeitswert um 1 und wird auf "1-Sofort" gesetzt. Es wird eine Bestätigungsmeldung angezeigt, die Sie daran erinnert, dass das Ticket eine spezielle Verarbeitung erfordert. Das Aktivitätsprotokoll auf der Seite "Incident - Detail" gibt die Dringlichkeitswertänderungen an.

Hinweis: Informationen zur Erstellung von Kontakten und Bereichen finden Sie in der *Online-Hilfe*.

Statusübergänge und abhängige Attributsteuerungen

Mithilfe der folgenden konfigurierbaren Steuerelemente können Sie den Ablauf von Ticket-Status für Changes, Issues und Incidents/Probleme/Requests beschränken und bestimmen, welche Felder für die einzelnen Ticketstatus angezeigt werden oder erforderlich sind:

Übergänge

Steuert, wie Anwender verfügbare Status auf dem Incident-/Problem-/Request-, Issue- oder Change-Formular auswählen. Angenommen, ein Problem hat den Status "Offen", und der Übergangsablauf erlaubt es dem Analysten nur, den Status auf "Geschlossen" zu aktualisieren. In diesem Beispiel hat der Analyst keine weiteren Statusoptionen, was den Problem Management-Prozess unterstützt.

Übergänge ermöglichen es Ihnen, eine Teilmenge der vollständigen Statusliste zu definieren und den neuen (oder nächsten) Standardstatus eines Tickets auf der Grundlage des aktuellen Status anzugeben. Sie können für jeden Ticket-Typ eindeutige Statusübergänge definieren. Ziehen Sie die Verwendung von Übergängen in Betracht, wenn Sie Status-Workflows für Ihre Endanwender beschränken möchten.

Abhängige Attribute

Steuert, wie Attribute je nach Ticket-Status als erforderlich (Angabe erforderlich) oder gesperrt (Aktualisierung nicht möglich) gekennzeichnet werden. Beispielsweise kann der Change Manager einen Analysten daran hindern, das Attribut "Zusammenfassung" zu bearbeiten, nachdem ein Change genehmigt wurde. Ziehen Sie die Verwendung von Attributsteuerungen in Betracht, wenn Sie bestimmte Attribute in Abhängigkeit vom Status beschränken möchten.

Hinweis: Sie können angeben, wie streng das System die Statusrichtlinien erzwingt, indem Sie die Option für Statusrichtlinienverletzungen im Optionsmanager (Allgemeine Optionen) konfigurieren. Diese Option bezieht sich nur auf automatisierte Systemprozesse wie Integrationen und Makros.

Weitere Informationen:

[Arbeiten mit Statusübergängen und abhängigen Attributsteuerungen](#) (siehe Seite 459)

[Konfigurieren der Statusübergänge](#) (siehe Seite 460)

[Best Practices: Vordefinierte Statusübergänge](#) (siehe Seite 468)

Arbeiten mit Statusübergängen und abhängigen Attributsteuerungen

So arbeiten Sie mit Statusübergängen und abhängigen Attributsteuerelementen:

1. Konfigurieren Sie auf der Registerkarte "Administration" geeignete Mandanten, Kontakte, und Rollen für Ihre Umgebung.
2. Geben Sie im Knoten "Service Desk" einen Ticket-Typ (beispielsweise "Change") an, und wählen Sie dann die Option "Status".

Auf der Seite "Statusliste" werden die aktiven Statuscodes angezeigt.

3. Bearbeiten Sie den bei Bedarf den Statuscode wie gewünscht (beispielsweise "Bestätigt") und verwenden Sie die verfügbaren Steuerelemente auf den Registerkarten am Fuß der Detailseite des Ticket-Status, um die folgenden Aufgaben auszuführen:

- [Konfigurieren der Statusübergänge](#) (siehe Seite 460)
- [Konfigurieren abhängiger Attributsteuerelemente](#) (siehe Seite 461)

Hinweis: Sie können einmalige Übergänge und abhängige Attributsteuerelemente für jeden Ticket-Typ konfigurieren.

Konfigurieren der Statusübergänge

Übergänge ermöglichen es Ihnen, eine Teilmenge der vollständigen Statusliste zu definieren und den neuen (oder nächsten) Standardstatus eines Tickets auf der Grundlage des aktuellen Status anzugeben. Übergänge werden erzwungen, wenn der Status auf dem Ticket-Detailformular geändert wird.

So konfigurieren Sie Statusübergänge:

1. Klicken Sie auf die Registerkarte "Übergänge" unten auf der Seite mit den Statusdetails für das Ticket.

Die Seite "Übergänge - Liste" enthält eine vollständige Liste der gültigen Übergänge für den Status.

Hinweis: Bei entsprechender Konfiguration werden zugehörige Übergangstypen in der Incident- und der Anfrageübergangsliste aufgeführt.

2. Klicken Sie auf die Schaltfläche "Übergänge aktualisieren".

Die Seite "Ticket-Statusübergänge aktualisieren" wird angezeigt.

3. Markieren Sie die folgenden Kontrollkästchen je nach Bedarf:

Erlaubt

Gibt einen gültigen Übergang für den Status an. Verwenden Sie diese Option, um Status-Workflows einzuschränken.

Standard

(Optional) Gibt den Standardstatusübergang an. CA SDM wendet den Standardübergang an, wenn ein Benutzer auf der Ticketdetailseite auf die Standardübergangsschaltfläche klickt oder ein Benutzer (auch: Webservice-Benutzer) den Status auf einen "<d>"-Wert aktualisiert. Für jeden Status (oder jeden Mandanten in einem mandantenfähigen System) ist nur ein Standardübergang vorhanden.

Kommentar erforderlich

(Optional) Gibt an, dass beim Ändern des Status in einem Ticket ein Aktivitätsprotokollkommentar erforderlich ist.

Hinweis: Diese Option gilt nur für CA SDM-Tickets. Es gilt nicht für andere Bereiche, wie Web-Services, oder die Funktion "In Liste bearbeiten".

4. (Optional) Wählen Sie in der Spalte "Name" einen Statuscode aus, um dessen Details zu aktualisieren.
5. Klicken Sie auf "Speichern".

Die Liste der für den neuen Status konfigurierten Übergängen wird auf der Übergangsliste angezeigt. Wenn der Analyst auf dem Formular des Tickets aus der Dropdownliste die Option "Status" auswählt, wird die neue Statusliste angezeigt.

Hinweis: Informationen zu Verfahren bei der Festlegung der Statusübergänge finden Sie in der *Online-Hilfe*.

Konfigurieren abhängiger Attributsteuerelemente

Mit abhängigen Attributsteuerelementen können Sie festlegen, welche Felder für den Ticket-Status angezeigt werden oder erforderlich sind.

Hinweis: Wenn Sie abhängige Attribute für den Ticket-Status als "erforderlich" konfigurieren, sollten Sie beachten, dass die Option "In Liste bearbeiten" auf der Seite des Tickets möglicherweise nicht die erforderlichen Attributfeldwerte anzeigt. Wenn der erforderliche Attributfeldwert nicht bereits in dem gespeicherten Ticket angegeben ist und auch nicht im Listenbearbeitungsformat vorhanden ist, wird das Ticket nicht gespeichert. Daher muss der Analyst die erforderlichen abhängigen Attributfeldwerte statt über die Option "In Liste bearbeiten" auf der Detailseite des Tickets bearbeiten.

So konfigurieren Sie ein abhängiges Attributsteuerelement:

1. Wählen Sie auf der Statusdetailseite des Tickets die Registerkarte "Abhängiges Attributsteuerelement" am Seitenende aus.

Die Attributsteuerungsliste wird angezeigt.

2. Klicken Sie auf "Erstellen".

Die Seite "Status abhängiger Attributsteuerelemente aktualisieren" wird angezeigt.

3. Füllen Sie die folgenden Felder aus:

Mandant

(Optional) Gibt in einem System mit installierter Mandantenfähigkeit einen optionalen Mandantennamen an. Wenn ein Mandant angegeben wird, gilt die Abhängigkeit nur für diesen Mandanten und seine Untermantanten.

Attribut

Gibt den Namen des zu steuernden Attributs an, z. B. "Zusammenfassung".

Gesperrt

Kennzeichnet das Attribut als gesperrt. Gesperrte Attribute, die einem Status zugeordnet sind, können in Tickets mit demselben Status nicht aktualisiert werden. Das Attribut wird entsperrt, wenn der Status geändert wird.

Erforderlich

Kennzeichnet das Attribut als erforderlich. Für erforderliche Attribute für einen Status darf in Tickets mit demselben Status nicht der Null-Wert verwendet werden.

4. Klicken Sie auf "Speichern".

Das neue Attributsteuerelement für den Status wird in der Liste der Attributsteuerelemente angezeigt, wenn Sie die Seite erneut aufrufen. Wenn ein Benutzer den Ticket-Status aktualisiert, ruft das System die Liste der erforderlichen Attribute ab, die dem neuen Status entsprechen, und aktualisiert das Ticket-Formular bei Bedarf. Wenn ein Benutzer versucht, ein Ticket zu schließen, und ein erforderliches Feld ist noch nicht ausgefüllt, wird oben im Formular des Tickets eine entsprechende Fehlermeldung angezeigt.

Hinweis: Informationen zu Verfahren bei der Festlegung der abhängigen Attributsteuerelemente finden Sie in der *Online-Hilfe*.

Web-Service-Methoden

Sie können den folgenden Statusübergang und abhängige Attributsteuerungsmethoden für SOAP-Webservices konfigurieren:

getValidTransitions

Listet die Transitionen für ein Ticket auf. Diese Methode ähnelt der vorhandenen Methode "getValidTaskTransitions", mit dem Unterschied, dass das Argument ein Ticket oder ein Status sein kann.

getDependentAttrControls

Listet die gesperrten und erforderlichen Attribute für ein Attribut eines Objekts mit permanenter ID auf. Das Status-Attribut wird ab diesem Zeitpunkt unterstützt.

Hinweis: Weitere Informationen zu Webservice-Methoden finden Sie im *technischen Referenzhandbuch*.

Vordefinierte Übergangsabläufe

Sie können für jeden Ticket-Typ die vordefinierten Statusübergänge verwenden, die im Lieferumfang des Produkts enthalten sind. Sie können diese Übergänge auch anpassen, um den Übergangsablauf in Ihrer Organisation zu modellieren.

Hinweis: Da Statusübergänge unter Integrationen wie CA Workflow von verschiedenen Komponenten genutzt werden können, sollten Sie die vordefinierten Statusübergänge nur dann deaktivieren, wenn dies explizit angefordert wird.

So zeigen Sie die Liste der vordefinierten Übergänge an:

Erweitern Sie auf der Registerkarte "Administration" den Knoten "Service Desk", und wählen Sie eine der folgenden Optionen:

- Change-Übertragungen
- Issue-Übergänge
- Anfrage-/Incident-/Problemübergänge

Die Übergangsliste zeigt die vordefinierten Übergänge an, über die Sie steuern können, wie ein Ticket (Incident/Anfrage/Problem, Change und Issue) seinen Lebenszyklus durchläuft.

Hinweis: Ausführliche Informationen zum Festlegen und Ändern von Übergängen finden Sie in der *Online-Hilfe*.

Incident-Übergangsablauf

Die folgende Tabelle enthält den vordefinierten Incident-Übergangsablauf.

Aktueller Status:	Standardübergang	Verfügbare Folgestatus
Bestätigt	In Bearbeitung <d>	Vermieden, Wartet auf Lieferant, Abgebrochen, Geschlossen, Ungelöst geschlossen, In Bearbeitung, Offen, Ausstehender Change, Gelöst
Vermieden		Bestätigt, Vermieden, Wartet auf Antwort des Endbenutzers, Geschlossen, Ungelöst geschlossen, In Bearbeitung, Lösung verworfen, Nachforschen, Gelöst
Wartet auf Antwort des Endbenutzers	Nachforschen <d>	Geschlossen, Ungelöst geschlossen, In Bearbeitung, Offen, Nachforschen, Gelöst
Wartet auf Anbieter	Nachforschen <d>	Bestätigt, Geschlossen, Ungelöst geschlossen, In Bearbeitung, Offen, Ausstehender Change, Nachforschen, Gelöst
Abgebrochen		Geschlossen
Geschlossen		Öffnen
Ungelöst geschlossen		Bestätigt
Ungelöst geschlossen		Geschlossen
Ungelöst geschlossen		Öffnen
Halten		Bestätigt, Geschlossen, In Bearbeitung, Offen, Ausstehender Change, Gelöst
In Bearbeitung	Nachforschen <d>	Bestätigt, Wartet auf Antwort des Endbenutzers, Wartet auf Lieferant, Geschlossen, Ungelöst geschlossen, Offen, Ausstehender Change, Nachforschen, Gelöst
Pending Change (Anstehende Änderung)	Nachforschen <d>	Bestätigt, Geschlossen, In Bearbeitung, Offen, Gelöst
Nachforschen	Gelöst <d>	Geschlossen, Offen, Gelöst
Gelöst	Geschlossen <d>	Wartet auf Antwort des Endbenutzers, Geschlossen, Offen

Problem-Übergangsablauf

Die folgende Tabelle enthält den vordefinierten Problem-Übergangsablauf.

Aktueller Status:	Standardübergang	Verfügbare Folgestatus
Bestätigt	In Bearbeitung <d>	Bestätigt, Genehmigt, Abgebrochen, Geschlossen, Behebung in Bearbeitung, Offen, Abgelehnt, Nachforschen
Analyse abgeschlossen	Genehmigt <d>	Bestätigt, Abgebrochen, Geschlossen, Behebung in Bearbeitung
Genehmigt	Behebung in Bearbeitung <d>	Geschlossen, Gelöst, Ausstehender Change
Wartet auf Anbieter	Nachforschen <d>	Bestätigt, Geschlossen, Ungelöst geschlossen, Gelöst, In Bearbeitung, Offen, Ausstehender Change, Nachforschen
Abgebrochen	Geschlossen <d>	Geschlossen, Ungelöst geschlossen, Offen
Ungelöst geschlossen		Bestätigt, Geschlossen, Offen
Behebung in Arbeit	Gelöst <d>	Bestätigt, Abgebrochen, Gelöst, Behebung in Arbeit, Nachforschen, Abgelehnt
Fest	Geschlossen <d>	Geschlossen
Halten	Nachforschen <d>	Bestätigt, Geschlossen, Gelöst, In Bearbeitung, Offen, Ausstehender Change, Nachforschen
In Bearbeitung	Nachforschen <d>	Bestätigt, Genehmigt, Abgebrochen, Geschlossen, Behebung in Bearbeitung, Ausstehender Change, Abgelehnt, Nachforschen
Bekannter Fehler	Behebung in Bearbeitung <d>	Geschlossen, Behebung in Bearbeitung, Gelöst
Öffnen	Bestätigt <d>	Bestätigt, Genehmigt, Abgebrochen, Geschlossen, Behebung in Bearbeitung, Abgelehnt, Nachforschen
Pending Change (Anstehende Änderung)	Gelöst <d>	Geschlossen, Nachforschen, Gelöst
Abgelehnt	Geschlossen <d>	Geschlossen, Ungelöst geschlossen, Offen
Nachforschen	Analyse abgeschlossen <d>	Bestätigt, Analyse abgeschlossen, Genehmigt, Abgebrochen, Geschlossen, Behebung in Bearbeitung, Gelöst, Abgelehnt

Issue-Übergangsablauf

Die folgende Tabelle enthält den vordefinierten Issue-Übergangsablauf.

Aktueller Status:	Standardübergang	Verfügbare Folgestatus
Bestätigt	In Bearbeitung <d>	Wartet auf Antwort des Endbenutzers, Wartet auf Lieferant, Geschlossen, Ungelöst geschlossen, In Bearbeitung, Offen, Ausstehender Change, Gelöst
Wartet auf Antwort des Endbenutzers	Nachforschen <d>	Bestätigt, Geschlossen, Ungelöst geschlossen, In Bearbeitung, Offen, Nachforschen
Wartet auf Anbieter	Nachforschen <d>	Bestätigt, Geschlossen, In Bearbeitung, Offen, Ausstehender Change, Nachforschen, Gelöst
Abgebrochen	Geschlossen <d>	Geschlossen
Geschlossen		Bestätigt, Offen.
Ungelöst geschlossen		Bestätigt, Geschlossen, Offen
Halten		Bestätigt, Geschlossen, In Bearbeitung, Offen, Ausstehender Change, Gelöst
In Bearbeitung	Nachforschen <d>	Bestätigt, Wartet auf Antwort des Endbenutzers, Wartet auf Lieferant, Geschlossen, Ungelöst geschlossen, Offen, Ausstehender Change, Nachforschen, Gelöst
Öffnen	Bestätigt <d>	Bestätigt, Durch Self-Service vermieden, Wartet auf Antwort des Endbenutzers, Wartet auf Lieferant, Geschlossen, Ungelöst geschlossen, In Bearbeitung, Ausstehender Change, Gelöst
Pending Change (Anstehende Änderung)	Nachforschen <d>	Bestätigt, Geschlossen, In Bearbeitung, Offen, Nachforschen, Gelöst
Nachforschen	Gelöst <d>	Geschlossen, Offen, Gelöst, Wartet auf Antwort des Endbenutzers, Geschlossen, Offen

Change-Übergangsablauf

Die folgende Tabelle enthält den vordefinierten Change-Übergangsablauf.

Aktueller Status:	Standardübergang	Verfügbare Folgestatus
Genehmigung in Arbeit	Genehmigt <d>	Bestätigt, Abgebrochen, Geschlossen

Aktueller Status:	Standardübergang	Verfügbare Folgestatus
Genehmigt	Geplant <d>	Abgebrochen, Geschlossen, Implementierung in Bearbeitung, Geplant
Rückgängig gemacht		Genehmigung in Arbeit, Geschlossen, Offen, RFC
Abgebrochen		Geschlossen
Kundenzurückstellung		Abgebrochen, Geschlossen, Implementierung in Bearbeitung, Abgelehnt, Geplant, Prüfung in Bearbeitung
Halten		Abgebrochen, Geschlossen, Implementierung in Bearbeitung, Geplant
Implementierung in Arbeit		Zurückgestellt, Abgebrochen, Geschlossen, Kundenzurückstellung, Abgelehnt, Geplant, Anbieterzurückstellung, Prüfung in Bearbeitung
Öffnen	RFC <d>	Genehmigung in Arbeit, Abgebrochen, Geschlossen, Kundenzurückstellung, Implementierung in Bearbeitung, Abgelehnt, RFC, Geplant, Anbieterzurückstellung
Abgelehnt	Geschlossen <d>	Genehmigung in Arbeit, Abgebrochen, Geschlossen
RFC	Genehmigung in Arbeit <d>	Genehmigung in Arbeit, Abgebrochen, Geschlossen, Kundenzurückstellung, Implementierung in Bearbeitung, Offen, Abgelehnt, Geplant, Anbieterzurückstellung
Geplant	Implementierung in Bearbeitung <d>	Abgebrochen, Geschlossen, Kundenzurückstellung, Implementierung in Bearbeitung, Anbieterzurückstellung, Prüfung in Bearbeitung, Abgebrochen, Geschlossen, Implementierung in Bearbeitung, Geplant, Zurückgestellt, Geschlossen

Best Practices: Vordefinierte Statusübergänge

Die vordefinierten, mit dem Produkt gelieferten Statusübergänge sind "aktiv" in einer neuen Installation und "inaktiv" nach der Aktualisierung. Für jeden auf der Seite mit der Übergangsliste aufgelisteten Status ist ein Standard-Statusübergang (oder nächster Status) vorhanden. Der von Standard-Statusübergang gewählte Pfad stellt die Best Practice dar. Die zusätzlichen auf der Übergangsliste aufgelisteten Statusübergänge dienen dazu, eine Reihe von Ticketverwaltungs-Workflows durchzuführen. Allerdings können nur "aktive" Statusübergänge, die diese Best Practice verwenden, sicherstellen, dass der richtige Workflow für die Verwaltung von Requests, Incidents, Problemen und Changes verwendet wird. Diese Best Practice unterstützt die Verschiebung der Tickets auf dem Weg zu Lösung und Abschluss in der IT-Umgebung.

So sind z. B. die folgenden vordefinierten Incident-Übergänge, die auf der Seite "Incident-Übergang - Liste" aufgelistet sind, auf "inaktiv" gesetzt, um die Lösung und den Abschluss von Incidents zu unterstützen:

Status	Neuer Status	Standard	Status Description	Datensatzstatus
Bestätigt	Geschlossen	No	Statusübergang: von "Bestätigt" auf "Geschlossen"	Inaktiv
Bestätigt	Ungelöst geschlossen	No	Statusübergang: von "Bestätigt" auf "Ungelöst geschlossen"	Inaktiv
Bestätigt	Öffnen	Ja	Statusübergang: von "Bestätigt" auf "Offen"	Inaktiv
Wartet auf Antwort des Endanwenders	Bestätigt	No	Statusübergang: von "Wartet auf Antwort des Endanwenders" auf "Bestätigt"	Inaktiv
Wartet auf Antwort des Endanwenders	Öffnen	No	Statusübergang: von "Wartet auf Antwort des Endanwenders" auf "Öffnen"	Inaktiv
Wartet auf Anbieter	Bestätigt	No	Statusübergang: von "Wartet auf Anbieter" auf "Bestätigt"	Inaktiv
Wartet auf Anbieter	Geschlossen	No	Statusübergang: von "Wartet auf Anbieter" auf "Geschlossen"	Inaktiv
Wartet auf Anbieter	Öffnen	No	Statusübergang: von "Wartet auf Anbieter" auf "Offen"	Inaktiv
Geschlossen	Bestätigt	No	Statusübergang: von "Geschlossen" auf "Bestätigt"	Inaktiv

Status	Neuer Status	Standard	Status Description	Datensatzstatus
Ungelöst geschlossen	Bestätigt	No	Statusübergang: von "Ungelöst geschlossen" auf "Bestätigt"	Inaktiv
Ungelöst geschlossen	Geschlossen	No	Statusübergang: von "Ungelöst geschlossen" auf "Bestätigt"	Inaktiv
Halten	Bestätigt	No	Statusübergang: von "Halten" auf "Bestätigt"	Inaktiv
Halten	Geschlossen	No	Statusübergang: von "Halten" auf "Geschlossen"	Inaktiv
Halten	Öffnen	No	Statusübergang: von "Halten" auf "Offen"	Inaktiv
In Bearbeitung	Bestätigt	No	Statusübergang: von "In Bearbeitung" auf "Bestätigt"	Inaktiv
In Bearbeitung	Geschlossen	No	Statusübergang: von "In Bearbeitung" auf "Geschlossen"	Inaktiv
In Bearbeitung	Öffnen	No	Statusübergang: von "In Bearbeitung" auf "Offen"	Inaktiv
Öffnen	Geschlossen	No	Statusübergang: von "Offen" auf "Geschlossen"	Inaktiv
Pending Change (Anstehende Änderung)	Bestätigt	No	Statusübergang: von "Ausstehender Change" auf "Bestätigt"	Inaktiv
Pending Change (Anstehende Änderung)	Geschlossen	No	Statusübergang: von "Ausstehender Change" auf "Geschlossen"	Inaktiv
Pending Change (Anstehende Änderung)	Öffnen	No	Statusübergang: von "Ausstehender Change" auf "Offen"	Inaktiv
Nachforschen	Öffnen	No	Statusübergang: von "Nachforschen" auf "Offen"	Inaktiv

Statusübergänge für Self-Service

Mit Hilfe von Statusübergängen können Sie den Statuswechsel eines Tickets kontrollieren (z. B. von "Offen" zu "Geschlossen"). Für Mitarbeiter, die Self-Service verwenden, können Sie Schaltflächen auf den Incident- und Request-Detailformularen hinzufügen, um [Statusübergänge](#) (siehe Seite 458) anzuzeigen.

Die Schaltfläche "Statusübergang" für Incident- und Request-Prozessworkflows wird in der Mitarbeiterschnittstelle angezeigt, wenn Incident- oder Request-Übergänge mit aktiven Übergangstypen verbunden sind. Ein Übergangstyp definiert den Schaltflächentext und steuert das Verhalten des Ticket-Detailformulars. Beim Definieren von Schaltflächen werden die Legacy-Schaltflächen "Incident schließen" (bzw. "Request schließen") und "Incident neu öffnen" (bzw. "Request neu öffnen") nicht auf den Ticket-Detailformularen angezeigt. Stattdessen kann der Mitarbeiter den Status des Incidents oder des Request nur mit Hilfe der vom Administrator konfigurierten Statusübergangsschaltflächen ändern.

Da alle mit dem Produkt gelieferten vordefinierten Übergangstypen standardmäßig inaktiv sind, sind keine Statusübergangsschaltflächen aktiviert. Als Systemadministrator können Sie vordefinierte Übergangstypen aktivieren und ändern oder Übergangstypen erstellen, um Ihre Statusübergang-Workflows aufzunehmen. Wenn Sie einen Übergangstyp erstellt oder geändert haben, können Sie ihn danach mit jedem beliebigen Incidentstatus- oder Request-Statusübergang verbinden.

Hinweis: Weitere Informationen zum Verwenden von Übergangstypen finden Sie in der *Online-Hilfe*.

Weitere Informationen:

[Funktionsweise der Übergänge für Self-Service](#) (siehe Seite 470)

[Erstellen oder Aktualisieren von Übergangstypen für Übergänge](#) (siehe Seite 471)

[Verknüpfen von Übergangstypen mit Übergängen](#) (siehe Seite 472)

[Aktivieren von vordefinierten Übergangstypen](#) (siehe Seite 472)

Funktionsweise der Übergänge für Self-Service

Mit Übergangstypen und den entsprechenden Status wird wie folgt gesteuert, wann Mitarbeiter Tickets schließen und neu öffnen können:

1. Aktive Übergangstypen werden durch den Administrator mit Incident- (oder Anfrage-) Statusübergängen verknüpft.
2. Der Mitarbeiter erstellt einen Incident mit Hilfe von Self-Service.
3. Der dem Incident zugewiesene Analyst findet eine Lösung und versetzt das Ticket in den Status "Gelöst".

4. Wenn das Ticket im Status "Gelöst" ist, werden auf dem Mitarbeiterdetailformular Statusübergangsschaltflächen zum Annehmen oder Ablehnen der Lösung angezeigt.
 - Wenn der Mitarbeiter die Lösung akzeptiert, erfolgt der Übergang von "Gelöst" zu "Geschlossen".
 - Wenn der Mitarbeiter die Lösung ablehnt, erfolgt der Übergang von "Gelöst" zu "Offen".
5. Wenn der Mitarbeiter auf eine Schaltfläche geklickt hat, kann er Anmerkungen in das angezeigte Lösungsformular einfügen.

Erstellen oder Aktualisieren von Übergangstypen für Übergänge

Als Systemadministrator können Sie auf der Seite "Übergangstypenliste" Übergangstypen für Workflows von Incident- und Anfragestatusübergängen erstellen und aktualisieren.

So erstellen Sie einen Übergangstyp für einen Statusübergang:

1. Wählen Sie auf der Registerkarte "Administration" die Option "Service Desk" > "Anfragen/Incidents/Probleme" > "Übergangstypen" aus.
2. Klicken Sie auf der Listenseite auf "Erstellen".
3. Bearbeiten Sie die Felder auf der Detailseite.

Der Übergangstyp für den Statusübergang wird erstellt.

4. Klicken Sie auf "Speichern".

Der neue Übergangstyp wird in der Übergangstypenliste angezeigt, wenn Sie die Seite wieder einblenden.

So aktualisieren Sie einen Übergangstyp:

1. Öffnen Sie auf der Seite "Übergangstyp – Liste" den gewünschten Übergangstyp zum Bearbeiten.
2. Bearbeiten Sie die Felder nach Bedarf.
3. Klicken Sie auf "Speichern".

Der aktualisierte Übergangstyp wird auf der Liste "Übergangstyp" angezeigt.

Verknüpfen von Übergangstypen mit Übergängen

Wenn Statusübergänge mit Übergangstypen verknüpft sind, werden auf dem Ticket-Detailformular des Mitarbeiters Statusübergangsschaltflächen zum Annehmen oder Ablehnen der Lösung angezeigt. Um einen Übergangstyp mit einem Statusübergang zu verknüpfen, gehen Sie wie folgt vor:

1. Wählen Sie auf der Registerkarte "Administration" die Option "Service Desk" > "Anfragen/Incidents/Probleme" > "Incident-Übergänge" (oder "Anfrage-Übergänge") aus.
2. Öffnen Sie auf der Seite "Anfrage-Übergang - Liste" oder "Incident-Übergang - Liste" den gewünschten Statusübergang zum Bearbeiten.
3. Geben Sie den gewünschten Übergangstyp im Feld "Übergangstyp" an.
4. Klicken Sie auf "Speichern".

Der Übergangstyp wird mit dem Statusübergang verknüpft.

Aktivieren von vordefinierten Übergangstypen

Da alle mit dem Produkt gelieferten vordefinierten Übergangstypen standardmäßig inaktiv sind, sind keine Statusübergangsschaltflächen aktiviert. Sie können diese Übergangstypen aktivieren und ändern, um sie dem gewünschten Statusübergangsablauf anzupassen.

So aktivieren Sie einen vordefinierten Übergangstyp:

1. Wählen Sie auf der Seite "Übergangstyp – Liste" die Option "Filter anzeigen".
Im oberen Teil der Seite werden weitere Suchfelder angezeigt.
2. Wählen Sie im Feld "Datensatzstatus" die Option "Inaktiv", und klicken Sie auf "Suchen".

Auf der Seite "Übergangstyp – Liste" werden alle inaktiven Übergangstypen angezeigt.

3. Klicken Sie mit der rechten Maustaste auf den gewünschten Übergangstyp und wählen Sie im Menü die Option "Bearbeiten".
4. Wählen Sie im Feld "Datensatzstatus" die Option "Aktiv".
5. Klicken Sie auf "Speichern" und "Fenster schließen".
6. Klicken Sie auf "Suche".

Auf der Seite "Übergangstyp – Liste" wird der aktive Übergangstyp angezeigt.

Weitere Informationen:

[Beispielübergangstypen für Incident-Statusübergänge](#) (siehe Seite 473)

[Beispielübergangstypen für Request-Statusübergänge](#) (siehe Seite 473)

Beispielübergangstypen für Incident-Statusübergänge

Die folgende Tabelle beschreibt die Beispielübergangstypen für Incident-Statusübergänge:

Symbol	Schaltflächentext	Kopfzeilentext des Formulars	Incident-Statusübergang
Schaltfläche "Vorgangslösung akzeptieren"	Annehmen	Lösung akzeptieren	"Gelöst" zu "Geschlossen"
Schaltfläche "Vorgangslösung ablehnen"	Ablehnen	Lösung ablehnen	"Gelöst" zu "Offen"
Schaltfläche zum Ablehnen der Incident-Schließung	Schließung anfordern	Schließung anfordern	■ Von "Offen" zu "Ungelöst geschlossen" ■ Wartet auf Antwort des Endanwenders ■ Wartet auf Anbieter ■ In Bearbeitung ■ Bestätigt

Beispielübergangstypen für Request-Statusübergänge

Die folgende Tabelle beschreibt die Beispielübergangstypen für Request-Statusübergänge:

Hinweis: Der Status "Schließung angefordert" für Requests ist die Entsprechung des Status "Gelöst" für Incidents.

Symbol	Schaltflächentext	Kopfzeilentext des Formulars	Request-Statusübergang anfordern
Schaltfläche "Request-Lösung akzeptieren"	Annehmen	Lösung akzeptieren	"Schließung angefordert" zu "Geschlossen"

Symbol	Schaltflächentext	Kopfzeilentext des Formulars	Request-Statusübergang anfordern
Schaltfläche "Request-Lösung ablehnen"	Ablehnen	Lösung ablehnen	"Schließung angefordert" zu "Offen"
Schaltfläche "Request schließen"	Schließung anfordern	Schließung anfordern	■ Von "Abgebrochen" zu "Offen" ■ Wartet auf Antwort des Endanwenders ■ Wartet auf Anbieter ■ Genehmigung in Bearbeitung ■ Bestätigt
Schaltfläche "Request schließen"	Schließen	Schließung angefordert	Von "In Bearbeitung" zu "Geschlossen"

Timer

Timer fungieren als Stoppuhr mit verschiedenen Grenzwerten, die dem Analysten Angaben über die verstrichene Zeit liefern. Sie können die Zeit definieren, die der Timer an jedem Grenzwert verweilt, und Sie können angeben, dass der Timer die Farbe ändern, einen Signalton ausgeben oder eine Erinnerung anzeigen soll, wenn er einen Grenzwert erreicht. Ein Service Desk-Analyst kann die Stoppuhr nicht steuern; dies ist nur dem Administrator vorbehalten.

Anfragen sind der einzige Tickettyp, der Timer verwendet. Daher müssen Sie Timer für das interne und kombinierte Service Desk-Modell einrichten.

Die folgenden Grenzwerte sind für Timer vordefiniert:

Grenzwertdauer	Farbe
00:00:00	Grün
00:01:00	Gelb
00:05:00	Rot

Die vordefinierten Werte starten den Timer bei Grün. Nach einer Minute ändert der Timer seine Farbe in Gelb. Nach 5 Minuten ändert der Timer seine Farbe in Rot. Die verstrichene Zeit wird angezeigt, wenn der Analyst die Anfrage im Detail anzeigt. Sie wird jeweils zurückgesetzt, wenn eine neue Anfrage ausgewählt wird.

Sie können einen Timer als aktiv oder inaktiv kennzeichnen. Wenn Sie einen Timer als inaktiv kennzeichnen, ist er nicht länger Teil des Prozesses, bleibt aber für die spätere Verwendung verfügbar (d. h., er wird nicht aus der Datenbank gelöscht). Wenn Sie später entscheiden, den Timer zu verwenden, kehren Sie zu ihm zurück, und markieren Sie ihn als aktiv.

Zeitzone

Sie können bestimmte Zeitzone für Server, Servicetypen, Kontakte und Lokationen in Ihrem CA SDM-System einrichten. So können Sie sowohl lokale Servicetypen einrichten, die für eine bestimmte Zeitzone gelten, als auch globale Servicetypen, die für das gesamte Unternehmen gelten. Damit muss der Administrator auch nicht mehr wissen, in welcher Zeitzone sich ein Server befindet, und er muss die Schichtzeiten nicht mehr manuell an die verschiedenen Zeitzone anpassen.

Weitere Informationen:

[Auslöser für Servicetypereignisse](#) (siehe Seite 475)

[Zeitzone-Event-Auslöser](#) (siehe Seite 476)

[Zeitzoneregeln](#) (siehe Seite 477)

Auslöser für Servicetypereignisse

Servicetypen definieren die Ereignisse, die nach einer angegebenen Zeitverzögerung ausgelöst werden.

Beispiel: Ereignis-Auslöser gemäß Schicht-Ablaufplan

In diesem Beispiel beschränkt ein Schicht-Ablaufplan, der mit dem Servicetyp verknüpft ist, den tatsächlichen Zeitpunkt, zu dem ein Ereignis ausgelöst wird:

- Schicht von 8:00 bis 17:00 Uhr.
- Die Ereignisverzögerung beträgt 3 Stunden.
- Aktuelle Serverzeit 15:00 Uhr.

Das Ereignis wird morgen um 9:00 Uhr Serverzeit aus folgendem Grund ausgelöst:

- Entsprechend der aktuellen Serverzeit verbleiben in der aktuellen Schicht noch zwei Stunden (aktuelle Uhrzeit 15:00 Uhr; Schicht endet um 17:00 Uhr)
- Die Ereignisverzögerung beträgt 3 Stunden. Zwei Stunden dieser Verzögerung fallen in die Schicht des aktuellen Tags (15:00 Uhr bis 17:00 Uhr) Eine zusätzliche Verzögerungsstunde wird in die Schicht des nächsten Tags übertragen (8:00 Uhr bis 9:00 Uhr)

Folglich beginnt das Ereignis am folgenden Tag um 9:00 Uhr.

Zeitzone-Event-Auslöser

Eine Zeitzone, die mit dem Servicetyp verknüpft wird, kann die Uhrzeiten zum Auslösen von Events beschränken.

Beispiel: Event-Auslöser nach Zeitzone

In diesem Beispiel beschränkt eine Zeitzone, die mit dem Servicetyp verknüpft ist, den tatsächlichen Zeitpunkt, zu dem ein Event ausgelöst wird, wie folgt:

- Schicht von 8:00 bis 17:00 Uhr.
- Die Event-Verzögerung beträgt 3 Stunden.
- Aktuelle Serverzeit 15:00 Uhr.
- Aktuelle Uhrzeit in Zeitzone ist 12:00 Uhr.

Das Event wird heute um 18:00 Uhr Serverzeit aus folgendem Grund ausgelöst:

- Entsprechend der aktuellen Serverzeit verbleiben in der aktuellen Schicht noch zwei Stunden (aktuelle Uhrzeit 15:00 Uhr; Schicht endet um 17:00 Uhr).
- Entsprechend der aktuellen Uhrzeit der Zeitzone verbleiben fünf Stunden für die Schicht für heute (aktuelle Uhrzeit 12:00 Uhr; Schicht endet um 17:00 Uhr).
- Die Event-Verzögerung beträgt drei Stunden (00:00 Uhr bis 3:00 Uhr Uhrzeit der Zeitzone; 15:00 Uhr bis 18:00 Uhr Serverzeit).

Folglich fängt das Event um 18:00 Uhr Serverzeit oder 15:00 Uhr Zeitzonezeit an.

Zeitzone

Sie können eine Zeitzone für einen Server, für eine Lokation und für einen Servicetyp angeben. Sie können auch CA SDM anweisen, die Zeitzone des betroffenen Endanwenders eines Tickets zu benutzen. CA SDM verwendet die folgenden Regeln, um zu bestimmen, welche Zeitzone ein Event auslöst:

- **Zeitzone des betroffenen Endanwenders** - CA SDM verwendet diese Regel, wenn die folgenden Bedingungen gelten:
 - Die Option "Zeitzone des Endanwenders verwenden" ist ausgewählt.
 - Für den betroffenen Endanwender des Tickets ist eine Zeitzone angegeben.
- **Zeitzone der betroffenen Endanwenderlokation** - CA SDM verwendet diese Regel, wenn die folgenden Bedingungen gelten:
 - Die Option "Zeitzone des Endanwenders verwenden" ist ausgewählt.
 - Für den betroffenen Endanwender des Tickets ist keine Zeitzone angegeben.
 - Für die betroffene Endanwenderlokation ist eine Zeitzone angegeben.
- **Servicetyp-Zeitzone** - CA SDM verwendet diese Regel, wenn die folgenden Bedingungen gelten:
 - Für den Servicetyp ist eine Zeitzone angegeben.
 - Die Option "Zeitzone des Endanwenders verwenden" ist nicht ausgewählt.
- **Serverzeitzone** - CA SDM verwendet diese Regel, wenn die folgenden Bedingungen gelten:
 - Für den Server ist eine Zeitzone angegeben.
 - Die Option "Zeitzone des Endanwenders verwenden" ist nicht ausgewählt.
 - Für den Server ist keine Zeitzone angegeben.
- **Kein Zeitzonensupport** - CA SDM verwendet diese Regel, wenn die folgenden Bedingungen gelten:
 - Für den Server ist keine Zeitzone angegeben.
 - Die Option "Zeitzone des Endanwenders verwenden" ist nicht ausgewählt.
 - Es gibt keine Server-Datensätze.

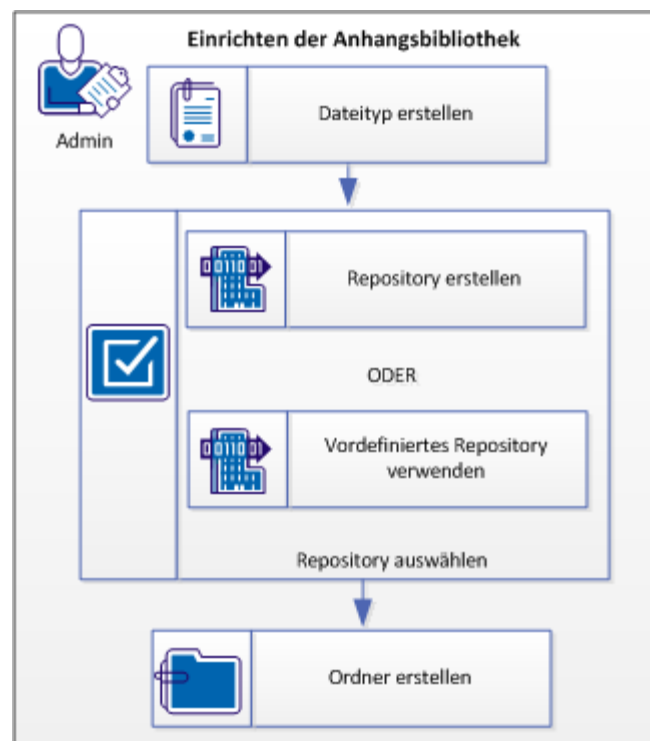
So richten Sie die Anhangsbibliothek ein

Sie können verschiedenen CA SDM-Entitäten verschiedene Anhangstypen hinzufügen. Zum Beispiel kann ein Kunde einen Snapshot eines Fehlers an den Incident anhängen. Als Administrator richten Sie die Anhangsbibliothek ein, wo Anwender Anhänge hochladen oder herunterladen können.

Anhänge können folgendermaßen klassifiziert werden:

- **Gespeichert:** Der Webserver verwendet das HTTP-Protokoll, um die gespeicherten Anhänge hochzuladen und in einem Repository zu speichern. Wenn ein Analyst einen gespeicherten Anhang überprüft, wird die Datei aus dem Repository abgerufen, und die Datei wird lokal angezeigt. Durch Verwendung eines Webserver zum Speichern von Dateien können Dateien über die Anwenderschnittstelle gespeichert und abgerufen werden.
- **Verknüpft:** Speichert nur eine Verknüpfung zur Datei in der Datenbank.

Folgendes Diagramm zeigt, wie eine Anhangsbibliothek eingerichtet werden sollte:



Gehen Sie wie folgt vor:

1. [Öffnen Sie die CA SDM-Web-Benutzeroberfläche.](#) (siehe Seite 202)
2. [Erstellen Sie einen Dateityp](#) (siehe Seite 479).
3. [Wählen Sie das Repository aus](#) (siehe Seite 480).

- [Richten Sie ein Repository auf einem Remote-Computer ein](#) (siehe Seite 482).
 - [Erstellen Sie ein Repository](#) (siehe Seite 482).
 - [Verwenden Sie ein vordefiniertes Repository](#) (siehe Seite 483).
4. [Erstellen Sie einen Ordner](#) (siehe Seite 487).

Öffnen der CA SDM-Web-Benutzeroberfläche

Melden Sie sich in der Web-Benutzeroberfläche aus folgenden Servern an, abhängig von Ihrer CA SDM-Konfiguration:

- Konventionell: Primärserver oder Sekundärserver
- Erweiterte Verfügbarkeit: Anwendungsserver oder Hintergrundserver

Erstellen von Dateitypen

CA SDM gibt vordefinierte Dateitypen an, die die Anhänge unterstützen können. Zum Beispiel unterstützt Adobe Acrobat, der vordefinierte Dateityp, die PDF-Dateiformate als Anhänge. Sie können auch Dateitypen erstellen. Erstellen Sie zum Beispiel den Dateityp "JPEG", den Anwender verwenden können, um einen Snapshot für einen Incident hochzuladen.

Gehen Sie wie folgt vor:

1. Melden Sie sich von folgenden CA SDM-Servern aus in der Web-Benutzeroberfläche an, abhängig von Ihrer CA SDM-Konfiguration:
 - Konventionell: Primärserver oder Sekundärserver
 - Erweiterte Verfügbarkeit: Anwendungsserver oder Hintergrundserver
2. Wählen Sie auf der Registerkarte "Administration" die Optionen "Anhangbibliothek", "Dateitypen" aus.

Die Seite "Dateitypen - Liste" wird geöffnet.
3. Klicken Sie auf "Neu erstellen".

Die Seite "Create New File Type" wird geöffnet.

4. Füllen Sie die folgenden Felder aus:

Typ

Gibt den Dateityp an oder identifiziert die dazugehörige Softwareanwendung, z. B. Word-Dokument, Bild, ausführbare Datei.

Erweiterung

Gibt die Zeichen an, die an den Basisdateinamen angehängt werden und den Dateityp bestimmen. Zum Beispiel kennzeichnet die Erweiterung doc ein Microsoft Word-Dokument.

Symbolname

Gibt den Namen der Grafikdatei an, die das Symbol enthält, das zur Kennzeichnung dieses Dateityps verwendet wird.

Status

Zeigt an, ob der Datensatz in der Datenbank aktiv und für die Verwendung verfügbar ist.

5. Klicken Sie auf "Speichern".

Der Dateityp ist nun erstellt.

Auswählen des Repository

Die Anhänge werden in Repositorys gespeichert, und Sie müssen die Repositorys einrichten, bevor Anwender mit Anhängen arbeiten können. Sie können beliebig viele Repositorys hinzufügen, um die Anforderungen Ihrer Organisation optimal zu erfüllen. Sie können z. B. separate Repositorys zum Speichern von Dateianhängen und Bildern hinzufügen. Zur besseren Dateiverwaltung können den Repositorys auch Ordner hinzugefügt werden, in die die Dateien anschließend hochgeladen werden.

Alle Client-Schnittstellen können auf vorhandene Repositorys zugreifen, um Dateianhänge hoch- bzw. herunterzuladen. Dabei gelten folgende Ausnahmen:

- Auf freigegebene Datei-Repositorys kann nur zugegriffen werden, wenn der Repository Daemon auf einem Computer ausgeführt wird, der auf die freigegebene Datei zugreifen kann. Der Servername in dem Repository-Datensatz (Detailformular) muss ein Windows-Computer sein, der Zugriff auf die Freigabe hat. Außerdem muss ein CA SDM Repository Daemon auf dem Computer ausgeführt werden.
- Das Herunterladen von Zip-Dateien hängt davon ab, wann sie heraufgeladen wurden. Anhänge von früheren Versionen werden heruntergeladen, ohne sie zu entpacken. Entpacken Sie die Datei auf dem Client-Computer; andernfalls werden Anhänge, die von einer Client-Schnittstelle hochgeladen werden, ebenfalls heruntergeladen, ohne sie zu entpacken. Das heißt, der Server entpackt die Datei während einer Download-Anfrage vom Client, bevor er die Datei zurückgibt.

Die verteilte Architektur ermöglicht die anwenderdefinierte Konfiguration der Repositorys eines Standorts. Das Servlet für ein Repository muss sich nicht auf dem gleichen Server wie die angehängten Dateien befinden. Ein Standort kann über ein zentrales Servlet für den Zugriff auf alle verteilten Repositorys verfügen. Wahlweise können Sie aber auch für jeden Repository-Server im Standort ein eigenes Servlet festlegen.

Die folgenden Setups sind bei der Konfiguration der Repositorys möglich:

- **Repository-Server auf einem geschützten CA SDM-Server** — Wenn Sie einen Repository-Server auf einem geschützten CA SDM-Server hinter einer Firewall einrichten, müssen Sie das Servlet nicht auf diesem Computer bereitstellen. Legen Sie stattdessen die Ausführung des Servlets auf einem anderen CA SDM-Server oder einem uneingeschränkten CA SDM-Server fest, wobei weiterhin ein erfolgreicher Upload oder Download zum Repository möglich ist. Abhängig von dem Netzwerk zwischen dem Repository-Server und dem Servlet-Server können einige Leistungsauswirkungen beim Hochladen und beim Herunterladen auftreten. Eine gute Art der Einrichtung für ein Remote-Repository ist die Installation und Konfiguration eines anderen Servers mit dem Repository auf dem Remote-Server und die Einstellung des Upload-Pfades als lokaler Pfad. Weitere Informationen finden Sie unter dem Thema [Einrichten eines Repository auf einem Remote-Computer](#). (siehe Seite 482)
- **Servlet auf dem gleichen Server wie der Repository-Server** - Standorte, die eine optimale Leistung beim Hochladen und Herunterladen von Anhängen wünschen, sollten das Servlet auf dem gleichen Server wie dem Repository-Server ausführen. Bei dieser Lösung muss der Tomcat-Port (normalerweise 8080) auf dem Server bereitgestellt werden. Diese Lösung bietet sich an, wenn der Computer sich hinter einer Firewall befindet.

CA SDM stellt vordefinierte Repositorys bereit, und ermöglicht es Ihnen, Ihre eigenen Repositorys zu erstellen, um sie den Anforderungen Ihrer Organisationsbedarf optimal anzupassen. Wählen Sie eine der folgenden Optionen:

- [Erstellen Sie ein Repository](#) (siehe Seite 482).
- [Verwenden Sie ein vordefiniertes Repository](#) (siehe Seite 483).

Einrichten eines Repository auf einem Remote-Computer

Standardmäßig befinden sich die Repositorys auf folgendem Server, abhängig von Ihrer CA SDM-Konfiguration:

- Konventionell: Primärserver
- Erweiterte Verfügbarkeit: Hintergrundserver

Die standardmäßigen Repositorys verwenden sowohl das Servlet als auch den Repository-Daemon (rep_daemon) von diesen Servern. Um ein Repository auf einem Remote-Computer zu erstellen, müssen Sie folgende Server abhängig von Ihrer CA SDM-Konfiguration installieren und konfigurieren:

- Konventionell: Sekundärserver. Das Servlet wird auf dem Primärserver ausgeführt, und "rep_daemon" wird auf dem Sekundärserver ausgeführt.
- Erweiterte Verfügbarkeit: Hintergrundserver. Das Servlet wird auf dem Anwendungsserver ausgeführt, und "rep_daemon" wird auf dem Hintergrundserver ausgeführt.

In der Konfiguration für erweiterte Verfügbarkeit wird "rep_daemon" standardmäßig auf allen Servern ausgeführt.

In der konventionellen Konfiguration wird "rep_daemon" standardmäßig auf dem Primärserver ausgeführt, und Sie müssen überprüfen, ob "rep_daemon" auf dem Sekundärserver für dieses Setup ausgeführt wird.

(Nur für konventionelle Konfiguration) Gehen Sie wie folgt vor:

1. Wählen Sie auf der Registerkarte "Administration" die Option "System", "Konfigurationen" aus.

Die Seite "Konfiguration - Liste" wird geöffnet.

2. Wählen Sie die Konfiguration für den Sekundärserver aus.

Die Seite "Konfigurationsdetail" wird geöffnet.

3. Klicken Sie auf "Zusätzliche Prozesse".

"Zusätzlicher Prozess - Liste" wird angezeigt.

4. Klicken Sie auf "Prozess hinzufügen".

5. Wählen Sie Repository-Daemon als Prozess aus.

6. Klicken Sie auf "Speichern".

Das Repository wird auf dem Sekundärserver eingerichtet.

Erstellen eines Anhang-Repository

Abhängig von Ihren Organisationsanforderungen können Sie ein großes Repository oder mehrere kleine Repositorys haben. Die Verschiebung oder Kombination von Repositorys ist einfach, da alle Attribute zu einem Repository im Repository-Datensatz definiert sind.

Gehen Sie wie folgt vor:

1. Wählen Sie auf der Registerkarte "Administration" die Optionen "Anhangbibliothek", "Repositorys" aus.

Die Seite "Repositorys" wird angezeigt.

2. Klicken Sie auf "Neu erstellen".

Die Seite "Neues Repository erstellen" wird geöffnet.

Hinweis: Wenn Sie der Service Provider sind, wählen Sie den entsprechenden Mandanten auf der Seite "Neues Repository erstellen" aus. Durch die Option "öffentlich (freigeben)" wird das Repository für alle Mandanten verfügbar.

3. Füllen Sie die übrigen Repository-Felder nach Bedarf aus.

4. Klicken Sie auf "Speichern".

Das Repository wird erstellt.

Verwenden eines vordefinierten Anhangs-Repository

Sie können ein vordefiniertes Repository verwenden ("Service Desk" oder "Knowledge" oder "Bilder"). Sie können ein Repository bearbeiten, um die Anforderungen Ihrer Organisation optimal anzupassen.

Gehen Sie wie folgt vor:

1. Wählen Sie auf der Registerkarte "Administration" die Optionen "Anhangbibliothek", "Repositorys" aus.

Die Seite Repositorys - Liste wird geöffnet.

2. Klicken Sie mit der rechten Maustaste auf das Repository, das Sie bearbeiten möchten, und wählen Sie "Bearbeiten" aus.

Die Seite "Repository aktualisieren" wird geöffnet.

3. Bearbeiten Sie die Felder nach Bedarf. Weitere Informationen finden Sie im Thema "Repository - Felder".

4. Klicken Sie auf "Speichern".

Die Repository-Definition wird gespeichert.

Repository - Felder

Folgende Felder werden verwendet, um ein Repository zu bearbeiten oder zu erstellen.

Name

Gibt den Namen an, um das Repository eindeutig zu identifizieren. Zum Beispiel kann das Repository "Incident-Bilder" alle Bilder speichern, die mit einem Incident verknüpft sind.

Repository-Typ

Gibt den Inhaltstyp an, der im Repository gespeichert ist. Um zum Beispiel Bildanhänge zu speichern, wählen Sie Bilder aus.

Standard

Gibt an, ob dies das standardmäßige Repository für den angegebenen Repository-Typ ist. Zum Beispiel: Wenn der Anwender den Incident erstellt und den Anhang an den Incident anhängen möchte, dann wird das standardmäßige Repository für die Auswahl angezeigt. Sie können nur ein Repository als Standard festlegen.

Dateigrößenbeschränkung (KB)

Gibt die maximale Größe der Datei (in Kilobyte) an, die ein Anwender in das Repository hochladen kann.

Upload-Pfad

Gibt den vollständigen Stammverzeichnispfad oder den UNC-Pfad an, wo sich die Dateien befinden, die auf das Repository hochgeladen wurden.

UNC-Daten

Gibt die Anmeldeinformationen an, um auf den UNC-Pfad zuzugreifen, der im Feld Upload-Pfad angegeben ist. Klicken Sie auf UNC-Daten, um die Seite Anmeldeinformationen - Suche zu öffnen.

- Wenn Sie die Anmeldeinformationen bereits erstellt haben, um auf den angegebenen UNC-Pfad zuzugreifen, führen Sie eine Suche mithilfe der Felder durch, und wählen Sie die Anmeldeinformationen aus.
- Wenn Sie die Anmeldeinformationen erstellen möchten, klicken Sie auf "Neu erstellen". Weitere Informationen über das Erstellen von Anmeldeinformationen finden Sie unter dem Thema "[Erstellen von UNC-Daten](#)" (siehe Seite 486)".

Hintergrundservices

Gibt die Services des Hintergrundservers für den Servlet-Pfad und für "rep_daemon" an.

Keine

Gibt an, dass der Hintergrundserver nicht für den Servlet-Pfad oder für "rep_daemon" verwendet wird. Wenn Sie diese Option auswählen, geben Sie die Werte für die Felder Servlet-Server und Repository-Server ein.

Nur Servlet

Gibt an, dass das Servlet auf dem Hintergrundserver gehostet wird. Wenn Sie diese Option auswählen, dann wird das Feld Servlet-Server automatisch mit dem Wert Hintergrundserver aufgefüllt. Geben Sie den Wert für das Feld Repository-Server ein. Wenn der Hintergrundserver heruntergefahren wird und der Standby-Server als neuer Hintergrundserver hochgestuft wird, dann wird das Feld Servlet-Server mit dem neuen Wert "Hintergrundserver" aufgefüllt.

Nur Daemon

Gibt an, dass "rep_daemon" auf dem Hintergrundserver ausgeführt wird. Wenn Sie diese Option auswählen, dann wird das Feld Repository-Server automatisch mit dem Wert Hintergrundserver aufgefüllt. Geben Sie den Wert für das Feld Servlet-Server ein. Wenn der Hintergrundserver heruntergefahren wird und der Standby-Server als neuer Hintergrundserver hochgestuft wird, dann wird das Feld Repository-Server mit dem neuen Wert "Hintergrundserver" aufgefüllt.

Servlet und Daemon

Gibt an, dass der Hintergrundserver für den Servlet-Pfad und "rep_daemon" verwendet wird. Wenn Sie diese Option auswählen, dann werden die Felder Servlet-Server und Repository-Server automatisch mit dem Wert Hintergrundserver aufgefüllt. Wenn der Hintergrundserver heruntergefahren wird und der Standby-Server als neuer Hintergrundserver hochgestuft wird, dann werden diese Felder mit dem neuen Wert "Hintergrundserver" aufgefüllt.

Servlet-Server

Gibt den Server an, auf dem das Servlet ausgeführt wird.

Repository-Server

Gibt den Server an, auf dem "rep_daemon" aktiv ist und ausgeführt wird.

Archivtyp

Die Archivierungs- und Löschungsaktion, die am Repository-Inhalt durchgeführt werden soll.

Keine

Es wird kein Archivierungs- und Löschvorgang durchgeführt.

Archivierung und Löschung

Die Verlaufsdatensätze werden in die Datei geschrieben, die im Archivfeld angegeben und von der Datenbank bereinigt wird.

Nur Löschung

Die Verlaufsdatensätze werden von der Datenbank bereinigt, jedoch werden sie nicht in die Archivdatei geschrieben.

Archivpfad

Gibt den Verzeichnispfad oder den UNC-Pfad an, zu dem Dateien im Repository während des Archivierungsprozesses verschoben werden.

UNC-Daten

Gibt die Anmeldeinformationen für den Zugriff auf den UNC-Pfad an. Klicken Sie auf UNC-Daten, um die Seite Anmeldeinformationen - Suche zu öffnen.

- Wenn Sie die Anmeldeinformationen bereits erstellt haben, um auf den angegebenen UNC-Pfad zuzugreifen, führen Sie eine Suche mithilfe der Felder durch, und wählen Sie die Anmeldeinformationen aus.
- Wenn Sie die Anmeldeinformationen erstellen möchten, klicken Sie auf "Neu erstellen". Weitere Informationen über das Erstellen von Anmeldeinformationen finden Sie unter dem Thema "[Erstellen von UNC-Daten](#)" (siehe Seite 486)".

Nicht zulässige Dateitypen

Die Dateierweiterungen, die nicht von den Anwendern in das Repository hochgeladen werden können.

Hinweis: Wenn der Wert in diesem Feld mit einem Ausrufezeichen (!) beginnt, sind diese Dateitypen im aktuellen Repository zugelassen. Beispiel: Der Wert ".jpg,.gif" in der Liste weist darauf hin, dass Dateien mit den Erweiterungen .jpg und .gif im Repository nicht zulässig sind. Der Wert "!jpg,.gif" bedeutet jedoch, dass nur Dateien mit den Erweiterungen .jpg und .gif im Repository zulässig sind.

Erstellen von UNC-Daten

Sie erstellen die UNC-Daten, um es Anwendern zu erlauben, auf freigegebene Ressourcen von den CA SDM-Servern zuzugreifen, indem der UNC-Pfad verwendet wird.

Wichtig! Die UNC-Komponente funktioniert nicht, wenn der CA SDM-Server in der Domäne ist und der freigegebene Speicherort in der WORKGROUP ist. Es funktioniert auch nicht, wenn das Administratorkennwort für den CA SDM-Server und den freigegebenen Speicherort unterschiedlich ist.

Gehen Sie wie folgt vor:

1. Klicken Sie auf die UNC-Daten auf der Seite "Allgemeine Einstellungen", oder wählen Sie auf der Registerkarte "Administration" die Optionen "Sicherheit und Rollenmanagement", "UNC-Daten" aus.

Die Seite Anmeldeinformationen - Liste wird geöffnet.

2. Klicken Sie auf "Neu erstellen".

Die Seite "Neue Anmeldeinformationen erstellen" wird geöffnet.

3. Füllen Sie die folgenden Felder nach Wunsch aus:

Symbol

Gibt die eindeutige Kennung an, um die Anmeldeinformationen während einer Suche einfacher zu identifizieren.

Anwender-ID

Gibt den Anwendernamen für den Zugriff auf den UNC-Pfad an. Der Anwender kann ein lokaler Anwender oder ein Windows-Domänenanwender sein, der Zugriff auf den Service Desk-Server hat.

Kennwort

Gibt das Kennwort für den Zugriff auf den UNC-Pfad an.

Aktiv

Gibt an, ob die UNC-Daten aktiv oder inaktiv sind. Die inaktiven Anmeldeinformationen können nicht verwendet werden.

4. Klicken Sie auf "Speichern".

Die UNC-Daten werden erstellt.

Erstellen eines Ordners

Ordner werden verwendet, um die Dokumente in Repositorys zu organisieren. Zum Beispiel können Sie den Ordner "Fehlerbilder" unter dem Repository "Bilder" erstellen. Dieser Ordner kann alle Snapshots von Fehlermeldungen enthalten, die der Anwender gefunden hat. Sie können keinen Ordner für den Repository-Typ "Service Desk-Anhänge" erstellen.

Gehen Sie wie folgt vor:

1. Wählen Sie auf der Registerkarte "Administration" die Optionen "Anhangsbibliothek", "Repositorys" aus.
Die Seite Repositorys - Liste wird geöffnet.
2. Klicken Sie mit der rechten Maustaste auf das Repository, in dem Sie den Ordner erstellen möchten, und wählen Sie "Ordner hinzufügen" aus.
Die Seite "Neuen Ordner erstellen" wird geöffnet.
3. Geben Sie den Namen des Ordners und eine Beschreibung seines Inhalts ein.
4. Wählen Sie die Registerkarte "Berechtigungen" aus, und geben Sie die entsprechenden [Zugriffsrechte](#) (siehe Seite 488) an.
5. Klicken Sie auf "Speichern".
Der Ordner wird erstellt.

Zugriffsrechte

Sie können dem Ordner im Repository folgende Zugriffsrechte hinzufügen:

Von übergeordnetem Element übernehmen

Gibt an, dass dieser Ordner die gleichen Berechtigungseinstellungen hat wie der übergeordnete Ordner. Diese Option wird nur für Unterordner angezeigt.

Steuerung nach Gruppe

Gibt den Lese- oder Schreibzugriff auf diesem Ordner für angegebene Gruppen an. Diese Option wird für alle Ordner und Unterordner angezeigt.

Allen Anwendern Schreibberechtigung erteilen

Gibt an, dass alle Anwender Schreibzugriff auf die Ordner haben.

Allen Anwendern Leseberechtigung erteilen

Gibt an, dass alle Anwender Lesezugriff auf die Ordner haben. Leseberechtigung gibt an, dass Sie den Ordner anzeigen können. Sie können ihn jedoch nicht bearbeiten, löschen oder Dateien darin speichern. Anwender mit Administratorrechten können einen Ordner bearbeiten, selbst wenn die ihnen zugeordnete Gruppe dies nicht kann. Gehört ein Anwender zu mehreren Berechtigungsgruppen mit unterschiedlichen Zugriffsebenen auf das Dokument, erhält der Anwender die höchste verfügbare Zugriffsebene (wenn zum Beispiel eine Gruppe nur Lesezugriff und die andere Schreibzugriff hat, erhält der Anwender Schreibzugriff).

Hinweis: Das Kontrollkästchen "Allen Anwendern Leseberechtigung erteilen" wird automatisch aktiviert, wenn Sie das Kontrollkästchen "Allen Anwendern Schreibberechtigung erteilen" aktivieren.

Verfügbare Gruppen

Zeigt alle Gruppen an. Sie können die Gruppen aus dieser Liste auswählen. Wählen Sie zum Beispiel eine Gruppe aus, und klicken Sie auf > für Gruppen mit Schreibberechtigung, um Lese- und Schreibzugriff für diesen Ordner für alle Anwender in dieser Gruppe bereitzustellen. Verwenden Sie Filter anzeigen, um Kriterien anzugeben und die Gruppen zu filtern.

Ankündigungen

Sie können CA SDM verwenden, um Anwendern Ankündigungen mitzuteilen. Mit Ankündigungen können die Anzahl der eingehenden Anrufe reduziert werden. Außerdem bietet diese Funktion eine gesteigerte Produktivität durch die proaktive Lösung von Tickets und die Übermittlung wichtiger Informationen an alle betroffenen Anwender. Anwender können einen Bildlauf durch mehrere gespeicherte Ankündigungen durchführen.

Hinweis: Ankündigungen gelten für alle Service Desk-Modelle.

Sie können neue Ankündigungen hinzufügen und bestehende aktualisieren. Ankündigungen sind Teil der Bezugsdatenfunktion von CA SDM. So können Sie durch Verwendung des Zugriffstyps steuern, welche Kontakte Ankündigungen erstellen können.

Eine Ankündigung kann eine oder auch beide der folgenden Angaben enthalten:

Standort

Gibt eine physische Lokation an (z. B. eine Stadt, ein Gebäude oder eine Etage).

Organisation

Gibt eine Organisations-ID an. Wenn Organisation für eine Ankündigung festgelegt wird, können nur Personen jener Organisation die Ankündigung anzeigen.

Wenn Lokation oder Organisation für eine Ankündigung festgelegt wird, bekommen sie nur Kontakte an jener Lokation oder Organisation. Kontakte können jedoch weiterhin Ankündigungen sehen, die nicht durch die Lokation oder die Organisation eingeschränkt sind. Wenn beispielsweise keine Festlegung getroffen wurde, können Kontakte an jeder Lokation und in jeder Organisation eine Ankündigung sehen.

Hinweis: Sie können Ankündigungen mit der administrativen Funktion der Web-Schnittstelle angeben. Weitere Informationen zur Definition von Ankündigungen finden Sie in der *Online-Hilfe*.

Weitere Informationen:

[Sichtbarkeit interner Ankündigungen](#) (siehe Seite 489)

[Angaben der Ankündigungsdringlichkeit](#) (siehe Seite 490)

Sichtbarkeit interner Ankündigungen

Mit dem Kontrollkästchens "Intern" auf der Seite "Neue Ankündigung erstellen" können Sie steuern, ob eine Ankündigung für interne Benutzern sichtbar ist. Die Einstellung "Interne Protokolle anzeigen" des Zugriffstyps des angemeldeten Benutzers steuert, ob ein Benutzer als intern markierte Elemente anzeigen kann.

Angeben der Ankündigungsdringlichkeit

Sie können die Dringlichkeit eines Ankündigungsdatensatzes angeben.

So geben Sie die Ankündigungsdringlichkeit an:

1. Erstellen Sie eine Ankündigung, oder navigieren Sie zur Seite "Ankündigung - Detail", um eine vorhandene Ankündigung zu bearbeiten.
2. Wählen Sie in der Dropdown-Liste "Ankündigungstyp" eine der folgenden Optionen aus:

Routine

Anzeige in schwarzem Text

Beratung

Anzeige in orangefarbenem Text

Notfall

Wird in rotem Text angezeigt.

Klicken Sie auf "Speichern".

Der Ankündigungsdatensatz ist auf der Seite "Ankündigungslisten" farblich gekennzeichnet.

Einrichten von gespeicherten Abfragen

CA SDM unterstützt die Verwendung von gespeicherten Abfragen zur Erzeugung von zweierlei Daten:

- Scoreboard-Abfragen ermöglichen Ihnen, das Web-Schnittstellen-Scoreboard durch Hinzufügen von Zählerfeldern für relevante Elemente anzupassen.
- KPI-Abfragen ermöglichen Ihnen, Verlaufsinformationen für einen angegebenen Zeitraum anhand des Wertes eines Zählers abzurufen und in webbasierten Berichten zu verwenden.

Gespeicherte Abfragen gelten für alle Service Desk-Modelle. Gespeicherte Abfragen dienen nicht der Absicht, Benutzer auf eine neue Seite zu bringen.

Administratoren definieren die gespeicherten Abfragen, die für Benutzer verfügbar sind. Sie können die gespeicherten Abfragen verwenden, die mit CA SDM installiert wurden, oder Ihre eigenen definieren. Sie können gespeicherte Abfragen definieren, indem Sie die administrative Funktion der Web-Schnittstelle verwenden.

Betrachten Sie die folgenden Informationen zu gespeicherten Abfragedefinitionen:

- Eine gültige gespeicherte Abfrageklausel ist in eine entsprechende SELECT-Anweisung integriert und wird an die zugrunde liegende DBMS-Engine zur Verarbeitung übergeben. Zur Erstellung von SELECT-Anweisungen siehe die Objektdefinitionsdateien in den folgenden Verzeichnissen:
 - Windows: `installation-directory\bopcfg:majic`
 - UNIX: `$NX_ROOT/bopcfg/majic`
- Gespeicherte Abfragen verwenden die Objekt- und Attributanweisungen zur Erstellung einer SQL WHERE-Klausel anstelle der Feldnamen auf Datenbankebene.
- CA SDM unterstützt keine kartesischen Produktverknüpfungen für gespeicherte Abfragen. Um sicherzustellen, dass Ihre gespeicherte Abfrage kartesische Produktverknüpfungen erzeugt, geben Sie den entsprechenden Befehl für Ihr System ein:
 - Windows: `bop_cmd -f installation-directory\bopcfg\interp\bop_diag.frg "check_queries()"`
 - UNIX: `bop_cmd -f $NX_ROOT/bopcfg/interp/bop_diag.frg "check_queries()"`Um kartesische Produktverknüpfungen zu vermeiden, müssen Sie alle als Ergebnis gekennzeichneten Abfragen aktualisieren.
- Die als URL gespeicherte Abfrage ist eine Option, die beim Erstellen von gespeicherten Abfragen angeboten wird. Die als URL gespeicherte Abfrage führt eine Abfrage aus und gibt numerische Ergebnisse zurück, die nur in Verbindung mit Knowledge Management eingesetzt werden können.

Hinweis: Weitere Informationen zur Syntax von Objektdefinitionen finden Sie im *Technischen Referenzhandbuch*. Weitere Informationen zum Definieren gespeicherter Abfragen finden Sie in der *Online-Hilfe*.

Sequenznummern

Wenn ein Ticket geöffnet wird, wird ihm automatisch die nächste verfügbare Sequenznummer zugewiesen. Wenn zum Beispiel der letzte geöffnete Request 5 lautet, wird der nächste Request die Nummer 6 zugewiesen.

Wichtig! Nachdem Sie eine neue Version von CA SDM installiert haben, wird die interne Datensatz-ID für alle Tickets auf 1 zurückgesetzt. Um sicherzustellen, dass keine doppelten Datensatz-IDs erstellt werden, legen Sie erst dann neue Tickets an, wenn Sie die gesicherten Daten wiederhergestellt haben.

Sie können festlegen, wie Requests, Changes und Issues nummeriert werden, indem Sie ein eindeutiges Präfix oder Suffix in das Nummerierungsschema für diese Elemente einschließen. Wenn Sie zum Beispiel Requests nach Monat verfolgen möchten, können Sie ein Monatskennzeichen als Präfix oder Suffix zum Nummerierungsschema für Requests hinzufügen.

Hinweis: Informationen zum Anpassen der Tickets zugewiesenen Nummern mit Hilfe der administrativen Funktion der Web-Schnittstelle finden Sie in der *Online-Hilfe*.

Da Sie für jeden Tickettyp ein getrenntes Nummerierungsschema definieren, müssen Sie Nummerierungsschemas für alle Service Desk-Modelle einrichten. Sie können das Format der Nummerierung für Requests, Changes und Issues steuern, indem Sie die Einstellungen für Sequenznummern ändern. Standardmäßig werden neue Tickets unter Verwendung fortlaufender Ganzzahlen nummeriert. Da das Nummernfeld eines Tickets keine Zahlen sondern Zeichenfolgen enthält, können Sie zusätzliche Zeichenfolgenwerte zuweisen, die bei der Generierung einer Ticketnummer für ein neues Ticket als Präfix oder Suffix verwendet werden. Zum Beispiel können Sie r:, c: und i: als Präfixe für Requests, Changes und Incidents angeben. Bei diesem Setup können Anwender problemlos zwischen den verschiedenen Tickettypen unterscheiden, so dass keine Verwirrung entsteht.

Incidents und Probleme haben teilen Nummerierungsschemas mit Requests, da es sich bei Incidents und Problemen intern um verschiedene Arten von Requests handelt.

Verwenden des Audit-Protokolls

CA SDM erstellt ein Audit-Protokoll, das die folgenden Informationen aufzeichnet:

- alle Changes an einem Issue
- alle Changes an einem Request (Call_Req)
- alle Changes an einem Change (Change_Request)
- alle Changes an einer Datenpartition (Domäne) Tabellen
- Die Anmelde-ID der mit dem Change verknüpften Person und ein verknüpfter Tag-/Datums-/Zeitstempel
- Die Werte vor und nach dem Aktualisieren, Einfügen oder Löschen
- Die Erstellung von Kontakten
- Die Erstellungs- und Aktualisierungsaktivitäten des "nr"-Objekts

Hinweis: Das Audit-Protokoll hält nur Änderungen am Feld mit den Datenpartitionen für die Kontakte fest, nicht jedoch andere Aktualisierungen an den Kontaktdatensätzen.

Die Audit-Protokollfunktion wird automatisch installiert, muss jedoch durch Installieren von zwei Audit-Protokolloptionen mit dem Optionsmanager aktiviert werden: "audit_ins" und "audit_upd". Nachdem Sie diese Optionen installiert haben, können Sie auf der Registerkarte "Administration" durch Auswählen von "Service Desk" > "Audit-Protokoll – Liste" auf das Audit-Protokoll zugreifen. Sie können die Audit-Protokollliste mit einem integrierten Suchtool durchsuchen und mit dieser Liste die Erzeugung von Berichten erleichtern.

Hinweis: Informationen zur Installation und Festlegung von Werten für Optionen finden Sie in der *Online-Hilfe*.

Integration in das CA-Netzwerk und Systemverwaltung

Sie können Ereignisverwaltungs-Meldungsdatensätze und zugehörige Meldungsdatensatz-Aktionen in CA NSM definieren, um automatisch Anforderungen zu erstellen, Kommentare zu vorhandenen Anforderungen zuzuordnen oder Ankündigungen in CA SDM bereitzustellen.

Hinweis: Weitere Informationen zur CA NSM-Integration finden Sie im *Implementierungshandbuch*.

Drucken von CA SDM-Webseiten

Zum Formatieren von Schaltflächen und Notizbuchregisterkarten verwendet CA SDM Hintergrundgrafiken. Die Standardeinstellung für die meisten Browser ist, diese Hintergrundbilder *nicht* zu drucken. Wenn Sie somit "Datei" > "Drucken" im Menü des Browsers oder im CA SDM-Menü auswählen, zeigt die gedruckte Seite nur die Ecken der Schaltflächen oder Registerkarten.

So drucken Sie CA SDM-Webseiten mit Internet Explorer:

1. Wählen Sie "Extras" und dann "Internetoptionen" aus.
Das Dialogfeld "Internetoptionen" wird angezeigt.
2. Wählen Sie die Registerkarte "Erweitert" aus.
3. Blättern Sie nach unten bis zum Eintrag "Drucken". Aktivieren Sie die Option "Druckhintergrundfarben und -bilder drucken".

Die gedruckten CA SDM-Webseiten enthalten Hintergrundgrafiken.

So drucken Sie CA SDM-Webseiten mit Firefox:

1. Wählen Sie "Datei" und dann "Seite einrichten".
2. Wählen Sie die Registerkarte "Format & Optionen".
3. Aktivieren Sie das Kontrollkästchen "Hintergrund drucken (Farben & Bilder)".

Die gedruckten CA SDM-Webseiten enthalten Hintergrundgrafiken.

Verhalten für die Anzeige von Datensätzen in der Web-Schnittstelle

Wenn ein Benutzer einen Datenbank-Datensatz über die Web-Schnittstelle bearbeitet, wird dem Benutzer der Datensatz zwei Minuten lang exklusiv angezeigt. Dies ist die Standardzeit. Sie können die Standardzeit durch die Benutzung der Eigenschaft "ExclLockSeconds" in der Datei "web.cfg" ändern.

Die folgenden Bedingungen wirken sich darauf aus, ob ein Datenbankdatensatz von den Änderungen eines Benutzers aktualisiert wird:

- Wenn ein Benutzer Änderungen innerhalb einer zugewiesenen Zeit bearbeiten und übermitteln *kann*, werden die Changes in die Datenbank aufgenommen.

Während der Zeit, für die der Datenbank-Datensatz gesperrt ist, können andere Benutzer (sowohl Web- als auch Nicht-Web-Benutzer) ihn anzeigen, aber nicht bearbeiten. Wenn ein anderer Benutzer versucht, den Datensatz zu bearbeiten, während dieser gesperrt ist, wird eine Fehlermeldung ausgegeben.

- Wenn ein Benutzer Changes innerhalb einer zugewiesenen Zeit *nicht* bearbeiten und übermitteln kann, wird die Datensatzsperre automatisch entfernt, und andere Benutzer können den Datensatz bearbeiten.

Wenn der Benutzer die Aktualisierungen schließlich absendet, werden die Zeitstempel geprüft, um sicherzustellen, dass der Datensatz nicht von einem anderen Benutzer geändert wurde. Dann geschieht Folgendes:

- Wenn der Datensatz nach Aufheben der exklusiven Sperre nicht geändert wurde, werden die Aktualisierungen des Benutzers in der Datenbank gespeichert.
- Falls ein anderer Benutzer den Datensatz nach Ablauf der Sperre bearbeitet hat, erhält der Benutzer eine Fehlermeldung, wenn er den Datensatz speichern möchte, und die Änderungen werden nicht gespeichert. Der Benutzer muss den Bearbeitungsprozess neu starten und die Änderungen neu eingeben.

Weitere Informationen:

[Änderung der Konfigurationsdatei](#) (siehe Seite 563)

Support-Struktur

Die *Support-Struktur* Ihres Service Desk besteht aus den Komponenten, die der Anwender zur Problemlösung benötigt. Sie können die CA SDM-Support-Struktur im Einklang mit dem Supportmodell (intern, extern oder beide) einrichten.

Hinweis: Sie können Issues, Anfragen und Changes anpassen, damit Sie den Bedürfnissen Ihres Standorts optimal entsprechen. Weitere Informationen finden Sie im *Implementierungshandbuch* und in der *Online-Hilfe*.

Aktivieren der CAPA-Hilfe

CA Productivity Accelerator (CAPA) stellt kontextabhängigen, integralen Performance-Support für die CA SDM-Analyst-Webformulare bereit. Das Paket des CAPA-Players wird direkt in die Kontext-Hilfemenüs der CA SDM-Analyst-Webseiten integriert. Die Integration des CAPA-Hilfe-Inhalts mit CA SDM wird durch die Hilfemenü-Skripte erreicht. Diese Skripte starten den aufgezeichneten CAPA-Hilfe-Inhalt über die CA SDM-Hilfemenü-Drow-down-Felder sowie die Kontexthilfe.

Hinweis: Dieses Thema schließt keine Informationen zum CAPA-Aufzeichnungs-Tool, zum Erhalten und Konfigurieren des CAPA-Hilfe-Inhalts und zum Installieren von Smart Help ein.

CA SDM stellt eine eindeutige Kennung bereit, mit der jedes Webformular eindeutig identifiziert wird. Wenn ein Identifizierungselement im oberen Frame von CA SDM vorhanden ist, kann das CAPA-Aufzeichnungs-Tool ein Webanwendungsformular erkennen. Sobald der obere Frame erkannt wurde, werden alle untergeordneten Frames als Teil dieser Anwendung betrachtet. Die untergeordneten Frames, die aus verschiedenen Domänen geladen werden, müssen auch identifiziert werden. Sie werden sonst nicht als Teil von CA SDM betrachtet. Um die CAPA-Hilfe zu aktivieren, müssen Sie den Hilfe-Inhalt erstellen und dann die Optionen zum Starten der CAPA-Hilfe konfigurieren.

Hinweis: Um die HTML-Dateien anzupassen, verwenden Sie die Aufrufmethoden der `ias_helper.js`-Dateien für den CAPA-Rekorder, damit die HTML-Formulare erkannt werden.

CAPA-Hilfe wird nicht für die Schnittstellen CA SDM Mitarbeiter, Kunde oder PDA nicht unterstützt. Weitere Informationen zu den Browsern, die CAPA unterstützen, finden Sie in der CAPA-Dokumentation.

Gehen Sie wie folgt vor:

1. Öffnen Sie die `capa.properties`-Datei aus dem folgenden CA SDM-Verzeichnis:

```
%NX_ROOT/bopcfg/www/wwwroot
```

2. Ändern Sie die folgenden Werte in der Datei:
 - Enable_Alerts = 0. Mit dieser Option werden die JavaScript-Warnmeldungen in einer Browserkonsole überprüft und angezeigt, wenn die CA SDM-Webseite geladen wird.
 3. Speichern Sie die Datei.
 4. Gehen Sie zur Datei "web.cfg" im CA SDM-Verzeichnis, fügen Sie "DebugScript=1" hinzu, und starten Sie die Web-Engine neu.

Der aufgezeichnete Inhalt wird vorbereitet, veröffentlicht und auf dem CAPA-Server bereitgestellt.
 5. Öffnen Sie die capa.properties-Datei, und ändern Sie die folgenden Werte:
 - Enable_For_Recording = 0
 - Show_Learn_Links = 1. Dieser Wert zeigt die CAPA-Hilfe-Option im CA SDM-Hilfemenü und im Kontextmenü an.
 - Server_Name = Name des Servers, auf dem der für CAPA veröffentlichte Inhalt bereitgestellt wird.
 - Server_Port = CAPA-Serverport, auf dem CAPA-veröffentlichte Inhalte bereitgestellt werden. Beispiel: TOMCAT-Port.
 - Virtual_Dir = virtuelles Verzeichnis, in dem der für CAPA veröffentlichte Inhalt auf dem CAPA-Server bereitgestellt wird.
 - Namespace = Anwendungskontext-Namespace. Beispiel: app.SDM.Project123;en.
 - Enable_Alerts = 0
 6. Speichern Sie die Datei.
- Sie können nun die CAPA-Hilfe über die CA SDM-Analyst-Webformularen starten.

Kapitel 11: Steuerung des Systemverhaltens

Dieses Kapitel enthält folgende Themen:

[Verwendung des Optionsmanagers](#) (siehe Seite 497)

Verwendung des Optionsmanagers

Mit dem CA SDM-Webclient können Sie den Optionsmanager von der Registerkarte "Administration" aus verwenden, um folgende Aktionen durchzuführen:

- Abrufen einer Liste aller verfügbaren Optionen
- Anzeigen einer Zusammenfassung jeder Option wie z. B. der Anwendung, mit der sie verknüpft ist, einer Kurzbeschreibung und ihren Status.
- Die Details einer bestimmten Option anzeigen.

Bei der Anzeige von Detailinformationen zu einer Option können Sie eine ausführliche Beschreibung ihrer Funktionalität von der *Online-Hilfe* abrufen. Die Beschreibung in der *Online-Hilfe* enthält alle speziellen Aktionen, die Sie beim Ändern der Option durchführen müssen. Zum Beispiel müssen Sie nach dem Installieren oder Deinstallieren einiger Optionen sicherstellen, dass Sie den CA SDM-Server neu starten, damit die Option wirksam wird. Die Beschreibung in der *Online-Hilfe* weist ebenfalls darauf hin.

- Den Status aller Optionen auf Zusammenfassungsebene prüfen.
- Deinstallieren Sie eine der verfügbaren Optionen (nur auf dem Hintergrundserver anwendbar)

Viele der Optionen sind vorkonfiguriert und werden bei der Installation von CA SDM installiert. Bei Verwendung des Optionsmanagers zur Installation oder Deinstallation von Optionen können einige oder alle Standardeinstellungen verändert werden.

- Installieren Sie eine definierte Option (nur auf dem Hintergrundserver anwendbar)

Hinweis: Während eines Release-Zyklus werden Optionen gelegentlich auf Anwenderanfrage vom CA SDM-Support zur Verfügung gestellt. Um weitere Informationen zu diesen Optionen zu erhalten, wenden Sie sich an den CA SDM-Support. Hinweis: Weitere Informationen zur Verwendung des Optionsmanagers finden Sie in der *Online-Hilfe*.

Ändern der System-Umgebung

CA SDM verwendet Umgebungsvariablen, die in der Umgebungsdateivorlage (NX.env.tpl) angegeben sind, um gewisse Verhalten zu definieren. Sie können Umgebungsvariablen verwenden, um einige Systemverhalten zu ändern. Normalerweise verwenden Sie den Optionsmanager zur Steuerung des Systemverhaltens. Der Technische Support von CA weist Sie jedoch ggf. an, eine bestimmte Umgebungsvariable direkt zu ändern.

Beachten Sie folgendes beim Bearbeiten der Umgebungsdateivorlage:

- In dieser Datei eingestellte Umgebungsvariablen können überschrieben werden, indem die Umgebungsvariable im Prozessraum eingestellt wird, in dem ein Prozess läuft. Obwohl dies in einigen Fällen praktisch sein kann, ist diese Konfiguration gewöhnlich nicht wünschenswert. Wenn Sie einer Variablen das Symbol (@) voranstellen, wird verhindert, dass Variablen im Prozessbereich diese Variable überschreiben. Sofern kein spezieller Grund für das Zulassen des Überschreibens vorliegt, sollte dem Variablennamen in der Vorlagendatei stets ein @-Zeichen vorangestellt werden.
- Die Kommentarzeichen für diese Datei sind Raute (#) und Ausrufezeichen (!). Das Ausrufezeichen wird auch zur Deaktivierung einer Option verwendet.

Wichtig! Ändern Sie die Vorlagendatei (NX.env.tpl) und ermöglichen Sie dem Konfigurationsvorgang, die Änderungen auf die Umgebungsdatei anzuwenden. Ändern Sie niemals die Umgebungsdatei (NX.env) direkt.

Gehen Sie wie folgt vor:

1. sichern Sie die Umgebungsdateivorlage (.tpl), die Ihrer Systemumgebung entspricht:
 - UNIX: \$NX_ROOT/pdmconf/NX.env.tpl.
 - Windows: installation-directory\pdmconf\NX.env_nt.tpl.
2. Bearbeiten Sie abhängig von Ihrer CA SDM-Konfiguration die Umgebungsdateivorlage auf dem folgenden Server:
 - Konventionell: Primärserver
 - Erweiterte Verfügbarkeit: Einer der Standby-Server

Hinweis: Sie können die Datei mit einem beliebigen Texteditor anzeigen und bearbeiten (Windows-Anwender sollten WordPad verwenden).

3. Nehmen Sie die Änderungen wie von Ihrem Supporttechniker angewiesen vor, und speichern Sie die Änderungen.
4. Führen Sie das Konfigurationshilfsprogramm auf der Primärserver- oder Standby-Server-Installation aus, um die Änderungen, die Sie an der Vorlagendatei für Umgebungsvariablen vorgenommen haben, auf die eigentliche Umgebungsdatei anzuwenden.

Hinweis: Weitere Informationen zum Ausführen des Konfigurationsprogramms finden Sie im *Implementierungshandbuch*.

5. Führen Sie abhängig von Ihrer CA SDM-Konfiguration eine der folgenden Aktionen aus:
 - Konventionell: Starten Sie den Primärserver neu, damit die an der Umgebungsdatei vorgenommenen Änderungen wirksam werden.
 - Erweiterte Verfügbarkeit: [Starten Sie alle CA SDM-Server neu](#) (siehe Seite 52).

Hinweis: Um das komplette Herunterfahren Ihres Systems zu vermeiden, kann der Supporttechniker Sie anweisen, nur bestimmte Prozesse neu zu starten, anstatt den gesamten CA SDM-Server zu aktualisieren.

Events

Sie können Ereignisse konfigurieren, die an Objekte angehängt sind, um konfigurierte Aktionen auszuführen. Ereignisse sind Prozeduren, die nach Ablauf einer bestimmten Zeitspanne abgearbeitet werden. Zum Beispiel kann ein Ereignis einem Service Desk-Analysten eine Meldung schicken, wenn ein Issue mit der "Priorität 1" nicht innerhalb einer Stunde erhalten wurde. Andere Teile des Systems verwenden Ereignisse, zum Beispiel, Servicetypen.

Sie können Ereignisse für Anfragen, Incidents, Probleme, Changes, Issues, Kontakte, Configuration Items und globale und spezifische Mandanten definieren. CA SDM plant die Ereignissablaufzeit basierend auf der Zeitverzögerung und der Schicht.

Hinweis: Weitere Informationen zu Ereignissen finden Sie in der *Online-Hilfe*.

Makros

Makros sind kleine Skripts, die Bedingungen oder Aktionen definieren. Wenn Ereignisse oder Verhalten ausgelöst werden, können sie ein oder mehrere Aktionsmakros ausführen. Vor der Ausführung von Makros kann ein Bedingungs makro verwendet werden, um zu bestimmen, welche Gruppe von Aktionsmakros ausgelöst wird.

Makros können in folgenden Bereichen verwendet werden:

- Events
- Verhaltensvorlagen für Issues oder Changes
- Aktivitätsbenachrichtigungen

Das Produkt enthält mehrere Makros. Anwender können zusätzliche Typen erstellen.

Hinweis: Kunden können keine Makros vom Typ "Aktion" oder "Bedingung" hinzufügen; sie können aber einfache Bedingungs makros mit standortdefinierten Bedingungen erstellen. Standortdefinierte Bedingungen sind nicht-komplexe Makros, die in Dialogen der grafischen Oberfläche erstellt werden können; sie sind kein Ersatz für Makros vom Typ "Bedingung".

Für jedes Makro müssen Sie den Objekttyp angeben, den das Makro verwenden soll. Wenn Sie eine standortdefinierte Bedingung erstellen möchten, um die Werte einer Anfrage zu prüfen, müssen Sie als Typ "Anfrage" festlegen. Bei der Auswahl von Makros für Ereignisse und Verhalten zeigt CA SDM nur Makros an, deren Typ dem Typ für das Ereignis oder Verhalten entspricht.

Makrotypen

Jedes der folgenden Makros hat einen bestimmten Typ, der seine Verwendung beschreibt:

Aktion

Dieser Typ führt eine Aktion aus, wie zum Beispiel die Erhöhung der Priorität eines Issues.

Event anhängen

Hängt ein Ereignisobjekt an einen Change, Issue, Anfrage, Kontakt oder Configuration Item an.

Bedingung

Dieser Typ bewertet Bedingungen als wahr (True) oder falsch (False).

CA IT-PAM Aktion ausführen

Führt eine CA IT-PAM-Aktion aus. CA IT-PAM ist eine Workflow-Engine, mit der die Verwaltung und Berichterstellung über solche Aufgabengruppen ermöglicht wird, die eine elektronische Genehmigung benötigen können.

Ausführen einer CA Workflow-Aktion

Führt eine CA Workflow-Aktion aus. Mit CA Workflow können Sie Workflow-Prozesse in Ihrer Umgebung verwalten, wie z. B. Nachverfolgungsaktivitäten für die Tickets, die mit einer spezifischen Kategorie oder einem spezifischen Bereich verbunden sind.

Remotebezug

Startet ein externes Programm auf dem Server.

Mehrere Benachrichtigungen

Schickt eine Benachrichtigung an einen oder mehrere Kontakte. Dieser Makrotyp ist besonders nützlich, da Sie die Meldung, die Empfänger und die Dringlichkeitsstufe angeben können.

Standortdefinierte Bedingung

Erstellt Ereignisse aufgrund von wahren oder falschen Bedingungstypen sowie basierend auf Attributen des Tickets, um Service-Ebenen durchzusetzen. Zum Beispiel können Sie ein Bedingungs makro erstellen, das abfragt, ob es Anfragen mit der Priorität 1 gibt, die noch nicht zugewiesen sind. Sie können die Bedingung einem Ereignis anhängen, das kurze Zeit nach der Erstellung einer Anfrage ausgeführt wird.

Verwenden von Makros in Verbindung mit Ereignissen

In den Ereignisdetails können Sie im Feld "Ereignisbedingung" optional ein Bedingungs makro angeben. In den Spalten "Ausführen bei 'True'" und "Ausführen bei 'False'" können Sie ebenfalls eine beliebige Zahl von Makros (außer Bedingungs makros) angeben. Wenn das Ereignis ausgelöst wird, wird zunächst das Bedingungs makro bewertet. Wenn es wahr (True) ist, werden alle Makros in der Spalte 'True' ausgelöst. Wenn es falsch (False) ist, werden alle Makros in der Spalte 'False' ausgelöst. Das Bedingungs makro kann auch prüfen, ob der Zuständige oder die Prioritätsebene festgelegt ist, ob eine Verletzung des Servicetyps vorliegt usw. Wenn kein Ereignisbedingungs makro angegeben ist, führt das Ereignis automatisch die Makros für 'True' aus.

In den Ereignisdetails können Sie eine Auswahl aus fast allen Makrotypen treffen, um Kontakte zu benachrichtigen, Werte für das Kontextobjekt festzulegen, einen Remotebezug durchzuführen oder ein anderes Ereignis anzuhängen.

Verwenden von Makros in Verbindung mit dem Verhalten für Issues- und Change-Kategorien

Sie können Makros auch in Verbindung mit dem Verhalten für Issues- und Change-Kategorien verwenden. In den Kategoriedetails können Sie auf der Registerkarte „Workflow“ einen Workflow-Status auswählen. In den Workflow-Details klicken Sie auf die Schaltfläche „Verhalten“. Ähnlich wie bei einem Ereignis können Sie eine Bedingung und resultierende Aktionen festlegen.

Auf der Registerkarte „Übergang“ in den Verhaltensdetails können Sie ein Bedingungs makro angeben, um zu bestimmen, ob die Aufgabe aus diesem Status in einen anderen Status übergehen kann. Dieses Makro wird ausgelöst, wenn ein Benutzer versucht, den Aufgabenstatus von diesem Wert in einen anderen Wert zu ändern. Wenn die Bedingung als falsch bewertet wird, ist die Statusaktualisierung nicht zulässig.

Die tatsächlichen Workflow-Aufgaben werden von den Vorlagen in der Kategorievorlage erstellt. Wenn der Statuswert einer Aufgabe geändert und gespeichert wird, wird das in der Kategorievorlage angegebene Verhalten ausgelöst, d. h. die Bedingung und die resultierenden Aktionen werden ausgeführt.

Hinweis: Verwenden Sie ein Makro vom Typ "Ereignis anhängen", um einer Workflow-Aufgabe ein Ereignis anzuhängen.

Verwenden von Makros mit mehreren Benachrichtigungen

Mehrere Benachrichtigungen

Der Meldungstext der mehrfachen Benachrichtigung verweist direkt auf die Tabelle des ausgewählten Objekts. Beim Verweisen auf Felder in der Objekttabelle (z. B. CR (Call_Req)) können Sie somit auf den Attributnamen des Feldes verweisen. Wenn Sie die Beschreibungsinformationen des Tickets "Aufrufanfrage" angeben möchten, können Sie als Meldungstext Folgendes eintragen:

Beschreibung: @{description}

QREL (Abfrage-Beziehung) ist eine Beziehung, die eine Liste mit Objekten enthält, welche durch eine Where-Klausel des Typs SQL definiert wird. Sie können QREL der Beschreibung eines Makros mit mehreren Benachrichtigungen hinzufügen. Wenn Sie QREL in die Beschreibung für "act_log-QREL-<--alg" setzen möchten, können Sie in einem Benachrichtigungsmakro Folgendes benutzen:

@{act_log.0.description}

Sie können Ersatzvariablen benutzen, um Benachrichtigungsmeldungen relevanter und dynamischer zu gestalten. Diese Ersetzungsvariablen haben die Form @{attribute_path_here}, wobei attribute_path_here ein Attribut eines CA SDM-Objekts ist. Wenn die Benachrichtigung gesendet wird, wird die Variable durch den angegebenen Attributwert ersetzt.

Eine Benachrichtigung (aus einem Aktivitätsprotokoll oder eine mehrfachen Benachrichtigung) hat immer einen Grundkontext (einen Bezugspunkt), der gewöhnlich ein Ticket oder eine Workflow-Aufgabe ist. Bei mehreren Benachrichtigungen gibt das Feld des Benachrichtigungs-Makrotypen das Basisobjekt an. Mit der Syntax @{} können Sie auf ein beliebiges Attribut in diesem Objekt verweisen.

Beispiel: Eine mehrfache Benachrichtigung vom Typ "Anfrage" verweist auf ein Attribut im Objekt "cr" (Call_Req). Um die Anfragebeschreibung einzuschließen, geben Sie @{description} an (mit der Punktnotation können Sie weitere Verweise auf andere Objekte angeben). Zum Beispiel, um den Nachnamen des Zuständigen der Anfrage einzuschließen: @{assignee.last_name}.

Verwenden von Makros mit einer standortdefinierten Bedingung

Standortdefinierte Bedingung

Das standortdefinierte Bedingungs makro besteht aus einer oder mehreren *atomaren* Bedingungen. Jedes Atom prüft den Wert eines einzelnen Attributs. Wenn Sie die Bedingung auf der Basis von Werten für "Zuständiger" und "Kategorie" definieren möchten, verwendet das konditionelle Makro daher wahrscheinlich zwei Atome, eines für "Zuständiger" und eines für "Kategorie". Wenn Sie ein konditionelles Makro in einem Ereignis verwenden, werden die einzelnen Atome durch einen booleschen Operator, meistens AND oder OR, verknüpft.

Die Details eines standortdefinierten Bedingungs makros zeigen eine Liste der Atome, die von links nach rechts folgendermaßen lauten:

Attribut	Operator	Wert	Logischer Operator	Übersetzung
Verantwortlicher	ist gleich	Jones	AND	Der Zuständige ist Jones und...
Kosten	kleiner als	600	ODER	Die Kosten sind eine Ganzzahl kleiner als 600 oder...
Gruppe	Empty/NULL		AND	Das Feld „Gruppe“ enthält keinen Wert.

Hinweis: Logische Verknüpfungen (AND, OR) verbinden zwei Atome miteinander. Angenommen, Sie haben zwei Atome, zum Beispiel eins und zwei, dann werden diese durch den Operator von Atom eins verknüpft. Der Operator von Atom zwei wird nicht verwendet. Des Weiteren ist die Auswahl mancher Operatoren nicht sinnvoll. Zum Beispiel ergibt der Operator *kleiner als* in Verbindung mit dem Attribut *Zuständiger* keinen Sinn. Weitere Informationen zum Erstellen von konditionellen Makros finden Sie in der *Online-Hilfe*.

Kapitel 12: Konfiguration der Option "Automatische Zuweisung"

Dieses Kapitel enthält folgende Themen:

[Automatische Zuweisung](#) (siehe Seite 505)
[Beziehungen bei der automatischen Zuweisung](#) (siehe Seite 506)
[Methoden der automatischen Zuweisung](#) (siehe Seite 506)
[Implementieren von automatischen Zuweisungen](#) (siehe Seite 507)
[Standardgruppe und -zuständiger](#) (siehe Seite 513)
[Aktivieren der automatischen Zuweisung](#) (siehe Seite 514)
[Überschreiben der automatischen Zuweisung](#) (siehe Seite 515)
[Zuweisungssteuerungen](#) (siehe Seite 516)
[Aktivitätsprotokoll](#) (siehe Seite 519)
[Aktivieren der Aktivitätsprotokollierung für zusätzliche Attribute](#) (siehe Seite 520)
[Ablaufverfolgung der automatischen Zuweisung](#) (siehe Seite 520)
[Gespeicherte Abfragen](#) (siehe Seite 521)
[Automatisches Zuweisen von Tickets](#) (siehe Seite 521)
[Automatisches Zuweisen von Workflow-Aufgaben](#) (siehe Seite 529)
[Configuration Item-basierte automatische Zuweisungen](#) (siehe Seite 533)

Automatische Zuweisung

Die *automatische Zuweisung* in CA SDM kann den Zeitaufwand bei der Verarbeitung von Tickets drastisch reduzieren, indem der Prozess der Zuordnung zu Analysten automatisiert wird. Mit dieser Automatisierung können die Aufgaben in Zusammenhang mit der Verteilung von Arbeiten und die Koordination von Arbeitsplänen sehr effizient durchgeführt werden.

Sie können die automatische Zuweisung so konfigurieren, dass Tickets auf der Basis der folgenden Faktoren zugewiesen werden:

- Welche Analystengruppe bearbeitet welche Tickets bzw. Aufgaben
- Wann die Arbeit durchgeführt werden muss
- Welche Lokationen die betroffenen Kunden betreuen
- Die Auslastung und Verfügbarkeit der einzelnen Analysten
- Der Wert eines Attributs für Configuration Items des Tickets

Hinweis: [Automatische Zuweisung auf der Basis von Configuration Items](#) (siehe Seite 533) ermöglicht die Festlegung von gruppenspezifischen Zuweisungen für Anfrage-/Incident-/Problem-Tickets.

Sie müssen die automatische Zuweisung nicht vollständig in einem Schritt implementieren. Sie können eine Strategie entwickeln, mit der die automatische Zuweisung schrittweise eingeführt wird. Sie können beispielsweise die automatische Zuweisung zunächst für einige ausgewählte Ticket-Typen, Analystengruppen bzw. Lokationen aktivieren.

Beziehungen bei der automatischen Zuweisung

Die automatische Zuweisung kann viele CA SDM-Elemente umfassen. Es stehen folgende Elementbeziehungen zur Verfügung:

- Bereiche und Kategorien, die sich auf Gruppen, Lokationen und Schichten beziehen
- Gruppen, die sich auf Lokationen und Schichten beziehen
- Workflow-Vorlagen, die sich auf Kontakte beziehen

Um die Verwaltung der automatischen Zuweisung zu vereinfachen, können alle Beziehungen von beiden Elementen verwaltet werden. Wenn Sie beispielsweise eine Analystengruppe mit einer Change-Kategorie verbinden, können Sie die Zuweisung wahlweise auf der Seite "Change-Kategorie – Detail" oder auf der Seite "Gruppe – Detail" verwalten.

Methoden der automatischen Zuweisung

Mit den folgenden einfachen Methoden können Sie Tickets automatisch zuweisen:

Auf einer Lokation basierende automatische Zuweisung

Erstellt Zuweisungen für alle Ticket-Typen basierend auf den folgenden Elementen:

- Bereiche und Kategorien, die mit Gruppen, Lokationen und Schichten verbunden sind.
- Gruppen, die mit Lokationen und Schichten verbunden sind.
- CA-Workflow-Vorlagen, die mit Kontakten verbunden sind.

Hinweis: Die auf einer Lokation basierende automatische Zuweisung wird kurz als automatische Zuweisung bezeichnet.

Auf einem Configuration Item basierende automatische Zuweisung

Erstellt Gruppenzuweisungen für Anfrage-, Problem- und Incident-Ticket-Typen basierend auf den folgenden Elementen:

- Bereiche, die mit Configuration Items verbunden sind, die mit Tickets verknüpft wurden.
- Configuration Item-Attribute, die zum Aufzeichnen von Kontakt/Gruppeninformation verwendet werden.

Die auf einer Lokation basierende automatische Zuweisung und die auf einem Configuration Item basierende automatische Zuweisung sind ausschließliche Optionen, weil Sie nur jeweils einen Algorithmus zur Verwendung in einem bestimmten Anfrage-/Incident-/Problembereich auswählen können. Sowohl die auf einer Lokation basierende automatische Zuweisung als auch die auf einem Configuration Item basierenden Methoden dienen dazu, Tickets bei ihrer Erstellung zuzuweisen. Die auf einem Configuration Item basierende automatische Zuweisung ist jedoch verschieden, weil sie außerdem immer dann die Zuweisungen für ein Ticket neu bewertet, wenn der Bereich oder das Configuration Item eines Anfrage-/Incident-/Problem-Tickets verändert wird. Wenn eine auf einem Configuration Item-basierende automatische Zuweisung angegeben ist, aber keine Gruppenzuweisung für ein Ticket erzeugen kann, dann wird die Option Area_Defaults herangezogen um zu entscheiden, ob die Standardwerte für Gruppen und Zuständige des Bereichs verwendet werden sollen, um das Ticket zuzuweisen.

Implementieren von automatischen Zuweisungen

Folgen Sie diesen Richtlinien, um automatische Zuweisungen für ausgewählte Analystengruppen und Analysten zu implementieren:

1. Geben Sie einen oder mehrere Bereiche oder Kategorien an, für die Sie automatische Zuweisungen aktivieren wollen.
Hinweis: Um die Konfiguration der Bereiche und Kategorien Ihres Standorts zu überprüfen, rufen Sie die entsprechenden Einstellungen in der CA SDM-Web-Schnittstelle auf. Weitere Anweisungen finden Sie in der *Online-Hilfe*.
2. Standardmäßig ist die automatische Zuweisung gesperrt. Aktivieren Sie sie nur für die [Bereiche und Kategorien](#) (siehe Seite 507), in denen Sie sie verwenden möchten.
3. Bauen Sie Beziehungen zwischen einem ermittelten Bereich oder einer Kategorie einerseits und den [Analystengruppen](#) (siehe Seite 508) andererseits auf, die für die Zuweisung von Tickets durch diesen Bereich oder diese Kategorie in Frage kommen.
4. Markieren Sie einzelne Mitglieder der [Analysten](#) (siehe Seite 509)gruppen als verfügbar.

Bereiche und Kategorien

Hinweis: Berücksichtigen Sie beim Konfigurieren von Bereichen und Kategorien die Einstellungen für [Standardgruppen und Zuständige](#) (siehe Seite 513).

Um Anfragen, Incidents, oder Problem-Tickets für die automatische Zuweisung zu konfigurieren, verwenden Sie die folgenden Steuerelemente auf der Registerkarte "Automatische Zuweisungen" der Detailseite für die Anfrage, den Incident bzw. das Problem befindet.

- Gruppen aktualisieren
- Lokationen aktualisieren
- Aktualisierungs-Schichten

Hinweis: Das Kontrollkästchen für die Aktivierung der automatischen Zuweisung befindet sich auch auf der Registerkarte "Automatische Zuweisungen" jeder dieser Seiten. Es wird nur angezeigt, während die Seite in Aufbereitungsmodus ist.

Die folgenden Seiten in der Schnittstelle bieten dieselben Steuerungen zum Konfigurieren der automatischen Zuweisung von Changes und Issues:

- "Change-Kategorie – Detail"
- "Issue-Kategorie – Detail"

Analystengruppen

Um die automatische Zuweisung zu konfigurieren, müssen Sie mindestens die Beziehungen zwischen Analystengruppen und Bereichen oder Kategorien definieren. Zuständige werden aus Gruppen ausgewählt, die *all* Ihre angegebenen Kriterien für die automatische Zuweisung erfüllen. Wenn keine zusätzlichen Einschränkungen definiert sind, werden die Tickets automatisch dem Gruppenmitglied zugewiesen, das die wenigsten aktiven Tickets aufweist.

Wenn keine Gruppen mit einem Bereich oder einer Kategorie verknüpft sind, werden die Standardgruppe und der Standardzuständige zugewiesen. Wenn diese Standardwerte nicht definiert sind, wird das Ticket für die manuelle Zuweisung zurückgestellt.

Sie können die Beziehungen zwischen Gruppen und Bereichen oder Kategorien auf der Bereichs- oder Kategoriendetailseite pflegen.

Alternativ können Sie die gleichen Beziehungen auf der Registerkarte "Automatische Zuweisungen" der Gruppen-Detailseite durch die Benutzung der folgenden Steuerelemente pflegen:

- Anfragebereiche aktualisieren
- Change-Kategorien aktualisieren
- Issue-Kategorien aktualisieren
- Lokationen aktualisieren

Analyst

Die Informationen in den Feldern auf der Detailseite "Analyst" kann dabei helfen herauszufinden, ob der Analyst für die automatische Zuweisung geeignet ist.

Analysten sind nur dann für die automatische Zuweisung geeignet, wenn sie als verfügbar gekennzeichnet sind.

Die Detailseite "Analyst" enthält ein Kontrollkästchen, über das die automatische Zuweisung aktiviert werden kann.

Ziehen Sie es in Betracht, dass Analysten ihre eigene Verfügbarkeit für die automatische Zuweisung kontrollieren können. Sie können die Verfügbarkeit von Analysten überwachen, indem Sie gespeicherte Abfragen verwenden.

Hinweis: Das Kontrollkästchen "Verfügbar" wird während der automatischen Zuweisung von Workflow-Aufgaben nicht berücksichtigt.

Das Feld "Arbeitsplan" ermöglicht es Analysten, dass Tickets nur während der geplanten Schicht automatisch zugewiesen werden. Analysten, den kein Arbeitsplan zugewiesen ist, die aber als verfügbar gekennzeichnet sind, stehen jederzeit für die automatische Zuweisung zur Verfügung, vorausgesetzt, es gibt keine weiteren Einschränkungen, die einen ungeeigneten Status zur Folge haben.

Automatisches Zuweisen von Tickets zu einer Gruppe und nicht zu Kontakten innerhalb der Gruppe

Die automatische Zuweisung in CA SDM weist Tickets zu Kontakten zu, bei denen die Option "Verfügbar" im Kontaktdatensatz ausgewählt ist. Allerdings können Sie Incidents/Issues/Changes/Requests automatisch einer Gruppe, aber nicht den Kontakten innerhalb der Gruppe zuweisen. Die Option NX_AUTOASG_GROUP_ONLY steuert das automatische Zuweisungsverhalten für Gruppen. Sie installieren diese Option, um die Tickets automatisch der Gruppe anstelle einzelner Kontakte zuzuweisen. NX_AUTOASG_GROUP_ONLY ist auf der Web-Schnittstelle nicht verfügbar. Sie installieren die Option über die Eingabeaufforderung.

Gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sich Ihre CA SDM-Installation mindestens auf der Ebene des kumulativen Version 12.9-Patch 2 befindet.
2. Öffnen Sie die Eingabeaufforderung auf einem beliebigen CA SDM-Server.

3. Führen Sie folgenden Befehl aus:

```
pdm_options_mgr -c -s AUTOASG_GROUP_ONLY -v 1 -a pdm_option.inst
```

Standardmäßig werden neue Optionen, die Sie zur Datei "NX.env" hinzufügen, nicht gespeichert, nachdem Sie "pdm_configure" ausgeführt haben. Sie können die Änderungen dauerhaft speichern, indem Sie die Option "-t" folgendermaßen festlegen:

```
pdm_options_mgr -c -s AUTOASG_GROUP_ONLY -v 1 -a pdm_option.inst -t
```

Diese Befehle aktualisieren die folgenden Dateien in CA SDM mit der neuen Option:

- Windows—NX_ROOT/NX.env und NX_ROOT\pdmconf\nx.env.nt.tpl
 - UNIX/Linux—NX_ROOT/pdmconf/NX.env.tpl
4. Öffnen Sie die Datei "NX.env" im CA SDM-Installationsverzeichnis, und suchen Sie nach der Variablen "@NX_AUTOASG_GROUP_ONLY=1" (befindet sich am Ende der Datei).
 5. Öffnen Sie die Datei "nx.env.nt.tpl", die sich unter NX_ROOT/pdmconf befindet, und suchen Sie nach der Option @NX_AUTOASG_GROUP_ONLY=1.
 6. Starten Sie den Dienst "CA SDM-Daemon-Server" neu.
CA SDM weist die Tickets nur der Gruppe automatisch zu.
 7. [Starten Sie die CA SDM-Server neu](#) (siehe Seite 52).

Automatische Zuweisung nach Lokation

Wenn Ihr Servicebereich groß ist und zahlreiche Lokationen umfasst, die verschiedene Kundengruppen betreuen, sollten Sie die Lokation wie folgt als Faktor in der Konfiguration der automatischen Zuweisung verwenden:

- **Lokation, die einem Bereich oder einer Kategorie zugewiesen ist** - Wenn Sie einem Bereich oder einer Kategorie eine Lokation zuweisen, werden Tickets in diesem Bereich oder dieser Kategorie nur automatisch zugewiesen, wenn eine übereinstimmende Lokation gefunden wird. Ein Anfrageticket wird beispielsweise automatisch zugewiesen, wenn es an den folgenden Lokationen einen berechtigten Analysten gibt:

1. Lokation des betroffenen Assets
2. Lokation des betroffenen Kunden

Wenn für das betroffene Asset oder den betroffenen Kunden keine Lokation angegeben ist, wird der Request der Standardgruppe und dem Standardzuständigen zugewiesen. Wenn diese Standardwerte nicht definiert sind, wird der Request für die manuelle Zuweisung zurückgestellt. Sie können die Bereichs- oder Kategoriedetailseiten verwenden, um Beziehungen zwischen Lokationen und Bereichen oder Kategorien zu pflegen.

- **Lokation, die einer Gruppe zugewiesen ist** - Wenn Sie eine Lokation mit einer Gruppe verknüpfen, kommen nur Mitglieder dieser Gruppe für die automatische Zuweisung der Tickets, die ihre Lokation betreffen, in Frage. Sie können Gruppenseiten benutzen, um Beziehungen zwischen Gruppen und Lokationen zu pflegen.

Mit den folgenden Steuerungen auf der Registerkarte "Automatische Zuweisung" der Seite "Lokation - Detail" können Sie Beziehungen zwischen Lokationen und Bereichen, Kategorien oder Gruppen verwalten:

- Anfragebereiche aktualisieren
- Change-Kategorien aktualisieren
- Issue-Kategorien aktualisieren
- Gruppen aktualisieren

Beispiele: Verwenden der Lokation beim Konfigurieren der automatischen Zuweisung

Im Folgenden finden Sie Beispiele, wie Sie die Lokation in Ihrer Konfiguration der automatischen Zuweisung verwenden können:

- **Automatische Zuweisung von Tickets nur an einer angegebenen Lokation** - Tickets von anderen Lokationen erhalten die Standardgruppe und/oder den Standardbevollmächtigten oder werden für die manuelle Zuweisung zurückbehalten. Beispielsweise sind viele Benutzer an Ihrem Unternehmenshauptsitz tätig und kleinere Benutzergruppen in den regionalen Niederlassungen. Eine Analystengruppe am Hauptsitz betreut ihre lokalen Benutzer, während mobile Analystengruppen die regionalen Niederlassungen besuchen. In diesem Fall könnten Sie die automatische Zuweisung der Tickets nur für die Analysten am Hauptsitz konfigurieren und den mobilen Analysten die Tickets manuell zuweisen.
- **Automatische Zuweisung von Tickets nach Benutzer- oder Asset-Lokation** - Sie können die automatische Zuweisung auf Analystengruppen an Lokationen einschränken, die mit der Lokation des betroffenen Benutzers oder der Lokation des betroffenen Assets übereinstimmen. Zum Beispiel kann Ihre Organisation über viele Büros verfügen, und Tickets von jedem Büro werden von den Mitarbeitergruppen in diesem Büro bearbeitet. Sie können jede Gruppe zu entsprechenden Bereichen oder Kategorien *und* zur entsprechenden Lokation in Beziehung setzen. Mit der Logik der automatischen Zuweisung werden die in Frage kommenden Analysten ausschließlich aus Gruppen an der richtigen Lokation ausgewählt.

Automatische Zuweisung nach Schicht

Sie können die automatische Zuweisung beschränken, indem Sie einer Schicht einen Bereich oder eine Kategorie zuordnen. Die Schicht bestimmt den Zeitrahmen, innerhalb dessen die Tickets für die automatische Zuweisung in Frage kommen. Tickets, die außerhalb der Arbeitszeit in dieser Schicht geöffnet werden, werden der Standardgruppe und dem Standardanalysten zugewiesen oder für die manuelle Zuweisung zurückgestellt.

Sie können Schichten auch dazu verwenden, um die Gruppen- und Analystenqualifikation für die Zuweisung zu steuern:

- Wenn Sie einer Gruppe einen Arbeitsplan zuweisen, sind Analysten in jener Gruppe nur zur automatischen Zuweisung zu Tickets berechtigt, die während ihres Arbeitsplans geöffnet wurden.

Hinweis: Die Schicht einer Gruppe wird im Feld "Arbeitsplan" der Gruppen-Detailseite angegeben.

- Wenn Sie einen Arbeitsplan einem individuellen Analysten zuweisen, ist der Analyst nur zur automatischen Zuweisung zu Tickets berechtigt, die während dieser Schicht geöffnet wurden.

Hinweis: Die Schicht eines Analysten wird im Feld "Arbeitsplan" der Detailseite "Analyst" angegeben.

Während der Ticket-Erstellung versucht die Logik für automatische Zuweisung, den Analysten mit den wenigsten aktiven Tickets in einer Gruppe zu identifizieren, die die Qualifikationskriterien für die Zuweisung erfüllen. Wenn kein geeigneter Analyst identifiziert wird, wird das Ticket der Standardgruppe und dem Bevollmächtigte zugewiesen. Wenn diese Standardwerte nicht definiert sind, wird das Ticket für die manuelle Zuweisung zurückgestellt.

Für Changes oder Issues zugewiesene Workflow-Aufgaben verwendet die automatische Zuweisung eine einfachere Auswahlstrategie. Bevollmächtigte werden aus Gruppen ausgewählt, die zu Workflow-Vorlagen zugeordnet sind. Bevollmächtigte für Workflow-Aufgaben können jeden Kontaktyp außer "Gruppe" annehmen. Wenn eine Aufgabe in den Status "In Bearbeitung" wechselt, wählt die automatische Zuweisung einen Kontakt aus, der über die geringste Anzahl von zugewiesenen Workflow-Aufgaben für Changes oder Issues verfügt. Um unerwünschte Ergebnisse zu verhindern, werden Aufgaben nicht automatisch zugewiesen, wenn die übergeordnete Change- oder Issue-Kategorie für die automatische Zuweisung nicht aktiviert ist. Da Workflow-Aufgaben potenziell Personen außerhalb der Service Desk-Organisation umfassen können, könnte es problematisch werden, sich darauf zu verlassen, dass diese ihre Verfügbarkeit mit dem verfügbaren Flag wiedergeben.

Hinweis: Die automatische Zuweisung von Workflow-Aufgaben wertet nicht den Verfügbarkeits-Flag aus und ist nicht für Kategorien verfügbar, die zur Verwendung der CA Workflow-Verarbeitung konfiguriert sind.

Sie können die Bereichs- oder Kategoriedetailseiten verwenden, um eine Schicht mit einem Bereich oder einer Kategorie in Beziehung zu setzen, oder Sie können die folgenden Steuerelemente auf der Schicht-Detailseite verwenden:

- Anfragebereiche aktualisieren
- Change-Kategorien aktualisieren
- Issue-Kategorien aktualisieren

Beispiele: Verwenden von Schichten bei der Konfiguration der automatischen Zuweisung

Im Folgenden finden Sie Beispiele, wie Sie Schichten in Ihrer Konfiguration für die automatische Zuweisung verwenden können:

- **Automatische Zuweisung von Tickets zur laufenden Schicht** - Wenn Ihr Service Desk 24 Stunden pro Tag arbeitet, sollten Sie die automatische Zuweisung so konfigurieren, dass Netzwerkausfallprobleme der laufenden Schicht zugewiesen werden, sobald das Ticket geöffnet wird.
- **Aktivieren der automatischen Zuweisung nur während einer angegebenen Schicht** - Unter Umständen sollten Sie die automatische Zuweisung der Tickets in einigen Bereichen oder Kategorien weiter einschränken. Wenn zum Beispiel die Anwendungsanalysten eines Standorts nur während einer Tagesschicht im Dienst sind, möchten Sie möglicherweise nur während der Tagesschicht Anwendungsprobleme automatisch zuweisen.

Standardgruppe und -zuständiger

Wenn die automatische Zuweisungslogik, die Sie konfiguriert haben, nicht in der Lage ist, eine passende Gruppe oder einen passenden Verantwortlichen zu identifizieren, wird das Ticket der Standardgruppe und dem Standardzuständigen zugeordnet. Sie können diese Standardwerte in den Feldern "Gruppe" und "Zuständiger" der folgenden Web-Schnittstellen-Seiten angeben:

- Anfrage-/Incident-/Problembereich - Detail
- Change-Kategorie - Detail
- Issue - Detail

Wenn die automatische Zuweisung keine geeignete Gruppe oder keinen geeigneten Zuständigen identifizieren kann und die Standardwerte nicht angegeben sind, wird das Ticket der manuellen Zuweisung zugeordnet.

Aktivieren der automatischen Zuweisung

Optionen und Steuerungen ermöglichen die Konfiguration automatischer Zuweisungen. Sie können steuern, ob der automatische Zuweisungsprozess folgendermaßen abläuft:

- Verwenden Sie für Requests, Incidents und Probleme, die diesem Bereich zugeordnet sind, die Registerkarte "Automatische Zuweisung aktiviert" auf der Detailseite für den Request-/Incident-/Problembereich.
- Wählen Sie für Changes, Issues und Workflow-Aufgaben die Registerkarte "Automatische Zuweisung", und aktivieren Sie das Kontrollkästchen "Automatische Zuweisung aktiviert" auf den Seiten "Change-Kategorie - Detail", "Issue-Kategorie - Detail" "Workflow-Vorlage - Detail".

Hinweis: Klicken Sie auf "Bearbeiten", um das Kontrollkästchen "Automatische Zuweisung aktiviert" sichtbar zu machen.

Beispiel: Automatische Zuweisung für einen Request-/Incident-/Problembereich aktivieren

Dieses Beispiel zeigt, wie die automatische Zuweisung für einen Request-/Incident-/Problembereich aktiviert wird.

1. Wählen Sie auf der Registerkarte "Administration" die Option "Service Desk" > "Requests/Incidents/Probleme" "> "Bereiche" aus.
Die Listenseite für den Request-/Incident-/Problembereich wird angezeigt.
2. Klicken Sie auf den Bereich, für den Sie die automatisch Zuweisung konfigurieren möchten.
Die Detailseite für den Request-/Incident-/Problembereich wird angezeigt.
3. Klicken Sie auf "Bearbeiten".
Die Seite "Request-/Incident-/Problembereich aktualisieren" wird angezeigt.

4. Wählen Sie die Registerkarte "Automatische Zuweisung" aus, und geben Sie Folgendes in die Felder ein:

Automatische Zuweisung – Modus

Gibt an, wie die automatische Zuweisung durchgeführt wird. Verwenden Sie die Option "Configuration Item-basiert, um eine automatische Zuweisung auf der Basis des Attributwerts für "CI zuweisbar" durchzuführen.

- **Deaktiviert** – Legt der automatischen Zuweisung die Option "Bereichsstandardwerte" zugrunde, sofern diese installiert ist.
- **Auf einem Configuration Item basierend** – Legt der automatischen Zuweisung den Wert des zuweisbaren CI-Attributs zugrunde.
- **Lokationsbasiert** – Legt der automatischen Zuweisung den Speicherortwert zugrunde.

Zuweisbares CI-Attribut

Gibt das für die Gruppenzuweisung zu verwendende Configuration Item-Attribut an. Sie können direkt einen Wert eingeben oder auf das Lupensymbol klicken, um nach einem Attribut zu suchen.

5. Klicken Sie auf "Speichern".

Im aktivierten Request-/Incident-/Problembereich können Sie Standardwerte definieren, die automatisch in Request-, Incident- oder Problem-Tickets eingetragen werden, die dem Bereich zugewiesen werden.

Überschreiben der automatischen Zuweisung

Über die Option "Automatische Zuweisung überschreiben" ("autoasg_override") im Optionsmanager wird festgelegt, ob die automatische Zuweisung einen Analysten oder eine Gruppe überschreiben kann, der bzw. die während der Erstellung eines Tickets festgelegt wurden.

Möglicherweise wurde der Verantwortliche bzw. die Gruppe von anderen CA SDM-Funktionen bereits vor Aktivierung der automatischen Zuweisung festgelegt. Sie können das System anpassen, indem Sie für diese Option einen der folgenden Werte angeben:

0

Berücksichtigt den vorhandenen Zuständigen und/oder die vorhandene Gruppe. Die automatische Zuweisung findet nicht statt, wenn der Verantwortliche und/oder die Gruppe während der Erstellung der Anfrage festgelegt werden.

1

Ignoriert den vorhandenen Zuständigen und/oder die vorhandene Gruppe. Die automatische Zuweisung wird fortgesetzt und es wird versucht, einen Verantwortlichen und/oder eine Gruppe zu finden.

Sie können den Zuständigen und/oder die Gruppe auf verschiedene Weise festlegen:

- manuell durch den Analytiker
- durch Optionen für Bereichs-Standardwerte und die Festlegung des Zuständigen
- Vorlagen für Requests
- CA NSM-Integration

Hinweis: Die Deinstallation der Option "Automatische Zuweisung überschreiben" bewirkt, dass sie den Standardmodus, d. h. 0, verwendet.

Zuweisungssteuerungen

Optionen und Steuerungen ermöglichen die Konfiguration automatischer Zuweisungen. CA SDM-Funktionen können die Felder für den Zuständigen bzw. die Gruppe in einem Ticket vor Aktivierung der automatischen Zuweisung beeinflussen. Wir empfehlen, dass Sie Zuweisungssteuerungen vor der Implementierung der automatischen Zuweisung überprüfen.

Manuelle Zuweisung

Der Analyst kann den Verantwortlichen bzw. die Gruppe manuell auswählen, während er ein Ticket anlegt.

Option „Assignee_set“

Standardmäßig legt CA SDM automatisch den angemeldeten Benutzer als Zuständigen der Anfrage fest, wenn dieser Benutzer ein Analyst ist. Mit der Optionsmanager-Option "Assignee_set" können Sie dieses Verhalten steuern. Diese Option wird normalerweise standardmäßig installiert.

Iss assignee_set

Die Option "Iss assignee_set" legt den angemeldeten Benutzer automatisch als der Zuständigen für den Issue fest, wenn dieser Benutzer ein Analyst ist. Sie ist mit der Option "Assignee_set" vergleichbar, bezieht sich aber auf Issues anstatt auf Anfragen.

Area_Defaults

Über diese Option wird festgelegt, was geschieht, wenn der Anforderungsbereich auf dem Detailformular einer Anforderung aufgeführt ist. Diese Option ermöglicht Ihnen, den Zuständigen und die Gruppe festzulegen, wenn sich der Anfragebereich ändert. Der Standardbevollmächtigte und die Standardgruppe aus dem Anfragebereich werden verwendet, und die Verarbeitung findet vor der automatischen Zuweisungsverarbeitung statt.

Diese Option ist standardmäßig nicht installiert.

Hinweis: Die Option "Category_Defaults" bietet eine ähnliche Funktion für Changes. Die Option "Iss_Category_Defaults" bietet eine ähnliche Funktion für Issues.

Optionen, die einen Zuständigen/eine Gruppe erfordern

Im Optionsmanager sind mehrere Optionen zur Steuerung der Erstellung von nicht zugeordneten Tickets verfügbar. Diese Optionen sind in ihrem Umfang global. Sie betreffen die Erstellung aller angegebenen Tickettypen, unabhängig davon, ob die automatische Zuweisung in Kraft ist. Wenn die angegebene Bedingung nicht erfüllt ist, kann das neue oder aktualisierte Ticket nicht gespeichert werden.

Die folgenden Optionen steuern die Erstellung von Tickets ohne Angabe eines Zuständigen:

require_change_assignee

Anwendung: Change-Mgr

Beschreibung: Macht das Feld "Zuständiger" eines Change-Tickets obligatorisch.

require_issue_assignee

Anwendung: Issue-Mgr

Beschreibung: Macht das Feld "Zuständiger" eines Issue-Tickets obligatorisch.

require_incident_assignee

Anwendung: Request-Mgr

Beschreibung: Macht das Feld "Zuständiger" eines Incident-Tickets obligatorisch.

require_problem_assignee

Anwendung: Request-Mgr

Beschreibung: Macht das Feld "Zuständiger" eines Problem-Tickets obligatorisch.

require_request_assignee

Anwendung: Request-Mgr

Beschreibung: Macht das Feld "Zuständiger" eines Request-Tickets obligatorisch.

Die folgenden Optionen steuern die Erstellung von Tickets ohne Gruppenangabe:

require_change_group

Anwendung: Change-Mgr

Beschreibung: Macht das Feld "Gruppe" eines Change-Tickets obligatorisch.

require_issue_group

Anwendung: Issue-Mgr

Beschreibung: Macht das Feld "Gruppe" eines Issue-Tickets obligatorisch.

require_incident_group

Anwendung: Request-Mgr

Beschreibung: Macht das Feld "Gruppe" eines Incident-Tickets obligatorisch.

require_request_group

Anwendung: Request-Mgr

Beschreibung: Macht das Feld "Gruppe" eines Request-Tickets obligatorisch.

require_problem_group

Anwendung: Request-Mgr

Beschreibung: Macht das Feld "Gruppe" eines Problem-Tickets obligatorisch.

Vorlagen

Vorlagen können verwendet werden, um die Werte einer neuen Anfrage, eines neuen Changes oder eines neuen Issues festzulegen. Zu den Feldern, die von Vorlagen beeinflusst werden können, zählen Verantwortlicher und Gruppe.

CA Network and Systems Management-Schnittstelle

Wenn CA NSM und CA SDM integriert sind und Sie Anfragen von CA NSM-Ereignissen erstellen, wird der Parameter "user_parms" in den Erstellerregeldefinitionen an die Text-API übergeben. Der CA SDM-Erstellerprozess (tngwriter) definiert seine eigenen Ersetzungsparameter zum Ändern des Textes, bevor dieser an die Text-API gesendet wird. Das Schlüsselwort LOG_AGENT wird zum Ende der Eingabe hinzugefügt, um das "log_agent" für die Anfrage zu setzen.

Hinweis: Sie müssen das die Datei "Text_API.cfg" für alle Felder aktualisieren, die von CA NSM-Alert Management Systemen an CA SDM weitergegeben werden. Diese Datei wird für Integrationen in Webservices, E-Mail und AHD.DLL. verwenden.

Weitere Informationen:

[Schlüsselwörter](#) (siehe Seite 582)

Aktivitätsprotokoll

Die automatische Zuweisung protokolliert Informationen als Ereignisse im Aktivitätsprotokoll des Tickets. Der Erfolg oder das Fehlschlagen der automatischer Zuweisung sowie Anomalien, die während Verarbeitung aufgetreten sind, werden protokolliert.

Aktivieren der Aktivitätsprotokollierung für zusätzliche Attribute

Aktivitätsprotokolle zeigen Änderungen an Attributwerten von Objekten an. Die Aktivitätsprotokollierung funktioniert für Objekte wie sämtliche Tickettypen, klassische Workflow-Aufgaben, Umfragen, Kontakte und Configuration Items. Sie können Aktivitätsprotokollierung für zusätzliche Attribute in WSP aktivieren.

Hinweis: Sie können einfache Attribute des Aktivitätsprotokolls einschließlich Zeichenfolgen, Ganzzahlen, Datumsangaben, Dauer und SREL-Typen anzeigen. Sie können keine Aktivitätsprotokolle für Listentypen wie QREs und BREs anzeigen.

Gehen Sie wie folgt vor:

1. Öffnen Sie WSP und starten Sie den Schemadesigner.
2. Wählen Sie die Tabelle aus, die Sie ändern wollen, und fügen Sie zusätzliche Attribute hinzu.
3. Fügen Sie für jedes Attribut +AUDITLOG() zum durch den Standort definierten UI_INFO-Feld hinzu.
Wichtig! Wenn Sie das Flag AUDITLOG hinzufügen, *müssen* Sie die Funktion `val_fieldupdate_site()` entfernen, um doppelte Aktivitätsprotokolle zu verhindern.
4. Speichern und veröffentlichen Sie das Schema.
5. Öffnen Sie WSP erneut, und fügen Sie die neuen Attribute zu den entsprechenden Detailformularen hinzu.
6. Öffnen Sie CA SDM, und definieren Sie eine Aktivitätszuordnung für die zusätzlichen Attribute.
7. Testen Sie Ihre Änderungen.

Öffnen Sie zum Beispiel eine früher gespeicherte Instanz des Objekts und ändern Sie die betroffenen Attribute, um zu überprüfen, ob die passenden Aktivitätsprotokolle angezeigt werden.

Ablaufverfolgung der automatischen Zuweisung

In einer komplexen Implementierung der automatischen Zuweisung kann es vorkommen, dass die automatische Zuweisung nicht die Entscheidungen trifft, die erwartet werden. Damit Sie den Prozessablauf besser verstehen, kann die Ablaufverfolgung aktiviert werden. Die Ablaufverfolgung ist normalerweise deaktiviert. Wenn sie aktiviert ist, werden in den stdlog-Dateien in "\$NX_ROOT\log" zahlreiche Meldungen aufgezeichnet, die die verschiedenen Entscheidungen der automatischen Zuweisung beschreiben.

Gehen Sie mit Vorsicht vor, wenn Sie sie in einer Installation mit hoher Aktivität implementieren, da die Vielzahl der generierten Meldungen bewirken kann, dass die Protokolldateien anwachsen und schließlich zu anderen Protokolldateien gewechselt werden muss. Auf sehr aktiven Systemen kann dies eine Herabsetzung der Leistung bewirken. Die Ablaufverfolgung wird mit dem Dienstprogramm "pdm_logstat" gesteuert. Die von diesem Dienstprogramm verwendeten Parameter unterscheiden zwischen Groß- und Kleinschreibung. Achten Sie darauf, die Parameter genau wie gezeigt einzugeben.

Um die Ablaufverfolgung zu aktivieren, verwenden Sie folgenden Befehl auf jedem CA SDM-Server:

```
pdm_logstat -f auto.pm milestone
```

Um die Ablaufverfolgung zu deaktivieren, verwenden Sie folgenden Befehl auf jedem CA SDM-Server:

```
pdm_logstat -f auto.pm
```

Gespeicherte Abfragen

Zur Überwachung der Verfügbarkeit von Analysten werden zwei gespeicherte Abfragen bereitgestellt. CA SDM-Manager können diese ihrem Scoreboard hinzufügen:

- **Verfügbare Analysten** - Analysten, die als für automatische Zuweisung verfügbar markiert werden
- **Nicht verfügbare Analysten** - Analysten, die als für automatische Zuweisung nicht verfügbar markiert werden

Automatisches Zuweisen von Tickets

Die Funktion "Automatische Zuweisung" weist Tickets folgendermaßen zu:

1. Das Speichern eines neuen Tickets löst eine automatische Zuweisung aus.
Wenn ein Bereich oder eine Kategorie nicht für eine automatische Zuweisung konfiguriert ist, wird die Verarbeitung angehalten.
2. Die automatische Zuweisung bestimmt, ob "Autoasg_override" installiert ist.
Ist dies nicht der Fall und das Ticket besitzt einen Zuständigen oder eine Gruppe, wird die Verarbeitung angehalten.

3. Wenn sich Schichten auf das Ticket beziehen, wird das offene Datum ausgewertet, um zu entscheiden, ob eine Schicht das Ticket einschließt.

Wenn eine Schicht das Ticket nicht einschließt, hält die Verarbeitung an und die automatische Zuweisung versucht, die Standardgruppe und den Zuständigen zuzuweisen.

4. Die automatische Zuweisung entscheidet, ob Gruppen zu dem Ticket gehören.

Wird keine Übereinstimmung gefunden, so wird die Verarbeitung angehalten und die automatische Zuweisung versucht, die Standardgruppe und den Zuständigen zuzuweisen.

5. Die automatische Zuweisung filtert Gruppen mit einer zugeordneten Schicht heraus, bei denen das offene Datum außerhalb des Zeitraums der Schicht ist. Gruppen ohne Arbeitsschicht umgehen die Filterung.

6. Das Folgende tritt für Lokationen auf, die mit dem Ticket im Zusammenhang stehen:

- Wenn dieses Ticket eine Anforderung ist und über ein Configuration Item verfügt:

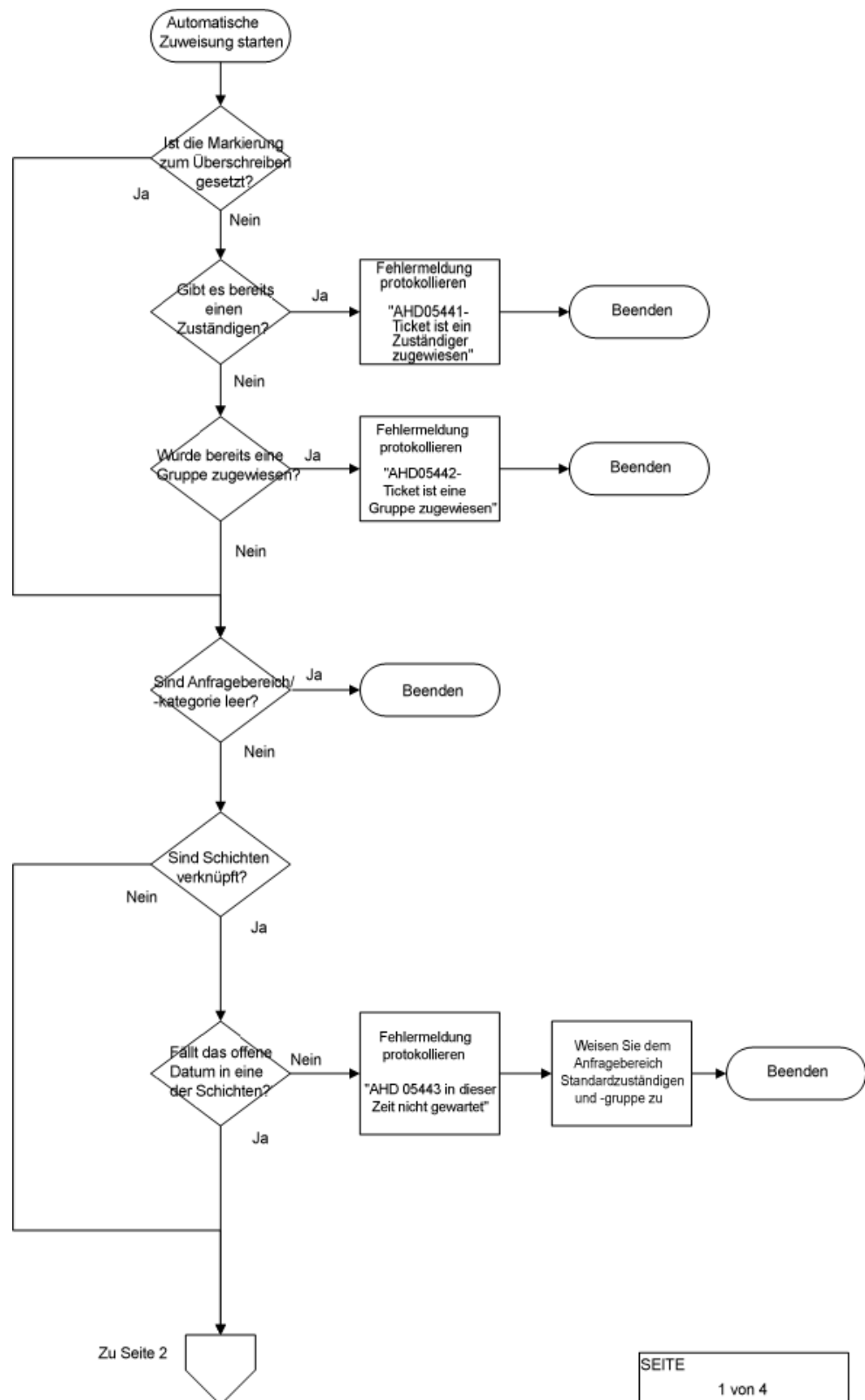
Die Lokation des Configuration Items wird mit den auf den Anfragebereich bezogenen Lokationen verglichen. Wird keine Übereinstimmung gefunden, so wird die Verarbeitung angehalten und die automatische Zuweisung versucht, die Standardgruppe und den Zuständigen zuzuweisen. Andernfalls wird die Kundenlokation mit den Positionen verglichen, die mit dem Anforderungsbereich oder der Kategorie im Zusammenhang stehen. Wird keine Übereinstimmung gefunden, so wird die Verarbeitung angehalten und die automatische Zuweisung versucht, die Standardgruppe und den Zuständigen zuzuweisen.

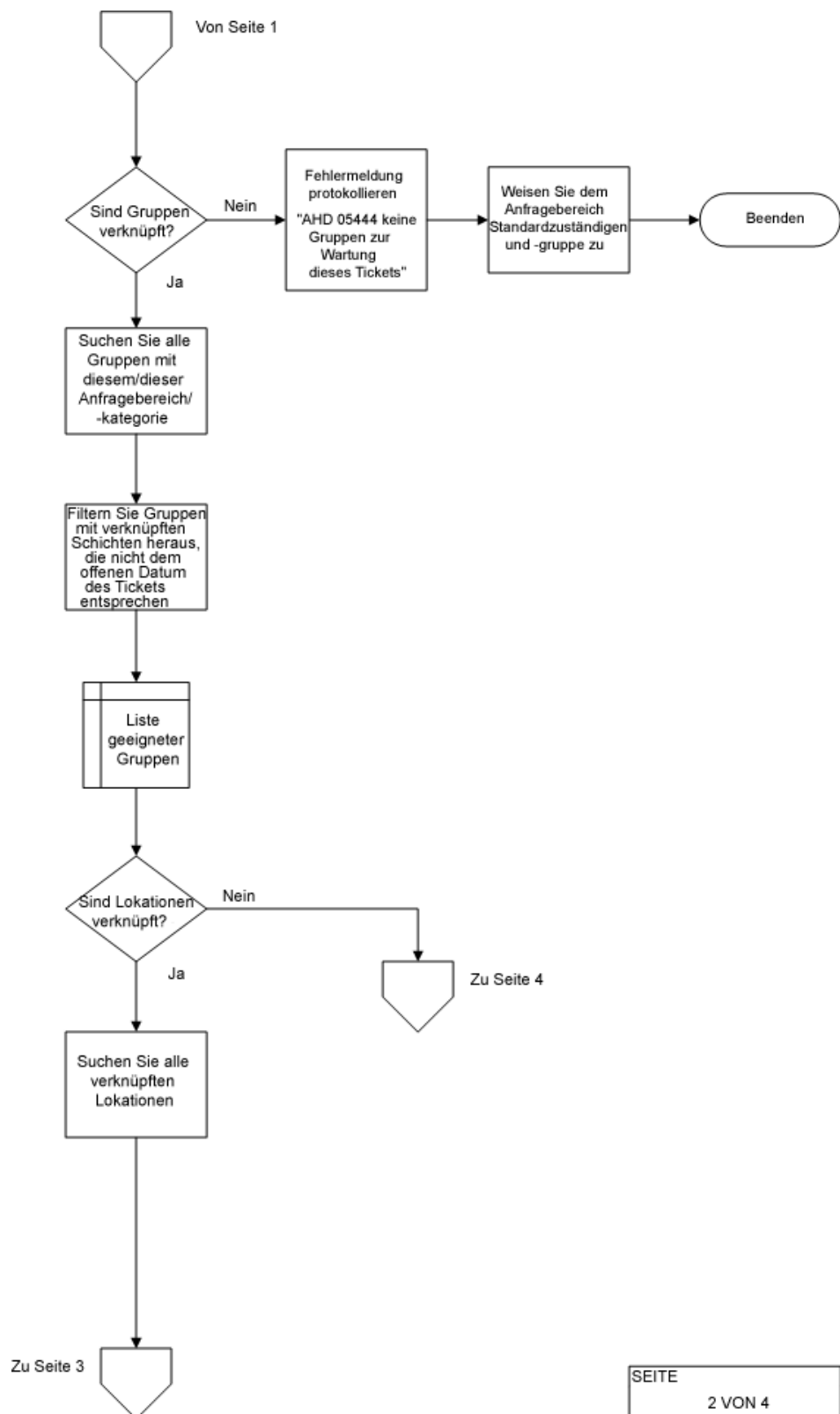
- Wenn Lokationen dem Anforderungsbereich oder der Kategorie zugeordnet sind:

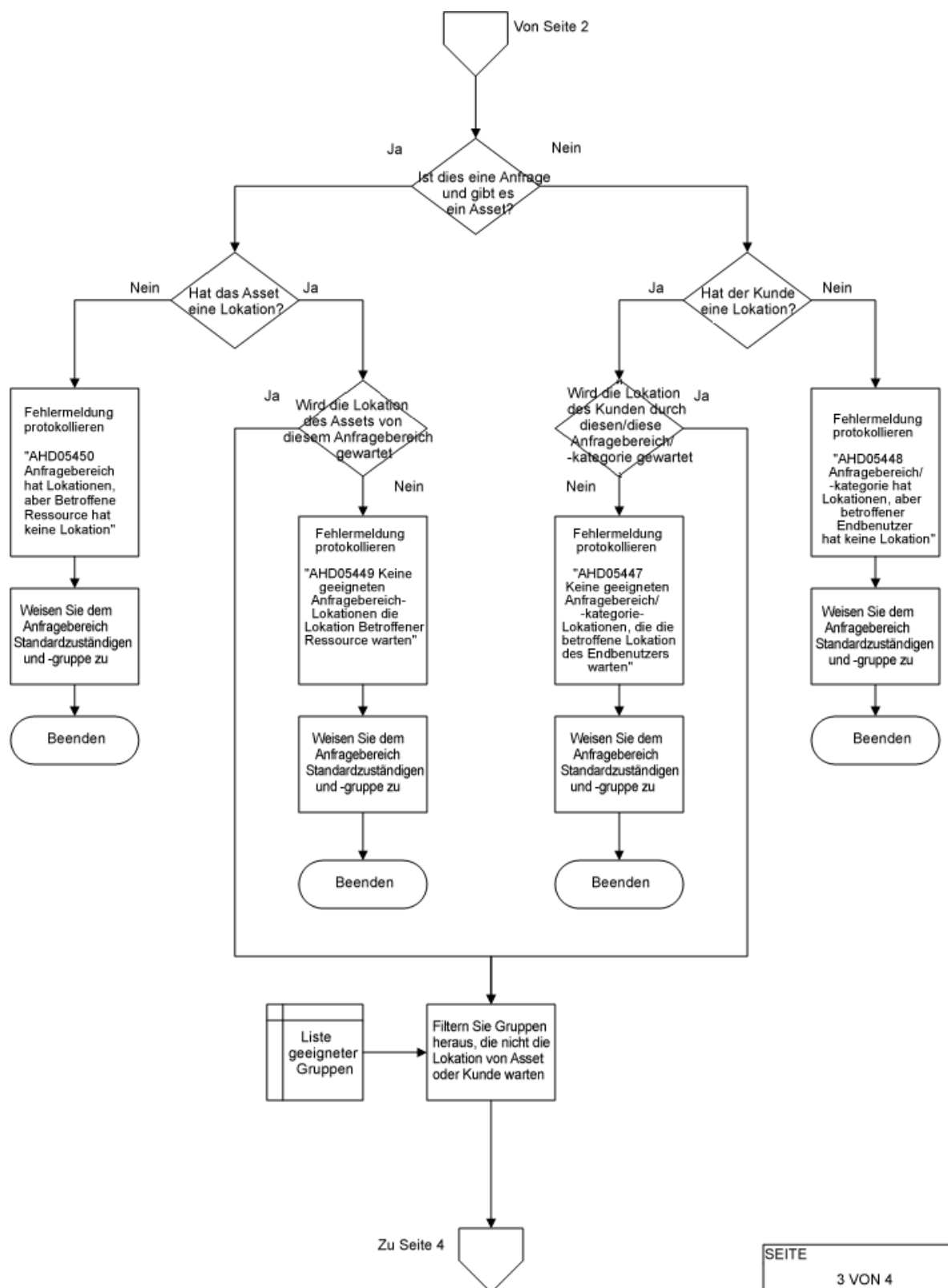
Wenn Lokationen dem Anfragebereich und dem Configuration Item zugeordnet sind (während der automatischen Zuweisung der Anfrage) oder der Kunde keine Lokationen hat, hält die automatische Zuweisung die Verarbeitung an.

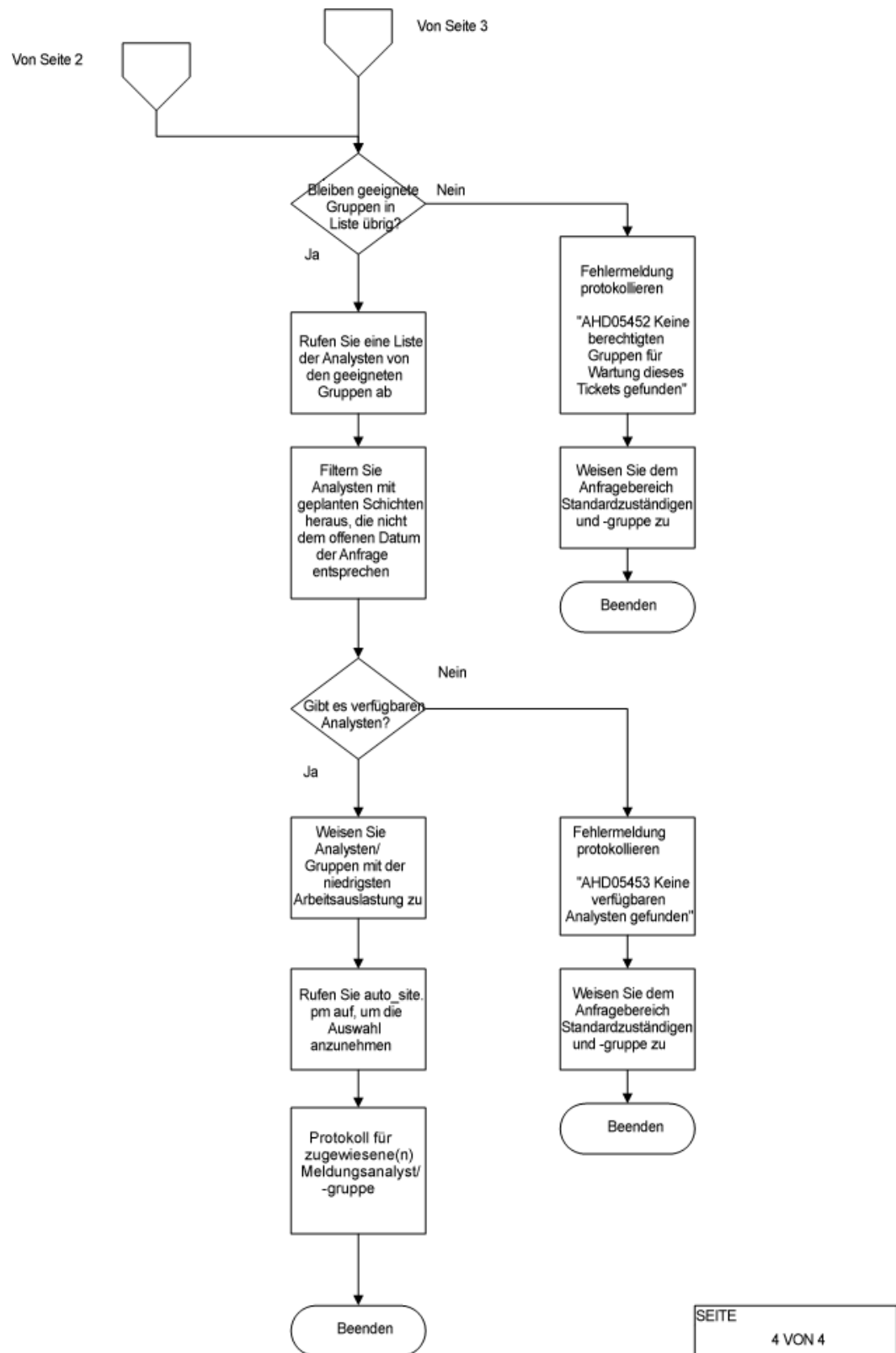
7. Die automatische Zuweisung filtert berechnete Gruppen mit zugehörigen Lokationen heraus, die nicht dem Configuration Item (nur für Anfragen) oder der Lokation des Kunden entsprechen. Wenn keine Gruppen übrigbleiben, so wird die Verarbeitung angehalten und die automatische Zuweisung versucht, die Standardgruppe und den Zuständigen zuzuweisen.
8. Die automatische Zuweisung erstellt von jeder der verbleibenden berechtigten Gruppen eine Liste von Analysten.
9. Nicht verfügbare Analysten werden herausgefiltert.
10. Für die restlichen Analysten wird geprüft, ob Arbeitspläne vorhanden sind. Analysten, für die Arbeitspläne vorhanden sind, werden herausgefiltert, wenn das Öffnungsdatum nicht innerhalb der Arbeitspläne des Analysten liegt.

11. Wenn keine Analysten übrigbleiben, so wird die Verarbeitung angehalten und die automatische Zuweisung versucht, die Standardgruppe und den Zuständigen zuzuweisen.
12. Alle verbleibenden Analysten werden gemäß der Anzahl der ihnen zugeteilten aktiven Tickets in eine Rangordnung eingeteilt.
13. Der Analyst (und die zugehörige Gruppe) mit der niedrigsten Anzahl aktiver Tickets werden dem Ticket zugewiesen. Wenn es zu einem Unentschieden kommt, wird der erste Analyst in der Gruppe ausgewählt.





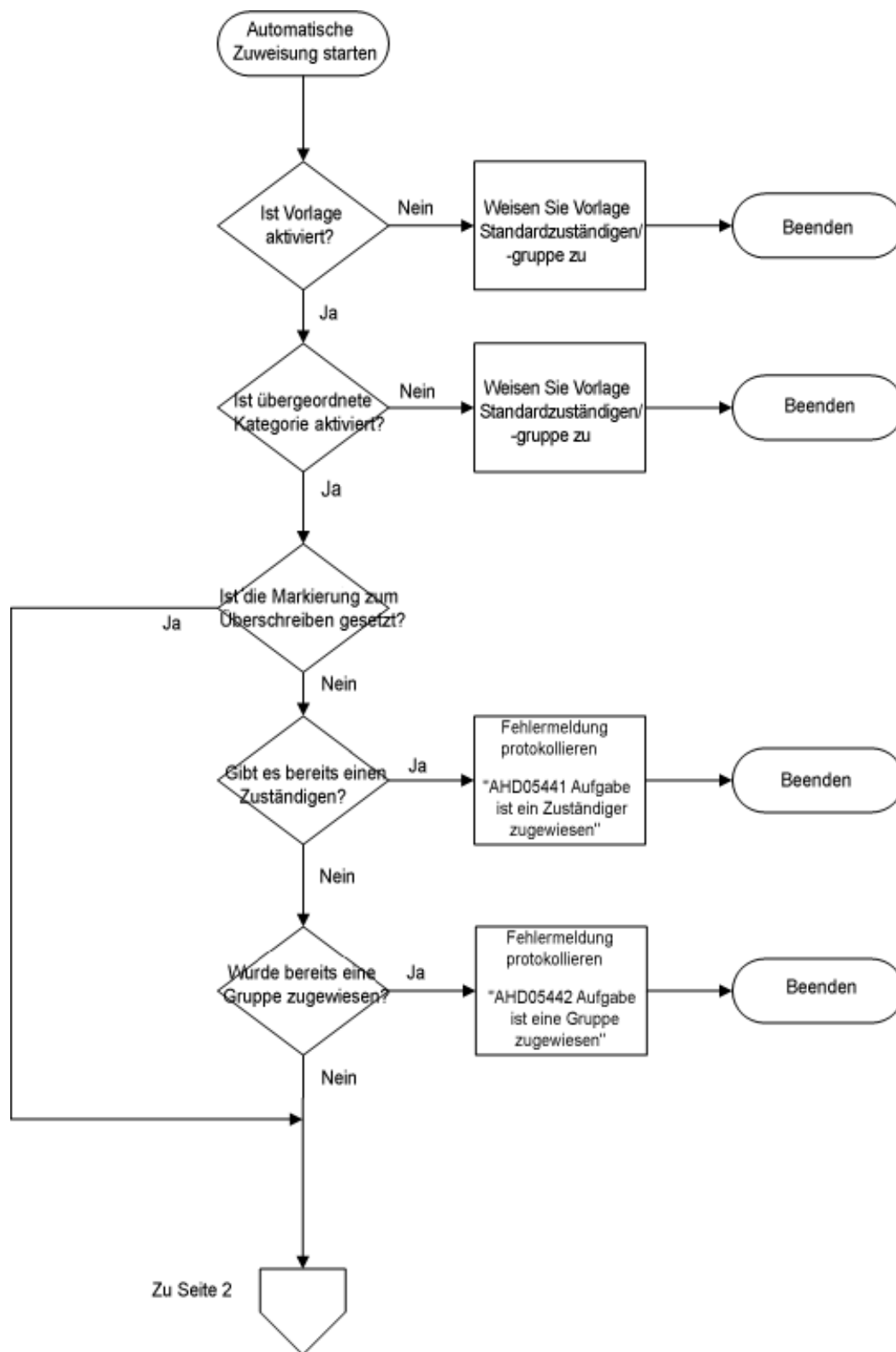


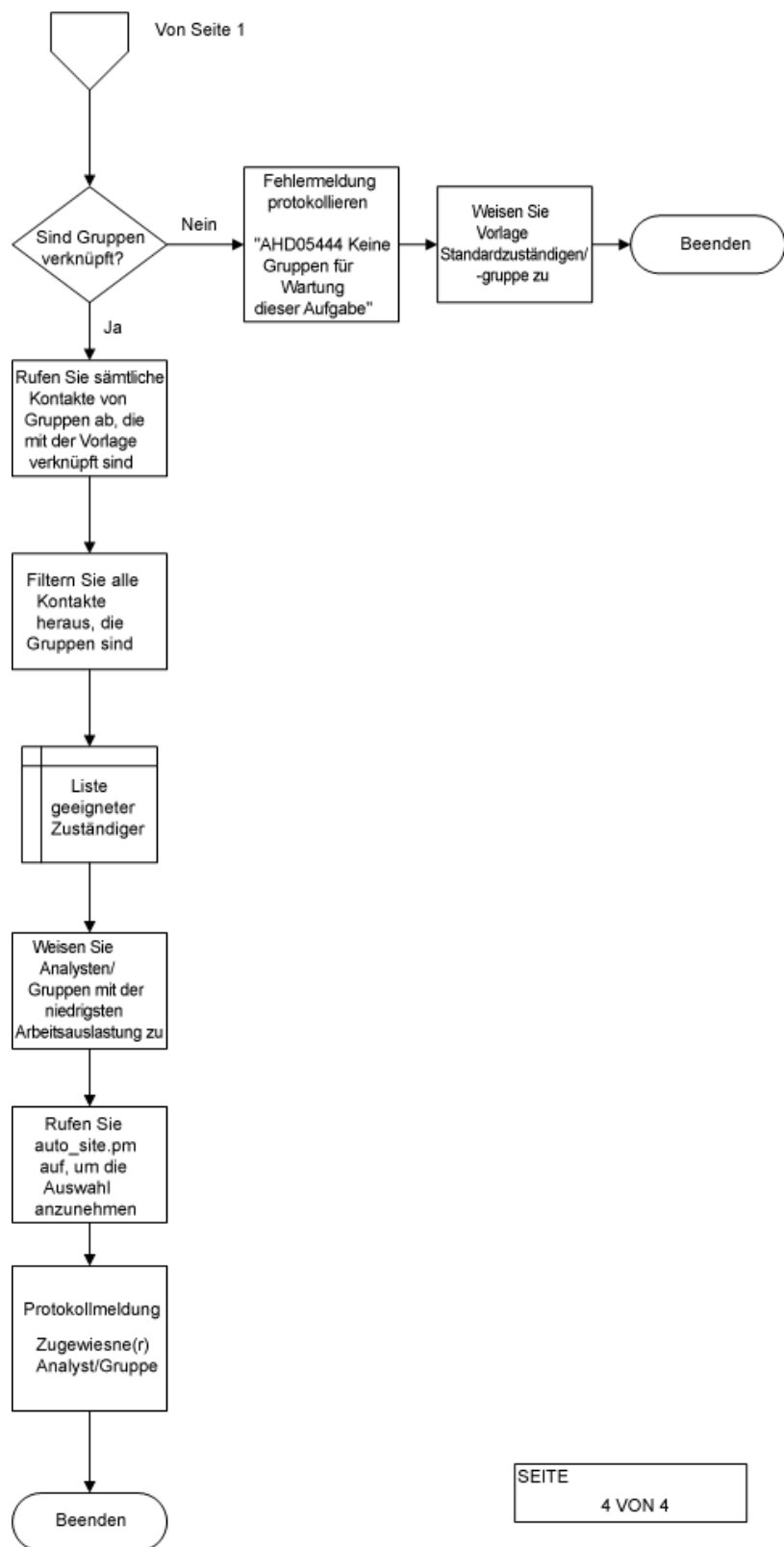


Automatisches Zuweisen von Workflow-Aufgaben

Die automatische Zuweisung setzt eine Verarbeitungslogik ein, um Workflow-Aufgaben folgendermaßen zuzuweisen:

1. Die automatische Zuweisung wird aufgerufen, wenn sich der Status einer Workflow-Aufgabe in "In Bearbeitung" ändert. Wenn die Workflow-Vorlage, auf deren Basis die Workflow-Aufgabe erstellt wurde, nicht für die automatische Zuweisung aktiviert ist, wird die Verarbeitung angehalten. Wenn die übergeordnete Change-Kategorie oder Issue-Kategorie nicht für die automatische Zuweisung aktiviert ist, wird die Verarbeitung angehalten.
2. Die automatische Zuweisung überprüft, ob Autoasg_override installiert ist. Ist dies nicht der Fall und die Aufgabe besitzt einen Zuständigen oder eine Gruppe, wird die Verarbeitung angehalten.
3. Die Workflow-Vorlage, auf deren Basis die Workflow-Aufgabe erstellt wurde, wird geprüft, um festzustellen, ob ihr Kontakte zugewiesen sind. Wenn keine Kontakte vorhanden sind, wird die Verarbeitung angehalten.
4. Die automatische Zuweisung erstellt eine Liste aller Kontakte, die Mitglieder der Gruppen sind, die aktuell mit der als Basis für die Workflow-Aufgabe verwendeten Workflow-Vorlage verknüpft sind. Handelt es sich bei Kontakten in dieser Liste um Gruppen, so werden diese herausgefiltert.
5. Alle verbleibenden Kontakte werden gemäß der Anzahl der ihnen zugewiesenen aktiven Change- oder Issue-Aufgaben in eine Rangordnung eingeteilt.
6. Der Kontakt und die zugehörige Gruppe mit der niedrigsten Anzahl aktiver Aufgaben werden der Aufgabe zugewiesen.





Configuration Item-basierte automatische Zuweisungen

Mithilfe von Configuration item-basierter automatischer Zuweisung können Sie gruppenspezifische Zuweisungen erstellen, die für bestimmte Szenarios gelten. Sie können angeben, dass die Zuweisung eines Anfrage-/Incident-/Problem-Tickets, das für einen bestimmten Bereich geöffnet wird, von dem Wert des mit dem Ticket verknüpften Configuration Item abhängen soll.

Configuration item-basierte und speicherortbasierte automatische Zuweisungen sind exklusive Optionen, da Sie nur einen Algorithmus zur Anwendung auf einen Anfrage-/Incident-/Problembereich auswählen können. Configuration Item-basierte und lokationsbasierte Modi zur automatischen Zuweisung dienen beide zum Zuweisen von Tickets, wenn sie erstellt werden; die Configuration Item-basierte automatische Zuweisung ist allerdings unterschiedlich, da sie Tickets auch erneut zuweist, wenn der Anfrage-/Incident-/Problembereich eines Tickets oder Configuration Items geändert wird.

Beispiel: Anfrage-/Incident-/Problembereich weist Tickets einer Gruppe zu

Wenn Sie den Netzwerkbereich (für Anfragen/Incidents/Probleme) konfigurieren, um Configuration Item-basierte automatische Zuweisungen mit Hilfe des Attributs "network_contact_uuid" (Netzwerkoperationen) als Wert "Zuweisbares CI-Attribut" durchzuführen, werden alle für den Netzwerkbereich geöffneten Tickets automatisch der Gruppe zugeordnet, die im Feld "Netzwerkoperationen" des dem Ticket zugeordneten CI angegeben ist. Wenn dem Ticket kein CI zugeordnet ist oder der Wert des Feldes "Netzwerkoperationen" des CI leer ist oder aber keine Gruppe angibt, findet die Zuweisung nicht statt. In solchen Fällen handelt das System in Übereinstimmung mit der Option "Bereichs-Standardwerte" im Optionsmanager und weist das Ticket mit Hilfe der Felder "Gruppe" und "Zuständiger" der Kategorie zu.

Funktionsweise der auf einem Configuration Item basierenden automatischen Zuweisungen

Anfrage/Incident/Problem-Tickets müssen Folgendes angeben, damit eine auf einem Configuration Item basierende automatische Zuweisung erfolgt:

- ein Configuration Item und einen Bereich.
- Für den Bereich muss die Option "Automatische Zuweisung" auf "Auf einem Configuration Item basierend" eingestellt sein.

Wenn ein Analyst ein Ticket erstellt und es diesem Bereich zuweist oder den Bereich auf einem bestehenden Ticket ändert, prüft CA SDM das Feld "Zuweisbares CI-Attribut" des Bereiches. CA SDM verwendet den Wert von "Zuweisbares CI-Attribut" als Name eines Attributs und versucht dann, ein gleich benanntes Attribut auf dem Configuration Item zu finden, das mit dem Ticket verknüpft ist. Wenn das Attribut auf dem Configuration Item eine Gruppe mit einschließt, wird das Ticket jener Gruppe zugewiesen.

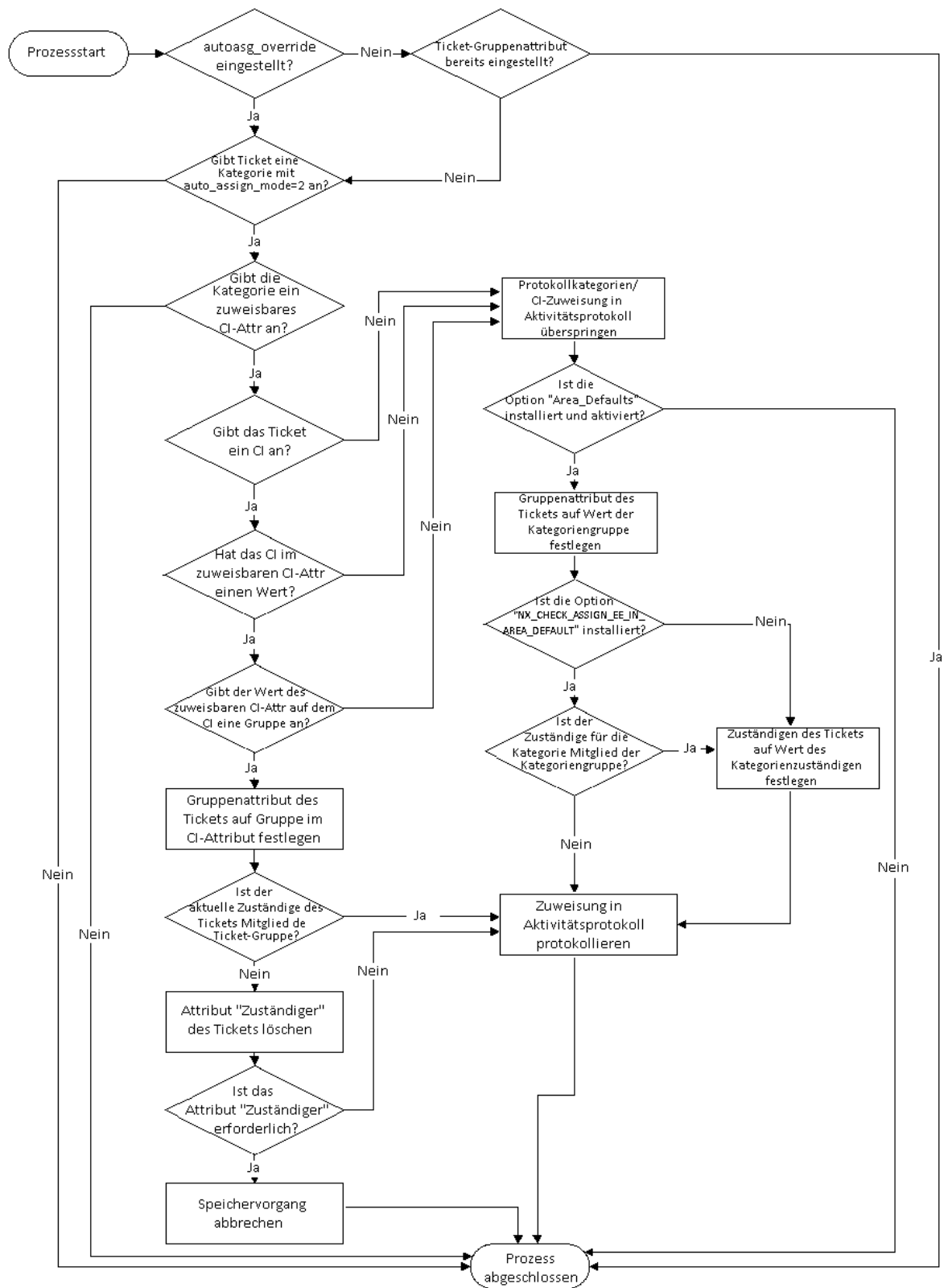
Das folgende Diagramm beschreibt den Prozess für eine auf einem Configuration Item basierende automatische Zuweisung ausführlicher:

1. CA SDM überprüft Folgendes:
 - a. Ist die Option "autoasg_override" eingestellt?
 - b. Gibt ein Ticket einen Bereich mit der automatischen Zuweisung "auto_assign_mode=2" an?
 - c. Gibt die Kategorie ein zuweisbares CI-Attribut an?
 - d. Ist auf dem Ticket ein Configuration Item angegeben?
 - e. Weist das Configuration Item einen zuweisbaren CI-Attributwert auf?
 - f. Gibt der Wert eine Gruppe im CI-Attribut an?
 - g. Ist der Zuständige des Tickets ein Mitglied der Ticketgruppe?

2. Wenn alle Fragen im vorherigen Schritt bejaht werden, stellt CA SDM das Gruppenattribut des Tickets auf das CI-Gruppenattribut ein und trägt die Zuweisung ins Aktivitätsprotokoll ein.

Hinweis: Das Diagramm zeigt, wie eine auf einem Configuration Item basierende automatische Zuweisung die Variable `NX_CHECK_ASSIGNEE_IN_AREA_DEFAULTS` verwendet, um zu entscheiden, ob die Option "Bereich" aktiviert ist. `NX_CHECK_ASSIGNEE_IN_AREA_DEFAULTS` ist eine Variable in der Datei "NX.env", die sich im Verzeichnis "\$NX_ROOT\" befindet.

3. CA SDM weist der Gruppe das Ticket zu.



Weitere Informationen:

[Überschreiben der automatischen Zuweisung](#) (siehe Seite 515)

Aktivieren von Configuration Item-basierten automatischen Zuweisungen

Mit Hilfe der automatischen Zuweisung auf der Basis von Configuration Items können Sie gruppenspezifische Zuweisungen erstellen, die für bestimmte Szenarios gelten. Sie können angeben, dass die Zuweisung eines Anfrage-/Incident-/Problem-Tickets, das für einen bestimmten Bereich geöffnet wird, von dem Wert des mit dem Ticket verknüpften Configuration Item abhängen soll. Bei automatischer Zuweisung auf der Basis von Configuration Items werden Tickets erneut zugeordnet, wenn sich der Anfrage/Incident/Problem-Bereich des Tickets oder des Configuration Items ändert.

Hinweis: Die Option "autoasg_override" im Optionsmanager regelt die Umstände, unter denen die automatische Zuweisung stattfindet. Wenn Sie für diese Option den Wert 1 angeben, ignoriert CA SDM die bestehenden Einstellungen für Verantwortliche und Gruppen, und führt in jedem Fall eine automatische Zuweisung der Tickets durch. Wenn CA SDM nur Tickets automatisch zuweisen soll, die noch nicht zugewiesen wurden, legen Sie für diese Option "0" fest.

So aktivieren Sie die Configuration Item-basierte automatische Zuweisung

1. Wählen Sie auf der Registerkarte "Administration" die Option "Service Desk" > "Anfragen/Incidents/Probleme" > "Bereiche" aus.

Die Seite "Anfrage-/Incident-/Problembereiche - Liste" wird angezeigt.

2. Wählen Sie den zu bearbeitenden Bereich aus.

Die Seite "Bereich - Detail" wird angezeigt.

3. Klicken Sie auf "Bearbeiten".

Die Seite "Bereich aktualisieren" wird angezeigt.

4. Wählen Sie die Registerkarte "Automatische Zuweisung" aus, und geben Sie Folgendes in die Felder ein:

Automatische Zuweisung – Modus

Gibt an, wie die automatische Zuweisung durchgeführt wird. Verwenden Sie die Option "Configuration Item-basiert, um eine automatische Zuweisung auf der Basis des Attributwerts für "CI zuweisbar" durchzuführen.

Zuweisbares CI-Attribut

Gibt das für die Gruppenzuweisung zu verwendende Configuration Item-Attribut an. Sie können direkt einen Wert eingeben oder auf das Lupensymbol klicken, um nach einem Attribut zu suchen.

Klicken Sie auf "Speichern".

Die automatische Zuweisung wird aktiviert. CA SDM führt eine automatische Zuweisung auf der Basis von Configuration Items durch, und verwendet dabei das im Feld "Zuweisbares CI-Attribut" angegebene Attribut.

Kapitel 13: Verwalten Sie Ihre Datenbank

Dieses Kapitel enthält folgende Themen:

[Datenbankverwaltungsprogramme](#) (siehe Seite 539)

[Auswählen und Konfigurieren der Datenbank](#) (siehe Seite 539)

[Datenbanklader](#) (siehe Seite 540)

[Sichern von Datenbanken](#) (siehe Seite 543)

[Datenbankwiederherstellung](#) (siehe Seite 543)

[Datenbanktabellen-Ersatz](#) (siehe Seite 544)

[Daten-Dereferenzierung](#) (siehe Seite 546)

[Verbessern der Leistung mit Browser-Caching](#) (siehe Seite 561)

[Änderung der Konfigurationsdatei](#) (siehe Seite 563)

Datenbankverwaltungsprogramme

Sie können Dienstprogramme ausführen, um Ihre Datenbank zu verwalten, während CA SDM heruntergefahren ist. Wenn Sie Datenbankverwaltungsprogramme ausführen und als Datenbank nicht das CA SDM-Standard-Repository verwenden, müssen die Datenbank-Umgebungsvariablen eingestellt werden.

Hinweis: Informationen zu Einstellungsumgebungsvariable finden Sie in der Dokumentation für die verwendete Datenbank.

Auswählen und Konfigurieren der Datenbank

Sie können die Datenbank auswählen und für das Verwenden von CA SDM konfigurieren.

So wählen Sie eine Datenbank aus und konfigurieren sie:

1. Wählen Sie die Datenbank in der Dropdown-Liste "Datenbanktyp" aus, und klicken Sie auf "Weiter".

Die Konfigurationsseite für die ausgewählte Datenbank wird angezeigt.

2. Nachdem Sie die Datenbankinformationen eingegeben haben, klicken Sie auf "Weiter".

Die Konfiguration der Datenbank ist damit abgeschlossen.

Hinweis: Über die Schaltfläche "Hilfe" auf dieser Seite erhalten Sie Konfigurationsinformationen zu den Feldern für die ausgewählte Datenbank.

Die folgenden Schaltflächen erscheinen auf den Konfigurationsseiten.

Hilfe

Zum Aufrufen der Hilfe für die aktuelle Seite.

Abbrechen

Zum Abbrechen der bisher vorgenommenen Konfigurationseinstellungen.

Zurück

Hiermit gehen Sie zur vorherigen Seite zurück, ohne die vorgenommen Änderungen auf der aktuellen Seite zu speichern.

Weiter

Hiermit gehen Sie zur nächsten Seite, nachdem alle vorgenommen Änderungen auf der aktuellen Seite gespeichert wurden.

Datenbanklader

Das Datenbanklader-Dienstprogramm "pdm_userload" fügt CA SDM-Datenbankdatensätze hinzu, aktualisiert und löscht diese. Sie erstellen eine formatierte ASCII-Eingabedatei für das Dienstprogramm "pdm_userload" und wählen die zu ladenden Tabellen und die hinzuzufügenden optionalen Felder aus.

Wichtig! Das Dienstprogramm "pdm_userload" greift auf die CA SDM-Datenbank zu und interagiert nicht direkt mit Anwendersoftwareprozessen. Mit "pdm_userload" zur Datenbank hinzugefügte Bestandselemente aktualisieren Hilfe- oder Auswahllisten erst, nachdem die Anwendung beendet und neu gestartet wurde.

Das Dienstprogramm `pdm_userload` kann zwar bei aktiver Anwendung ausgeführt werden, jedoch wird die Systemleistung dadurch herabgesetzt. Zur Erzielung der besten Ergebnisse stellen Sie vor Ausführung von "pdm_userload" sicher, dass der Hintergrundserver aktiv ist, aber keine Anwender die Client-Schnittstelle verwenden.

Hinweis: Um Datensätze mit Feldern mit Querverweisen hinzuzufügen, verwenden Sie das Dienstprogramm "pdm_deref.-

Weitere Informationen:

[Daten-Dereferenzierung](#) (siehe Seite 546)

Erstellen und Nutzen einer Eingabedatei

Sie können eine Eingabedatei und das Hilfsprogramm "pdm_userload" dazu verwenden, Datenbanktabellen zu füllen.

Das Eingabedateiformat bestimmen Sie wie folgt:

- Umgeben Sie Feldwerte mit doppelten Anführungszeichen ("Wert") und trennen Sie Werte mit einem Komma und einer Leerstelle ("Wert1", "Wert2").
- Stellen Sie Anführungszeichen einen umgekehrten Schrägstrich (\) voraus, um sie in Textzeichenfolgen einzubetten. Um ein Feld für Datum und Uhrzeit auf das aktuelle Datum und die aktuelle Uhrzeit einzustellen, verwenden Sie @NOW@ als Eingabewert.
- Umgeben Sie jeden Datensatz mit geschweiften Klammern und mit Leerstellen getrennt, wie folgt:
 ({ record field values })
- Bei der korrekten Begrenzung können sich Eingabedatensätze über mehrere Zeilen in der Eingabedatei erstrecken, solange einzelne Felder in einer Zeile stehen. Bei einem mehrzeiligen Feld, wie zum Beispiel bei Kommentaren, können die Werte das Zeichen für eine neue Zeile (\n) enthalten, um eine neue Zeile zu erzwingen, wenn das Datenbankfeld angezeigt wird.
- Zeichen für eine explizite neue Zeile sind nur für spezielle Formatierungen erforderlich. Gewöhnlicher Text wird automatisch mit passenden Zeilenumbrüchen angezeigt (siehe folgendes Beispiel):
 "Record status is \"COMPLETE\""

Um eine Eingabedatei für das Dienstprogramm "pdm_userload" zu erstellen, gehen Sie wie folgt vor:

1. Bestimmen Sie die zu ladende Tabelle und die Felder, die in dieser Tabelle ausgefüllt werden sollen.
 Sie müssen das Schlüsselfeld „Name“ oder „Symbol“ für jeden Datensatz, den Sie laden, ausfüllen.
2. Erstellen Sie eine Kopie der entsprechenden Datei "*Dateiname.dat*" für die zu ladende Tabelle.
3. Bearbeiten Sie die neu erstellte Kopie von "*Dateiname.dat*" wie folgt:
 - a. Fügen Sie einen Eintrag für jeden zu ladenden Datensatz hinzu.
 - b. Löschen Sie unter der Zeile TABLE (siehe folgendes Beispiel) die Felder, die Sie nicht ausfüllen wollen.

```
TABLE table_name
fieldname1 fieldname4 . . . fieldnameN
```

4. Speichern Sie die Datei, und beenden Sie den Editor.
5. Führen Sie das Hilfsprogramm "pdm_userload" aus und geben Sie die Datei an, wie im folgenden Beispiel gezeigt. In diesem Beispiel ist der Name der Eingabedatei myData.dat:

```
pdm_userload -f myData.dat
```

Die Datenbanktabelle wird gefüllt.

Weitere Informationen:

[pdm_userload – Hinzufügen, Aktualisieren und Löschen von Datenbank-Datensätzen](#)
(siehe Seite 1199)

Entfernen und Wiederherstellen von Bedingungen

Einige der MDB-Tabellen, die mit ca_ beginnen (wie zum Beispiel ca_contact_), enthalten referenzielle Bedingungen, die das Massensladen von Daten mit "pdm_load", "pdm_userload" und "pdm_restore" beeinträchtigen können. Wenn ein Massensladen dieser Tabellen erforderlich ist, müssen Sie die referenziellen Bedingungen vor dem Massensladen der Daten gegebenenfalls entfernen.

Zum Entfernen und Wiederherstellen von Bedingungen werden zwei SQL-Skripte für jeden DBMS-Typ bereitgestellt. Vor dem Massensladen von Daten, die sich auf „ca_*“-Tabellen auswirken, führen Sie die Skriptversion zum Entfernen aus. Wenn der Datenladevorgang abgeschlossen ist, führen Sie die Skriptversion zum Hinzufügen aus.

Skripts für SQL-Server sind im Verzeichnis "*installation-directory*\samples\views\SQLServer" abgelegt. Führen Sie das folgende Skript aus, um Bedingungen zu entfernen:

```
osql -E -e < SQLDropConstraints.sql
```

Führen Sie das folgende Skript aus, um Bedingungen wieder hinzuzufügen:

```
osql -E -e < SQLAddConstraints.sql
```

Skripts für Oracle sind im Verzeichnis "*installation-directory*\samples\views\Oracle" abgelegt.

Führen Sie das folgende Skript aus, um Bedingungen zu entfernen:

```
sqlplus mdbadmin/ <password> < OracleDropConstraints.sql
```

Führen Sie das folgende Skript aus, um Bedingungen wieder hinzuzufügen:

```
sqlplus mdbadmin/ <password> < OracleAddConstraints.sql
```

Sichern von Datenbanken

Möchten Sie die Inhalte einzelner oder mehrerer Datenbank-Tabellen oder den Inhalt der gesamten CA SDM-Datenbank sichern, können Sie das Dienstprogramm "pdm_backup" verwenden. Die Ausgabe des Sicherungsdienstprogramms ist eine ASCII-Datei, die vom Dienstprogramm "pdm_restore" verwendet werden kann.

Als Teil seiner Verarbeitung fährt pdm_backup zuerst die Daemons (UNIX) oder die Dienste (Windows) herunter.

Weitere Informationen:

[pdm_backup – Exportieren der Datenbank in eine ASCII-Datei](#) (siehe Seite 1155)

Datenbankwiederherstellung

Das Dienstprogramm zur Wiederherstellung der Datenbank, pdm_restore, lädt eine von pdm_backup erstellte Ausgabedatei in die CA SDM-Datenbank. Das Dienstprogramm "pdm_restore" schließt zunächst die Daemons (UNIX) oder Services (Windows). Dann werden alle vorhandenen Datenbank-Datensätze wiederhergestellt, bereinigt und ersetzt. Als Eingabe für "pdm_restore" verwenden Sie die von "pdm_backup" erstellte formatierte ASCII-Datei.

Sie können die Dienstprogramme pdm_restore und pdm_userload auch verwenden, um im Fall einer schwerwiegenden Beschädigung der Datenbank Zugriff auf die CA SDM-Anwendung zu erhalten. Wenn die Datenbank so beschädigt ist, dass Sie keinen Zugriff mehr auf die Anwendung erhalten und alle anderen Maßnahmen versagt haben, führen Sie die Konfiguration erneut durch und reinitialisieren Sie die Datenbank, um Ihre Datenbank wiederherzustellen und Referenzdaten und Systemtabellen zu füllen.

Dieses Verfahren initialisiert die Datenbank in derselben Weise wie während der ursprünglichen Installation. Sie können anschließend auf CA SDM zugreifen. Mit dem Dienstprogramm "pdm_restore" können Sie die zuletzt gesicherte Kopie Ihrer Datenbank wiederherstellen.

Weitere Informationen:

[pdm_restore – Wiederherstellen einer Datenbank](#) (siehe Seite 1189)

Datenbanktabellen-Ersatz

Das Dienstprogramm `pdm_replace` ist eine schnelle und einfache Methode, um den gesamten Inhalt einer CA SDM-Datenbanktabelle durch neue Informationen zu ersetzen. Dieses Dienstprogramm kann bei umfassenden Änderungen von Suchfeld-Tabellen nützlich sein.

Hinweis: "`pdm_replace`" verwendet das gleiche Eingabedateiformat wie "`pdm_userload`". Sie können mithilfe von `pdm_extract` eine Eingabedatei für `pdm_replace` erstellen, jedoch nicht die Ausgabe von `pdm_backup` als Eingabe für `pdm_replace` verwenden.

Weitere Informationen:

[pdm_replace – Ersetzen einer Datenbanktabelle](#) (siehe Seite 1186)

[Erstellen und Nutzen einer Eingabedatei](#) (siehe Seite 541)

Extrahieren von Daten

Das Dienstprogramm "`pdm_extract`" extrahiert Daten aus der CA SDM-Datenbank und erstellt die Ausgabe in verschiedenen Formaten. Sie können diese Daten weiterverarbeiten oder sie in andere Softwareanwendungen, wie zum Beispiel Tabellenkalkulationen oder Datenbanken, eingeben.

Mit dem Dienstprogramm "`pdm_extract`" können Sie das Folgendes tun:

- Erstellen eines Auszugs der gesamten CA SDM-Datenbank
- Erstellen eines Auszugs von einer oder mehreren Datenbanktabellen
- Extrahieren bestimmter Informationen aus der Datenbank und Erstellen einer Ausgabe in einem der folgenden drei Formate:
 - mit "`pdm_userload`" kompatible Ausgabe
 - CSV-Ausgabe-(Comma Separated Value)
 - Informelle Ausgabe-im Berichtsstil

Weitere Informationen:

[pdm_extract – Extrahieren von Daten aus der Datenbank](#) (siehe Seite 1165)

Verwenden Datenextraktors unter UNIX

Bevor Sie den CA SDM-Datenextraktor unter UNIX verwenden, müssen Sie folgende Schritte ausführen:

1. Geben Sie für die Umgebungsvariable \$NX_ROOT den vollständigen Pfadnamen des CA SDM-Installationsverzeichnisses an, das Sie während der Installation definiert haben.
2. Fügen Sie "\$NX_ROOT/bin/</cs>" an die Umgebungsvariable PATH an.
3. Stellen Sie „umask“ auf „000“ ein.

Auswählen von Daten für die Extraktion

Um die Daten für die Extraktion auszuwählen, verwendet der Datenextraktor eine Untermenge von SQL-Funktionen mit folgenden Regeln:

- Die folgenden SQL-Funktionen werden in der Untermenge explizit unterstützt:
 - IS NULL, IS NOT NULL, LIKE
 - SELECT-Anweisungen und WHERE-Klauseln
- Die folgenden SQL-Funktionen werden in der Untermenge nicht unterstützt:
 - Verbindungen
 - Eingebettete Tabulatoren und Zeilenvorschubzeichen
 - Klauseln, die keine SELECT-, FROM- oder WHERE-Klauseln sind
 - Sternchen (*) in SELECT-Anweisungen
 - verschachtelte SELECT-Anweisungen
 - Aggregatfunktionen
- Alle reservierten Wörter in SQL müssen in Großbuchstaben angegeben sein.
- Jedes Token in einer WHERE-Klausel muss zwischen Leerzeichen stehen.
- Alle Datums- und Zeitangaben müssen eines der folgenden drei Formate haben:
 - verstrichene Sekunden ab 12:00:00 Uhr. 1/1/1970 Greenwich-Zeit (GMT) :
start_date< or >174182431500
 - SQL DATE-Format:
start_date< or >DATE '2001-11-28'
 - SQL TIMESTAMP-Format:
start_date< or >TIMESTAMP '2001-07-04 15:45:00'

Note: Das TIMESTAMP-Format verwendet GMT. Sie können Zeitzonen einstellen, indem Sie die angemessene Anzahl von Stunden addieren bzw. subtrahieren. Beispiel: 2001-03-23 14:00:00+02:00 oder 2001-06-06 04:45:00-09:00.

Daten-Dereferenzierung

Das Dienstprogramm "pdm_deref" ist ein Dereferenzierungs-Tool, das Daten aus verschiedenen Quellen in ein Format konvertiert, das in die CA SDM-Datenbank geladen werden kann. Die Dereferenzierung extrahiert interne IDs für Felder mit Querverweisen-. Außerdem kann das Dienstprogramm zur Berechnung von Werten für Ausfallzeiten und SLA-Ausfallzeiten verwendet werden.

Das Dienstprogramm "pdm_deref" konvertiert Daten in eines der folgenden Formate:

- mit pdm_userload kompatible Ausgabe, eignet sich für den Import in die CA SDM-Datenbank
- CSV-Ausgabe-(Comma Separated Value)
- Informelle Ausgabe-im Berichtsstil

Weitere Informationen:

[pdm_deref – Dereferenzieren von ASCII-Daten](#) (siehe Seite 1159)

Beispiel für das Ausführen von "pdm_deref"

Das folgende Beispiel zeigt, wie man das Hilfsprogramm "pdm_deref" in einem CA SDM-Ticket-Nachverfolgungssystem benutzt.

Angenommen, ein vorhandenes Ticketverfolgungssystem, das Sie für eine Tabellenkalkulation implementiert haben, hat die Spalten „Fehlerbeschreibung“, „Techniker Vor- und Nachname“ und „Eingangsdatum“. Diese Spalten entsprechen den Feldern "Beschreibung", "Zuständiger" und "open_date" in der CA SDM-Tabelle "Change_Request". Das Feld „Fehlerbeschreibung“ enthält das gleiche Schlüsselwort wie das Feld „Beschreibung“. Das Feld "Zuständiger" ist jedoch ein numerisches Feld, während das Feld "Techniker" in der Tabellenkalkulation das Format "Nachname, Vorname" hat.

Anwendung von "pdm_deref"

1. Laden Sie die Namen der Techniker in die Tabelle "Kontakte".
2. Bereiten Sie eine "pdm_deref"-Eingabedatei mit der bestehenden Information vor.
3. Erstellen Sie eine Spezifikationsdatei, um die neuen Kontaktnamen auf die Werte von Zuständigen zu übertragen.
4. Bereiten Sie eine "pdm_userload"-Eingabedatei vor, um die Tabelle "Change_Request" zu aktualisieren.

Dieses Verfahren wird in den folgenden Schritten ausführlicher beschrieben:

1. Bereiten Sie eine "pdm_userload</cs>-Eingabedatei, "location.dat</cs>, für die Tabelle „Location“ wie folgt vor:

```
TABLE ca.location
location_name address_2 address_2
{"Boulder NCC - NQ", "716 Main
Street", "Boulder, CO 84302"}
{"Colorado Springs NCC", "2765 Spring Street",
"Colorado Springs, CO 84303"}
{"Denver NCC", "3765 Stoneridge Way", "Denver,
CO 80254"}
```

2. Laden Sie die Daten wie folgt:

```
pdm_load -f location.dat
```

3. Bereiten Sie eine Eingabedatei, "contact.dat</cs>, mit den ursprünglichen Informationen wie folgt vor:

```
TABLE ca.contact
last_name first_name middle_name location pri_phone_number
{"Harrison", "Frank", "Harold", "NCC - HQ", "303-555-2333"}
{"Hertzog", "William", "I.", "Colorado Springs NCC", "303-966-1987"}
{"Lyman", "Jeanie", "L.", "Denver NCC", "303-966-5301"}
```

4. Bereiten Sie eine Spezifikationsdatei, "contact.spec</cs>, für das Dereferenzierungstool wie folgt vor:

```
Deref
{
input = c_location
output = location_uuid
rule = "SELECT id FROM ca.location WHERE location_name=?"
}
```

Wichtig! Fügen Sie kein Leerzeichen vor dem SELECT-Schlüsselwort ein. „Deref“ verwendet die Vor- und Nachnamen der neuen Kontakte, um die entsprechenden numerischen ID-Felder für den Import in die Tabelle „Change_Request“ abzurufen. Zusätzlich entsprechen die durch Fragezeichen (?) dargestellten „Hooks“ den angegebenen Eingabefeldern. Sie müssen die gleiche Anzahl von Hooks wie Eingabefelder haben, und sie müssen in der gleichen Reihenfolge vorhanden sein.

5. Führen Sie "pdm_deref" wie folgt aus:

```
pdm_deref -s contact.spec < contact.dat > contact.out
```

Die Ausgabedatei, "contact.out", hat folgendes Aussehen:

```
TABLE ca.contact
last_name first_name middle_name location.uuid pri_phone_number
{"Harrison", "Frank", "Harold", "69499D5A2424884887E62EC9823F5E47",
"303-555-2333"}
{"Hertzog", "William", "I.", "86873FA40BA4234A8CF7A418D7C8B2DB",
"303-966-1987"}
{"Hertzog", "William", "I.", "86873FA40BA4234A8CF7A418D7C8B2DB",
"303-966-1987"}
```

6. Importieren Sie die Datei contact.out wie folgt in die CA SDM-Datenbank:

```
pdm_load -i -f contact.out
```

Hinweis: Die Funktion "-i" können Sie über den Befehl "pdm_load" nutzen.

7. (Nur für UNIX, optional): Schreiben Sie das Skript "Convert_Ticket", wie im Folgenden beschrieben:

```
#!/bin/sh
pdm_load -i $1
cat $2 | pdm_deref -s $3 | pdm_load -i
```

Sie können dieses Skript wie folgt ausführen:

```
Convert Ticket location.dat contact.dat contact.spec
```

In diesem Beispiel wird "pdm_load" mit dem Flag "-i" verwendet, um den Prozess zu beschleunigen. Wenn Sie diese Aktualisierungen regelmäßig durchführen, können Sie das Flag "-i" weglassen, damit "pdm_load" prüft, ob doppelte Datensätze vorhanden sind.

Es folgt ein weiteres Beispiel für eine Spezifikationsdatei für das Dereferenzierungstool:

```
Deref
{
    input = first_name, last_name, middle_name
    output = assignee
    rule = " SELECT id from ca.contact \
        WHERE first_name=? \
        AND last_name=? \
        AND middle_name=? "
}
```


Diese Regel konvertiert die drei Felder „first_name“, „last_name“ und „middle_name“ in die entsprechende Kontakt-UUID. Wenn alle drei Eingabefelder nicht vorhanden sind, wird die Regel nicht angewandt. Wenn keine Übereinstimmung vorhanden ist, wird eine Fehlermeldung ausgegeben, und die Verarbeitung wird fortgesetzt. Bei mehreren Übereinstimmungen wird der erste Wert verwendet. Eine Fehlermeldung wird ausgegeben, und die Verarbeitung wird fortgesetzt.

Verwenden des dbadmin-Modus

Der dbadmin-Modus ist ein Dienstprogramm, das die Datenmanipulationsschicht des CA SDM-Systems startet, ohne die Objektschicht zu starten, die die Möglichkeit bietet, die gesamte Datenbank zu sperren, um eine systemnahe Datenwartung durchzuführen, ohne die Datenintegrität zu gefährden.

Sie können z. B. "pdm_extract", "pdm_load", "pdm_deref" und "pdm_replace" verwenden, um Batchdatenaktualisierungen auf dem System durchzuführen. Mit "dbadmin</cs>" legt der Administrator eine Datenbanksperre für das gesamte System fest. Die Dienstprogramme zur Sicherung ("pdm_backup</cs>") und Wiederherstellung ("pdm_restore</cs>") versetzen das System jeweils automatisch in den dbadmin-Modus, um eine konsistente Sicherung und Wiederherstellung zu garantieren.

Der dbadmin-Modus ist auch nützlich, wenn Sie das System ohne Starten der Objektschicht erst nach der Datenänderung anpassen möchten. Wenn zum Beispiel auf einem bestehenden System ein Attribut in Majic auf „erforderlich“ eingestellt wird, kann dies den Animator verwirren, wenn er ein Objekt aktualisieren muss, für das das erforderliche Attribut null ist. Sie können System in den dbadmin-Modus versetzen und die Objekte mit "pdm_load" aktualisieren und anschließend das System wie gewöhnlich starten.

So setzen Sie das System auf den Modus "dbadmin":

1. Stoppen Sie CA SDM entweder über den Windows-Dienstmanager oder durch Ausführen von pdm_halt in der Befehlszeile.

Hinweis: Bevor Sie das System herunterfahren, empfiehlt es sich, allen Benutzern eine Ankündigung zu schicken, und sich zu vergewissern, dass alle Benutzer abgemeldet sind.

2. Geben Sie in der Befehlszeile den folgenden Befehl ein (verwenden Sie Groß- und Kleinschreibung wie dargestellt):

```
pdm_d_mgr -s DBADMIN
```

Hinweis: Es wird keine Meldung zurückgegeben, aber es entsteht eine Pause, bevor die Eingabeaufforderung wieder angezeigt wird. Wenn keine Pause entsteht, prüfen Sie die Schreibweise, um sicherzustellen, dass Sie den Befehl korrekt eingegeben haben.

- Führen Sie "pdm_status" aus, um zu prüfen, ob sich das System im dbadmin-Modus befindet.

Hinweis: Wenn sich das System im dbadmin-Modus befindet, gibt es den folgenden Status zurück, um anzuzeigen, dass das Arbeiten auf dem System sicher ist:

```
C:\>pdm_status
```

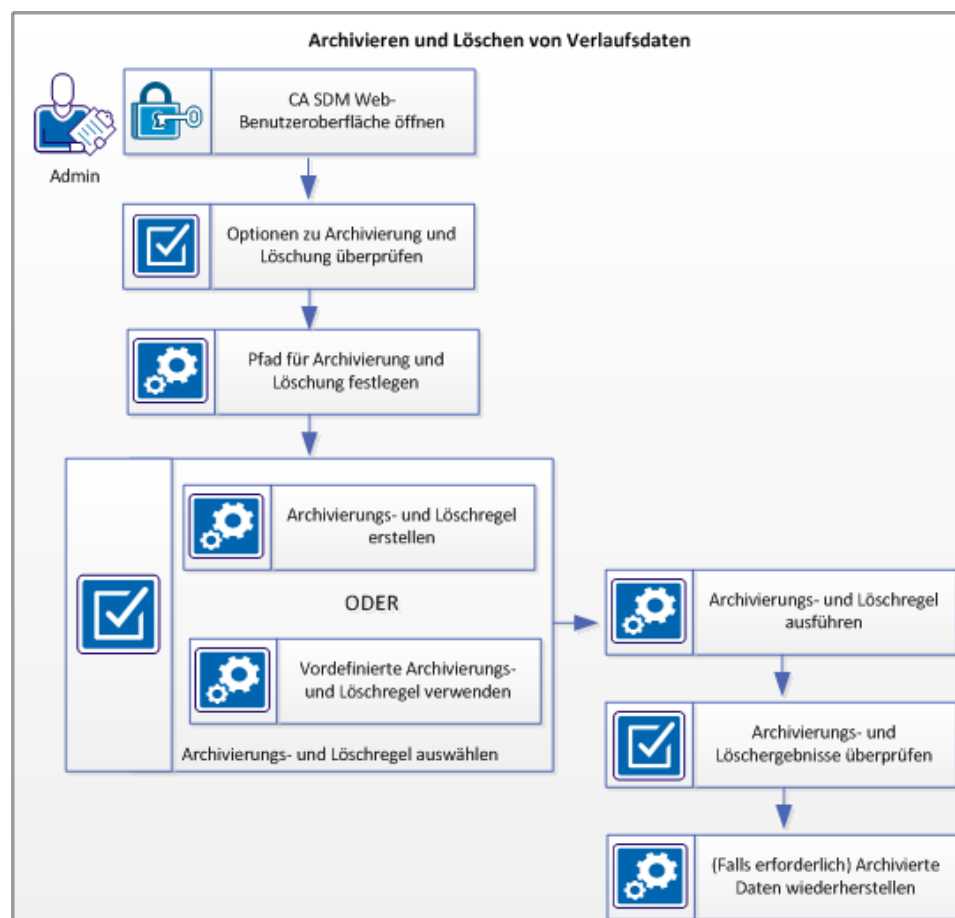
Die Daemons werden nicht ausgeführt.

- Wenn die Bearbeitung abgeschlossen ist, führen Sie "pdm_halt" aus, um den dbadmin-Modus zu beenden.
- Starten Sie das System in gewohnter Weise neu.

So archivieren und bereinigen Sie Verlaufsdaten

Entfernen Sie regelmäßig die Verlaufsdatensätze aus dem System, um die Datenbank in einer überschaubaren Größe zu halten und um so eine optimale Leistung zu erzielen. Sie erstellen Regeln oder deaktivieren die vordefinierten Regeln, um die Verlaufsdatensätze zu archivieren und sie aus der Datenbank zu löschen.

Folgendes Diagramm zeigt, wie Verlaufsdaten archiviert und gelöscht werden:



Gehen Sie wie folgt vor:

1. [Öffnen Sie die CA SDM-Web-Benutzeroberfläche](#) (siehe Seite 202).
2. [Überprüfen Sie die Archivierungs- und Löschungsoptionen](#) (siehe Seite 551)
3. [Definieren Sie den Archivierungs- und Löschungspfad](#) (siehe Seite 552).
4. [Wählen Sie die Archivierungs- und Löschregel aus](#) (siehe Seite 555).
 - [Erstellen Sie eine Archivierungs- und Löschregel](#) (siehe Seite 555).
 - [Verwenden Sie eine vordefinierte Archivierungs- und Löschregel](#) (siehe Seite 558).
5. Führen Sie eine Archivierungs- und Löschregel aus.
6. [Überprüfen Sie die Ergebnisse der Archivierung und Löschung](#) (siehe Seite 559).
7. (Im Bedarfsfall) [Stellen Sie die archivierten Daten wieder herstellen](#) (siehe Seite 560).

Öffnen der CA SDM-Web-Benutzeroberfläche

Melden Sie sich in der Web-Benutzeroberfläche aus folgenden Servern an, abhängig von Ihrer CA SDM-Konfiguration:

- Konventionell: Primärserver oder Sekundärserver
- Erweiterte Verfügbarkeit: Anwendungsserver oder Hintergrundserver

Überprüfen Sie die Archivierungs- und Löschungsoptionen

Bevor Sie die Archivierungs- und Löschungsregel einrichten, überprüfen Sie die Archivierungs- und Löschungsoptionen, die Sie abhängig von Ihren Organisationsanforderungen möglicherweise installieren oder deinstallieren müssen. Die Option "default_schedule" gibt z. B. den Standardablaufplan (Schichteintrag) fest, der von der Archivierungs- und Löschregel verwendet wird. Wird der Optionswert auf einen ungültigen Schichteintrag gesetzt oder eine leere Zeichenkette eingegeben, führt die Regel die Regel mit dem Ablaufplanwert nicht aus. Mit dem Feld "Optionswert" wird die Variable "NX_DEFAULT_SCHEDULE" festgelegt, die sich in der Datei "NX.env" befindet.

Wählen Sie auf der Registerkarte "Administration" die Option "Optionsmanager", "Archivierung und Löschung" aus. Installieren oder deinstallieren Sie die Option, die Sie benötigen.

Definieren des Archivierungs- und Löschungspfads

Sie können den Speicherort angeben, wo Sie die archivierten Daten speichern möchten. Dieser Pfad kann das Stammverzeichnis von einem Remote-Server oder von einem UNC-Pfad sein. Abhängig von Ihrer CA SDM-Konfiguration müssen folgende Server unter Windows ausgeführt werden, um auf den UNC-Pfad zuzugreifen:

- Konventionell: Primärserver
- Erweiterte Verfügbarkeit: Hintergrundserver

Gehen Sie wie folgt vor:

1. Melden Sie sich von folgenden CA SDM-Servern aus in der Web-Benutzeroberfläche an, abhängig von Ihrer CA SDM-Konfiguration:
 - Konventionell: Primärserver oder Sekundärserver
 - Erweiterte Verfügbarkeit: Anwendungsserver oder Hintergrundserver
2. Wenn Sie Anhänge archivieren und löschen möchten, führen Sie folgende Schritte durch:
 - a. Wählen Sie auf der Registerkarte "Administration" die Optionen "Anhangbibliothek", "Repositorys" aus.
Die Seite "Repositorys" wird angezeigt.
 - b. Klicken Sie mit der rechten Maustaste auf ein Repository (beispielsweise "Service Desk"), und klicken Sie auf "Bearbeiten".
Die Seite "Repository-Details" wird geöffnet.
 - c. Bearbeiten Sie die folgenden Felder:

Archivtyp

Gibt die Archivierungs- und Löschungsaktion an, die am Repository-Inhalt durchgeführt werden soll. Folgende Werte sind gültig:

Keine: Es wird kein Archivierungs- und Löschvorgang durchgeführt.

Archivierung und Löschung: Die Verlaufsdatensätze werden in die Datei geschrieben, die im Archivfeld angegebenen und von der Datenbank bereinigt wird.

Nur Löschung: Die Verlaufsdatensätze werden von der Datenbank bereinigt, jedoch werden sie nicht in die Archivdatei geschrieben.

Archivpfad

Gibt den Verzeichnispfad oder den UNC-Pfad an, zu dem Dateien im Repository während des Archivierungsprozesses verschoben werden.

UNC-Daten

Gibt die Anmeldeinformationen für den Zugriff auf den UNC-Pfad an. Klicken Sie auf UNC-Daten, um die Seite Anmeldeinformationen - Suche zu öffnen.

- Wenn Sie die Anmeldeinformationen bereits erstellt haben, um auf den angegebenen UNC-Pfad zuzugreifen, führen Sie eine Suche mithilfe der Felder durch, und wählen Sie die Anmeldeinformationen aus.
- Wenn Sie die Anmeldeinformationen erstellen möchten, klicken Sie auf "Neu erstellen". Weitere Informationen über das Erstellen von Anmeldeinformationen finden Sie unter dem Thema "[Erstellen von UNC-Daten](#)" (siehe Seite 486)".

d. Klicken Sie auf "Speichern".

3. Wenn Sie Daten, die keine Anhänge sind, archivieren und löschen möchten, führen Sie folgende Schritte durch:

- a. Navigieren Sie auf der Registerkarte "Administration" zu "Archivierung und Löschung" und dann zu "Einstellungen für Archivierung und Löschung".
- b. Geben Sie den Pfad ein, wo Sie die archivierten und gelöschten Daten als Archivierungs- und Löschregelpfad speichern möchten.
- c. Wenn Sie einen UNC-Pfad verwenden, um die archivierten Daten zu speichern, klicken Sie auf UNC-Daten.

Die Seite Anmeldeinformationen - Suche wird geöffnet.

- Wenn Sie die Anmeldeinformationen bereits erstellt haben, um auf den angegebenen UNC-Pfad zuzugreifen, führen Sie eine Suche mithilfe der Felder durch, und wählen Sie die UNC-Daten aus.
- Wenn Sie die Anmeldeinformationen erstellen möchten, klicken Sie auf "Neu erstellen". Weitere Informationen über das Erstellen von Anmeldeinformationen finden Sie unter dem Thema "[Erstellen von UNC-Daten](#)" (siehe Seite 486)".

d. Klicken Sie auf "Speichern".

Der Archivierungs- und Löschpfad ist definiert.

Erstellen von UNC-Daten

Sie erstellen die UNC-Daten, um es Anwendern zu erlauben, auf freigegebene Ressourcen von den CA SDM-Servern zuzugreifen, indem der UNC-Pfad verwendet wird.

Wichtig! Die UNC-Komponente funktioniert nicht, wenn der CA SDM-Server in der Domäne ist und der freigegebene Speicherort in der WORKGROUP ist. Es funktioniert auch nicht, wenn das Administratorkennwort für den CA SDM-Server und den freigegebenen Speicherort unterschiedlich ist.

Gehen Sie wie folgt vor:

1. Klicken Sie auf die UNC-Daten auf der Seite "Allgemeine Einstellungen", oder wählen Sie auf der Registerkarte "Administration" die Optionen "Sicherheit und Rollenmanagement", "UNC-Daten" aus.

Die Seite Anmeldeinformationen - Liste wird geöffnet.

2. Klicken Sie auf "Neu erstellen".

Die Seite "Neue Anmeldeinformationen erstellen" wird geöffnet.

3. Füllen Sie die folgenden Felder nach Wunsch aus:

Symbol

Gibt die eindeutige Kennung an, um die Anmeldeinformationen während einer Suche einfacher zu identifizieren.

Anwender-ID

Gibt den Anwendernamen für den Zugriff auf den UNC-Pfad an. Der Anwender kann ein lokaler Anwender oder ein Windows-Domänenanwender sein, der Zugriff auf den Service Desk-Server hat.

Kennwort

Gibt das Kennwort für den Zugriff auf den UNC-Pfad an.

Aktiv

Gibt an, ob die UNC-Daten aktiv oder inaktiv sind. Die inaktiven Anmeldeinformationen können nicht verwendet werden.

4. Klicken Sie auf "Speichern".

Die UNC-Daten werden erstellt.

Auswählen der Archivierungs- und Löschregel

Sie müssen die entsprechende Archivierungs- und Löschregel auswählen. Berücksichtigen Sie folgende Möglichkeiten:

- [Erstellen Sie eine Archivierungs- und Löschregel](#) (siehe Seite 555). Zum Beispiel erstellen Sie eine Archivierungs- und Löschregel für Knowledge Management-Foren.
- [Verwenden Sie eine vordefinierte Archivierungs- und Löschregel](#) (siehe Seite 558). Zum Beispiel verwenden Sie die vordefinierten Regeln für das Archivieren und Löschen von KPI-Daten.

Erstellen einer Archivierungs- und Löschungsregel

Bevor Sie einen Archivierungs- oder Löschvorgang ausführen können, erstellen Sie eine Regel. Die Regel legt fest, was Sie archivieren möchten und wann der Vorgang durchgeführt werden soll.

Beispiel: Sie erstellen eine Archivierungs- und Löschregel, um gelöschte Foren aus der Datenbank zu entfernen.

Gehen Sie wie folgt vor:

1. Navigieren Sie auf der Registerkarte "Administration" zu "Archivierung und Löschung" und dann zu "Archivierungs- und Löschregeln".
Die Seite "Archivierungs- und Löschungsregel - Liste" wird angezeigt.
2. Klicken Sie auf "Neu erstellen".
Die Seite "Neue Archivierungs- und Löschungsregel erstellen" wird geöffnet.
3. Stellen Sie entsprechend die [Felder für die Archivierungs- und Löschregel](#) (siehe Seite 557) fertig.
 - Wählen Sie "Knowledge-Dokument" als Name des Konfigurationsobjekts aus.
 - Fügen Sie "KS_TYPE=20" als "Zusätzliche Abfrage" hinzu.
4. Klicken Sie auf "Speichern".
Die neue Regel wird auf der Seite "Archivierungs- und Löschungsregel - Liste" angezeigt.

Beispiel: Sie erstellen eine optionale Konfigurationsregel innerhalb der Dateien "arcpur_cfg.xml" und "itil_arcpur_cfg.xml", um den Knoten "KPI_Ticket_Data" zu archivieren und zu löschen.

Gehen Sie wie folgt vor:

1. Melden Sie sich abhängig von Ihrer CA SDM-Konfiguration bei folgendem Server an:
 - Konventionell: Primärserver
 - Erweiterte Verfügbarkeit: Hintergrundserver

2. Folgende Dateien befinden sich im Verzeichnis "\$NX_ROOT/site/cfg/":
 - arcpur_cfg.xml
 - itil_arcpur_cfg.xml
3. Bearbeiten Sie die Dateien, um "end_time" (last_mod_dt) im Knoten "KPI_Ticket_Data" zu definieren. Es gibt die Kriterien für die Auswahl der Datensätze an, die archiviert und gelöscht werden sollen.
4. Verknüpfen Sie die Datensätze in der Tabelle "KPI_Ticket_Data" mit den Datensätzen in der Ticket-Tabelle (z. B. "cr", "chg" oder "iss"). So stellen Sie sicher, dass alle ticketrelevanten Datensätze in der Tabelle "KPI_Ticket_Data" archiviert und gelöscht werden.
5. Der Knoten "KPI_Ticket_Data" hat keinen SREL-Bezug zu Ticket-Knoten und basiert auf den Feldern "obj_name" und "obj_id", um eine Verknüpfung zu einem Ticket herzustellen. Der Wert "obj_name" kann "cr", "chg" oder "iss" sein und der Wert "obj_id" entspricht der Ticket-ID. Definieren Sie ein "main_obj" (Hauptobjekt) für jedes Ticket-Objekt.

Nachfolgend ist ein Beispiel für die Definition von "main_object" für das Ticket-Objekt (cr) dargestellt:

```
<!-- KPI-Ticket-Daten -->

<main_obj>

<Name>KPI-Ticket-Daten</name>

<Internal_name>KPI-Ticket-Daten</internal_name>

<factory>ktd</factory>

<default_query>obj_name='cr'</default_query>

<date_field>end_time</date_field>

<ref_by value="obj_id">cr.id</ref_by>

</main_obj>
```

Hinweis: Mit dieser Konfigurationsregel kann man nur Datensätze für "cr" auswählen. Das Etikett "ref_by" kann den Wert von "obj_id" in KPI-Ticket-Daten dem Wert von "id" in "cr" anpassen. Wenn eine Übereinstimmung festgestellt wird, bedeutet dies, dass ein KPI-Ticket-Datensatz durch einen cr-Datensatz referenziert ist, weshalb der KPI-Ticket-Datensatz nicht archiviert und gelöscht wird.

6. Nachdem Sie die Konfigurationsregeln für alle Ticket-Objekte hinzugefügt haben, führen Sie abhängig von Ihrer CA SDM-Konfiguration eine der folgenden Aktionen durch:
- [Starten Sie die CA SDM-Server für die konventionelle Konfiguration neu](#) (siehe Seite 52).
 - [Starten Sie die CA SDM-Server für Konfiguration für erweiterte Verfügbarkeit neu](#) (siehe Seite 52).

Diese Konfigurationsregeln werden zu auswählbaren Konfigurationsobjektnamen im Formular "Archivierungs- und Löschrregeln - Detail".

Archivierungs- und Löschrregeln - Felder

Sie können folgende Felder verwenden, um Regeldefinitionen zu definieren oder zu bearbeiten.

Regelname

Gibt die eindeutige Kennung der Regel an.

Status

Zeigt an, ob diese Regel aktiv ist. Die inaktive Regel wird einmal ausgeführt, auch wenn sie für einen wiederkehrenden Prozess geplant ist.

Ablauf

Gibt die Schicht an, für die die Regel gelten sollte.

Rekurrenzintervall

Gibt an, wie oft diese Regel ausgeführt wird.

Archiv-Dateiname

Gibt den Namen der Datei an, in der Sie die Verlaufsdatensätze speichern möchten. Geben Sie den Dateinamen ein, den Sie angegeben haben, während Sie den Archivierungs- und Löschungspfad definiert haben. Weitere Informationen finden Sie unter dem Thema "[Definieren des Archivierungs- und Löschungspfads](#) (siehe Seite 552)".

Vorgangstyp

Benennt einen der folgenden Vorgangstypen, den die Regel ausführen muss:

Archive/Purge

Archiviert die Verlaufsdatensätze in eine Datei, und löscht die archivierten Datensätze aus der Datenbank.

Nur Löschung

Verlaufsdatensätze werden aus der Datenbank gelöscht, jedoch nicht in die Archivdatei geschrieben.

Nur Archivierung (Testausführung)

Schreibt Verlaufsdatensätze in die Archivdatei, ohne sie aus der Datenbank zu löschen. Mit dieser Option können Sie eine neu erstellte oder bearbeitete Archivierungs- und Lösungsregel testen.

Konfig. Objektname

Gibt den Namen des Datenbankobjekts an, das von dieser Regel archiviert und gelöscht werden kann. Das Feld "Objektname" wird entsprechend Ihrer Auswahl im Feld "Name des Konfigurationsobjekts" automatisch aufgefüllt.

Inaktive Tage

Gibt die Zahl der Tage an, über die ein Datensatz inaktiv ist, bevor er archiviert und aus der Datenbank gelöscht werden kann.

Zusätzliche Abfrage

Archiviert und löscht zusätzlich zu den bestehenden inaktiven Datensätzen bestimmte inaktive Datensätze. Verwenden Sie dieses Feld, wenn Sie verschiedene Regeln für Archivierung und Löschung der Untermengen abgelaufener Datensätze für dasselbe Objekt erstellen möchten. Verwenden Sie die gleiche Syntax wie für gespeicherte Abfragen.

Die folgende Abfrage archiviert und bereinigt nur zugewiesene inaktive Request-Datensätze mit einer Priorität von 1:

```
priority = 1 AND (assignee IS NOT NULL OR group IS NOT NULL) and active = 0
```

Das folgende Abfrageformat archiviert und bereinigt auf Zeitspannen basierte Datensätze:

```
close_date < EndAtTime('\LAST_YEAR\')
```

Verwenden einer vordefinierten Archivierungs- und Lösungsregel

Sie können die vordefinierten Regeln in CA SDM verwenden, um Verlaufsdaten zu archivieren und zu löschen. Diese vordefinierten Regeln werden standardmäßig auf "Inaktiv" festgelegt. Setzen Sie sie auf "Aktiv", um die Regel zu verwenden.

Beispiel: Verwenden Sie die vordefinierte Regel, um die KPI-Daten zu archivieren und zu löschen.

Gehen Sie wie folgt vor:

1. Navigieren Sie auf der Registerkarte "Administration" zu "Archivierung und Löschung" und dann zu "Archivierungs- und Lösungsregeln".
2. Suchen Sie nach einer der folgenden vordefinierten Regeln für KPI-Daten:
 - KPI-Ticket-Daten
 - KPI-Daten (System)

- KPI-Daten (Gespeicherte Abfrage)
 - KPI-Daten (SQL)
3. Wählen Sie die Regel aus dem Suchergebnis aus.
 4. Klicken Sie auf "Bearbeiten", um das Feld "[Archivierungs- und Löschregel](#)" (siehe Seite 557)" zu ändern.

Wichtig! Stellen Sie sicher, dass Sie die Option "Aktiv" aus dem Feld "Status" ausgewählt haben.

5. Klicken Sie auf "Speichern".

Die vordefinierte Regel ist für die Verwendung bereit.

Überprüfen der Ergebnisse der Archivierung und Löschung

Sie überprüfen die Ergebnisse der Archivierungs- und Löschregel, die Sie geplant haben. Führen Sie eine oder beide der folgenden Aktionen aus:

- [Anzeigen des Archivierungs- und Löschverlaufs](#) (siehe Seite 559).
- Anzeigen der Archivierungs- und Löschprotokolldatei

Anzeigen des Archivierungs- und Löschverlaufs

Sie können den Verlauf für jede einzelne Archivierungs- und Löschregel anzeigen. Zeigen Sie zum Beispiel die Objekte an, die über eine Regel gelöscht werden.

Gehen Sie wie folgt vor:

1. Navigieren Sie auf der Registerkarte "Administration" zu "Archivierung und Löschung" und dann zu "Archivierungs- und Löschverlauf".
Die Seite "Archivierungs- und Löschverläufe - Liste" wird angezeigt.
2. Klicken Sie auf "Filter anzeigen", und geben Sie die Filterkriterien an. Geben Sie zum Beispiel das früheste Startdatum ein, um nur Einträge aus einem angegebenen Zeitraum anzuzeigen.

Hinweis: Um das Feld "Weitere Suchargumente" anzuzeigen, klicken Sie auf das Wasserhahnsymbol. Dieses Feld ist nur für erfahrene Anwender gedacht, die mit SQL und Majic umgehen und bestimmte weitere Suchargumente angeben können, die im Standard-Suchbereich nicht zur Verfügung stehen. Um ein zusätzliches Suchargument anzugeben, geben Sie eine SQL-WHERE-Klausel in dieses Feld ein.

Die Liste der übereinstimmenden Regeln werden angezeigt.

3. Klicken Sie auf den Regelnamen, für den Sie die Regelkonfiguration überprüfen möchten.

Die Seite "Archivierungs- und Löschregel - Detail" wird geöffnet.

Anzeigen der Archivierungs- und Löschmodaldatei

Sie können die Datei "arcpur.log" aus dem Verzeichnis "\$NX_ROOT/log/" überprüfen, um die Fehler zu finden, die während der Ausführung der geplanten Archivierungs- und Löschrregeln aufgetreten sind.

Hinweis: Die Größenbeschränkung für die Dateien "arcpur.log" ist in "\$NX_ROOT/NX.env" definiert.

Die Größenbeschränkung für die Protokolldatei "Archivieren und Löschen" sowie für die Datendatei.

@NX_ARCPUR_FILESIZE=2000000000

Beim Archivieren und Löschen werden arcpur.log.0 und arcpur.log.1 bis arcpur.log.9 erstellt, nachdem der Grenzwert für jede Protokolldatei erreicht ist.

Wiederherstellen der archivierten Daten

Sie können die archivierten Daten wiederherstellen, wenn Sie sie wieder in der Datenbank benötigen.

Gehen Sie wie folgt vor:

1. Starten Sie die Daemons im dbadmin-Modus. Der Modus "Dbadmin" erlaubt den beschränkten Zugriff, sodass Sie "pdm_load" sicher ausführen können, um archivierte Daten wiederherzustellen. Führen Sie den DBADMIN-Befehl "pdm_d_mgr -s" auf den folgenden Servern aus, abhängig von Ihrer CA SDM-Konfiguration:
 - Konventionell: Primärserver
 - Erweiterte Verfügbarkeit: Hintergrundserver
2. Navigieren Sie in das Stammverzeichnis oder in den UNC-Speicherort, wo Sie die archivierten Daten gespeichert haben.
3. Suchen Sie die archivierte Datendatei (.dat-Datei).
4. Kopieren Sie die Datei abhängig von Ihrer CA SDM-Konfiguration in folgende Server:
 - Konventionell: Primärserver
 - Erweiterte Verfügbarkeit: Hintergrundserver
5. Wenden Sie "pdm_load" auf die Datei an. Beispiel:
pdm_load -a -f 2004611T1726_Call_Request.dat
6. Wenn ein Problem mit dem Befehl "pdm_load" auftritt, führen Sie folgende Schritte durch:
 - a. Überprüfen Sie die Befehlszeile und "\$NX_ROOT/log/arcpur.log" nach Fehlern.
 - b. [Starten Sie die CA SDM-Server neu](#) (siehe Seite 52).

7. Um zu verhindern, dass der Datensatz im nächsten Zyklus archiviert und gelöscht wird, gehen Sie folgendermaßen vor:
 - a. Aktualisieren Sie den Datensatz, um ihn wieder zu aktivieren.
 - b. Deaktivieren Sie die verknüpfte Archivierungs- und Löschregel.

Verbessern der Leistung mit Browser-Caching

Die Web-Schnittstelle von CA SDM verwendet viele JavaScript-Dateien, Stylesheets und Bilddateien, die recht groß sein und die Leistung beeinträchtigen können.

Um die Leistung der Web-Schnittstelle zu verbessern, richten Sie Ihren HTTP-Server so ein, dass der Browser des Anwenders diese Dateien zwischenspeichert, damit sie nur einmal pro Tag geladen werden.

Damit wird die Web-Schnittstellenleistung verbessert.

Hinweis: Die Standardinstallation konfiguriert Caching für Apache und IIS automatisch. Das Caching kann allerdings auch manuell konfiguriert werden.

Konfigurieren von Microsoft Internet Information Server

Sie können Microsoft Internet Information Server (IIS) konfigurieren, um dem Browser mitzuteilen, dass vom CA SDM-Verzeichnis geladene Dateien einen Tag nach dem Herunterladen ablaufen. Dies bedeutet, dass der Browser nur einmal pro Tag vom Server diese Dateien abrufen, unabhängig davon, wie oft diese verwendet werden.

So konfigurieren Sie Microsoft Internet Information Server:

1. Starten Sie die Anwendung Internetdienste-Manager (für Windows 2000 und XP wählen Sie „Programme“, „Verwaltungstools“, „Internetdienste-Manager“).
2. Navigieren Sie zum CA SDM-Dateiordner. Das ist normalerweise CAIsd:
 - a. Klicken Sie auf das Pluszeichen neben dem Server, auf dem die CA SDM-Web-Schnittstelle ausgeführt wird.
 - b. Klicken Sie auf das Pluszeichen neben "Standardwebsite".
 - c. Scrollen Sie nach unten bis zu CAIsd.
3. Klicken Sie mit der rechten Maustaste auf den Ordner "CAIsd", und wählen Sie "Eigenschaften" aus.

Die Seite "Eigenschaften" wird angezeigt.
4. Klicken Sie auf die Registerkarte „HTTP-Header“.

5. Aktivieren Sie das Kontrollkästchen zum Aktivieren des Inhaltsablaufs.
6. Wählen Sie die Option "Ablaufen nach", geben Sie "1" in das Textfeld ein, und wählen Sie einen Tag aus der Dropdown-Liste.
7. Klicken Sie auf "OK".

Die Eigenschaften werden gespeichert und die Änderungen treten sofort in Kraft.

Konfigurieren von Apache

Sie können Apache so konfigurieren, dass der Browser informiert wird, dass aus dem CA SDM-Verzeichnis geladene Dateien einen Tag nach dem Laden ablaufen. Dies bedeutet, dass der Browser den Server nur einmal pro Tag nach diesen Dateien abfragt, unabhängig davon, wie oft diese verwendet werden.

Sie konfigurieren Apache, indem Sie eine Textkonfigurationsdatei aktualisieren. Die Standardinstallation ändert Ihre aktive Konfigurationsdatei im Apache-Verzeichnis "conf" (normalerweise "httpd.conf"), so dass diese die Anweisung enthält:

```
Include installation-directory/bopcfg/www/CAisd_apache.conf
```

installation-directory muss durch einen vollständigen Pfad ersetzt werden. Unter Windows ist dieser Pfad im Allgemeinen "C:\Programme\CA\CA SDM". Ersetzen Sie unter UNIX *installation-directory* durch den Wert "\$NX_ROOT".

Die durch diese Include-Anweisung referenzierte Datei CAisd_apache.conf enthält den folgenden Text: Auch hier wird *installation-directory* wie in der Include-Anweisung durch den vollständigen Pfad ersetzt.

```
<IfModule mod_alias.c>
    Alias /CAisd installation-directory/bopcfg/www/wwwroot/
    <IfModule mod_expires.c>
        <Directory installation-directory/bopcfg/www/wwwroot>
            ExpiresActive    On
            ExpiresDefault   "access plus 1 day"
        </Directory>
    </IfModule>
</IfModule>
```

Um Apache manuell für das Caching von CA SDM-Dateien durch den Browser zu konfigurieren, fügen Sie in Ihrer Apache-Konfigurationsdatei Anweisungen ein, die denen in CAisd_apache.conf entsprechen. Sie können diese Anweisungen entweder direkt in der Datei hinzufügen, oder Sie können eine Include-Anweisung hinzufügen, die auf eine andere Datei verweist, (wie dies bei der Standardinstallation der Fall ist).

Änderungen der Apache-Konfigurationsdateien werden erst wirksam nach Aktualisierung von Apache.

Löschen des Cache-Speichers

Wenn Sie ein JavaScript, Bild, Stylesheet, HTML, oder eine vom HTTP-Server selbst geladene Hilfsdatei ändern, dann müssen Sie Ihre Benutzer anweisen, ihren Browser-Cache zu löschen.

Hinweis: Damit die Änderungen an HTML-Dateien wirksam werden, müssen Sie entweder die Web-Engine neu starten oder das Dienstprogramm "pdm_webcache" verwenden. In einer Entwicklungsumgebung können Sie diese Anfrage umgehen, indem Sie die Konfigurationsdateieigenschaft "SuppressHtmlCache" angeben.

So löschen Sie den Browser-Cache für Internet Explorer:

1. Wählen Sie "Extras" und dann "Internetoptionen" aus.

Das Dialogfeld "Internetoptionen" wird angezeigt.

2. Klicken Sie auf "Dateien löschen".

Ein Bestätigungsfenster wird eingeblendet.

3. Klicken Sie auf "OK".

Der Browser-Cache wird gelöscht.

So löschen Sie den Browser-Cache für Firefox:

1. Wählen Sie "Extras" und dann "Private Daten löschen".

2. Klicken Sie auf die Schaltfläche "Private Daten jetzt löschen".

Der Browser-Cache wird gelöscht.

Änderung der Konfigurationsdatei

Wenn Sie die CA SDM-Web-Schnittstelle installieren, wird eine Beispieldatei (*web.cfg*) in `$NX_ROOT/bopcfg/www` installiert, die Sie entsprechend Ihrer Bedürfnisse ändern können. Die Datei *web.cfg* enthält hilfreiche Informationen in Form von Kommentaren, die Sie lesen können, wenn Sie die Datei anzeigen. Gehen Sie zur Datei *web.cfg* im entsprechenden Verzeichnis:

- (Windows) `%NX_ROOT%\bopcfg\www\`
- (UNIX) `$NX_ROOT/bopcfg/www/`

Hinweis: Einige zusätzliche Konfigurationsvariablen wie "charset" sind auch im Optionsmanager verfügbar. Diese sind über die Registerkarte "Administration" in der Web-Schnittstelle verfügbar. Hinweis: Weitere Informationen finden Sie in der *Online-Hilfe*.

AllowInactiveSrelEntry

Gibt an, ob ein Datensatz gespeichert werden kann, wenn er auf inaktive Datensätze in einer Referenztabelle verweist.

- Wenn diese Eigenschaft ausgelassen oder auf null eingestellt wird, werden inaktive Referenztableneinträge (zum Beispiel Anfragestatus oder Change-Kategorie) nicht in Dropdown-Auswahllisten eingeschlossen und können nicht für die Suche oder für hierarchische Suchfelder angegeben werden.
- Wenn diese Eigenschaft auf 1 eingestellt ist, wird das Inaktiv-Kennzeichen in Referenztableneinträgen ignoriert.

Unabhängig von der Einstellung dieses Kennzeichens können Datensätze, die bereits einen Verweis auf einen inaktiven Referenztableneintrag enthalten, gespeichert werden, ohne den Verweis zu ändern; das Kennzeichen beeinflusst nur neue Feldwerte.

AnnouncementLength

Gibt die maximale Anzahl der Ankündigungen an, die im Eröffnungsbildschirm für die Kunden- und die Analystenschnittstellen angezeigt werden können. CA SDM beginnt die Anzeige mit der neuesten Ankündigung und zeigt so viele weitere Ankündigungen an wie für "AnnouncementLength" festgelegt. Benutzer der Analystenschnittstelle können zusätzliche Ankündigungen anzeigen, indem sie im Menü "Suchen" die Option "Ankündigungen" wählen.

Standardwert: 10. Dies bedeutet, dass die zehn letzten Ankündigungen angezeigt werden.

AnonymousPrio

Gibt gültige Prioritäten für Tickets an, die von Gastbenutzern erstellt wurden. Diese Benutzer können nur eine der Prioritäten in der „AnonymousPrio“-Liste für ihre Tickets angeben. Einträge in der Prioritätenliste werden durch Leerzeichen getrennt. Jeder Eintrag muss entweder eine Zahl zwischen 1 und 5 sein oder „keiner“ lauten (ohne Anführungszeichen). Die Standardpriorität für Tickets, die von Gastbenutzern erstellt werden, sollte zuerst angegeben werden und kann in der Liste wiederholt werden.

Die gültigen Werte für „AnonymousPrio“ entsprechen den symbolischen Namen der Prioritäten, wie verteilt. Sie können den Java-Client verwenden, um diese symbolischen Namen anzupassen. Dies beeinflusst jedoch nicht die Angabe für „AnonymousPrio“, die weiterhin auf Prioritäten durch ihre Standardnamen verweisen muss, wobei 1 der höchsten Priorität entspricht.

Der **Standardwert** für "AnonymousPrio" ist "none". Das bedeutet, dass alle von einem Gastbenutzer erstellten Anforderungen die Priorität "none" (keine) haben.

Autom. Ausfüllen

Gibt an, dass die Web-Schnittstelle Suchfelder automatisch ausfüllen soll, wenn ein Benutzer nach dem Eintragen eines Wertes die Tabulatortaste drückt. Wenn in diesem Fall die Option zum automatischen Ausfüllen aktiviert ist, bittet der Browser den Server um die Bestätigung, dass die Aktualisierung korrekt ist. Dadurch wird entweder der vollständige Name in das Feld eingetragen (wenn der Benutzer einen Namen teilweise angegeben hat) oder ein Popup-Suchfenster wird angezeigt (wenn die Auswahl des Benutzers falsch oder nicht eindeutig war).

Diese Eigenschaft ist optional. "Autom. Ausfüllen" ist standardmäßig aktiviert. Wenn diese Eigenschaften-ID daher übergangen oder auf "Yes" eingestellt ist, wird beim Verlassen eines Suchfeldes mit der Tabulatortaste die Datenbank automatisch durchsucht. Wenn diese Eigenschaft auf "No" eingestellt ist, erfolgt kein automatisches Ausfüllen, und Suchfelder werden erst überprüft, wenn der Datensatz gespeichert wird.

CAisd

Gibt den Pfad (einschließlich eines führenden Schrägstrichs) zum Alias- oder virtuellen Verzeichnis in Ihrem HTTP-Server an, das die vom CA SDM-Webserver benötigten Dateien enthält. Diese Eigenschaft hat normalerweise den Wert "/CAisd" in UNIX- und in Windows-Installationen. Für Apache-Server sollte sie in einer Alias-Anweisung in einer Konfigurationsdatei definiert werden. Für IIS sollte sie einem Alias-Feld im Verzeichniseigenschaftenfenster entsprechen.

CGI

Gibt den Namen des ausführbaren CGI-Programms an, das mit der Web-Schnittstelle geliefert wird (ohne .exe-Suffix).

Standard: pdmweb

Hinweis: Wenn Sie dieses Programm umbenennen, müssen Sie diese Eigenschaft aktualisieren.

CgiReport

Gibt den Namen des ausführbaren CGI-Programms für Webberichte an, das mit der Web-Schnittstelle geliefert wird (ohne .exe-Suffix).

Standard: pdm_cgireport

Hinweis: Wenn Sie dieses Programm umbenennen, müssen Sie diese Eigenschaft aktualisieren.

ContactAutoDesc

Gibt an, ob der Name des Kontakts in die Beschreibung von neuen Issues und Anfragen eingefügt werden soll, die in der Kunden- und der Mitarbeiterschnittstelle erstellt werden. Wenn diese Eigenschaft ausgelassen oder mit 0 angegeben wird, werden keine automatischen Informationen zur Beschreibung neuer Issues und Anfragen hinzugefügt. Wenn für diese Eigenschaft 1 angegeben wird, wird der Name des Kontakts automatisch in die Beschreibung von Issues und Anfragen eingefügt, die in der Kunden- und der Mitarbeiterschnittstelle erstellt werden. Diese Eigenschaft wirkt sich nicht auf die Analytikerschnittstelle aus.

ContactAutoDescWithIP

Gibt an, ob der Name des Kontakts in die Beschreibung neuer Issues und Anfragen eingefügt werden soll, die in der Kunden- und der Mitarbeiterschnittstelle erstellt werden. Wenn diese Eigenschaft ausgelassen oder mit 0 angegeben wird, werden keine IP-Adressinformationen zur Beschreibung neuer Issues und Anfragen hinzugefügt. Wenn für diese Eigenschaft und für die Eigenschaft "ContactAutoDesc" jeweils 1 angegeben wird, werden der Name und die IP-Adresse des Kontakts automatisch in die Beschreibung von Issues und Anfragen eingefügt, die in der Kunden- und der Mitarbeiterschnittstelle erstellt werden. Diese Eigenschaft wirkt sich nicht auf die Analytikerschnittstelle aus. Sie wird ignoriert, es sei denn „ContactAutoDesc“ ist 1.

CstPrio

Gültige Prioritäten für Issues, die über die Kunden-Web-Schnittstelle erstellt werden. Benutzer der Kundenschnittstelle können nur eine der Prioritäten in der "CstPrio"-Liste für ihre Issues angeben. Außerdem können sie die Priorität eines Issue nicht aktualisieren, wenn ein Analyst sie in einen Wert geändert hat, der nicht in der Liste enthalten ist.

Einträge in der Prioritätenliste werden durch Leerzeichen getrennt. Jeder Eintrag muss entweder eine Zahl zwischen 1 und 5 sein oder „keiner“ lauten (ohne Anführungszeichen). Die Standardpriorität für Issues, die über die Kundenschnittstelle erstellt werden, sollte zuerst angegeben werden (und kann in der Liste wiederholt werden).

Standard: keine, 3, 4, 5

Die gültigen Werte für „CstPrio“ entsprechen den symbolischen Namen der Prioritäten, wie verteilt. Sie können den Java-Client verwenden, um diese symbolischen Namen anzupassen. Dies beeinflusst jedoch nicht die Angabe für „CstPrio“, die weiterhin auf Prioritäten durch ihre Standardnamen verweisen muss, wobei 1 der höchsten Priorität entspricht.

DateFormat

Definiert die Reihenfolge der Elemente in Datumseinträgen.

Standard: MM/DD/YYYY hh:mm hh:mm a(AM, PM – vormittags, nachmittags)

Symbol	Beschreibung
m	stellt den Monat in 1 oder 2 Ziffern dar
MM	stellt den Monat in 2 Ziffern dar
D	stellt den Tag in 1 oder 2 Ziffern dar
DD	stellt den Tag in 2 Ziffern dar
YY	stellt das Jahr in 2 Ziffern dar
YYYY	stellt das Jahr in 4 Ziffern dar
H	stellt die Stunde in 1 oder 2 Ziffern im 24-Stundenformat dar
HH	stellt die Stunde in 2 Ziffern im 24-Stundenformat dar
h	stellt die Stunde in 1 oder 2 Ziffern im 12-Stundenformat dar
hh	stellt die Stunde in 2 Ziffern im 12-Stundenformat dar
m	stellt Minuten in 1 oder 2 Ziffern dar
mm	stellt Minuten in 2 Ziffern dar
s	stellt Sekunden in 1 oder 2 Ziffern dar
ss	stellt Sekunden in 2 Ziffern dar
a(am, pm)	stellt am und pm als Zeichenfolge dar

DateFormatNoTime

Diese Eigenschaft entspricht "DateFormat", aber ohne Angabe der Uhrzeit.

DebugSource

Aktiviert das Standardbrowser-Kontextmenü in den CA SDM-Formularen- Wenn diese Eigenschaft nicht festgelegt ist, können Sie in einem Formular mit der rechten Maustaste klicken, um ein CA SDM-Menü anzuzeigen. Gehen Sie bei der Einstellung dieser Eigenschaft vorsichtig vor, da einige der Optionen im Standardbrowser-Kontextmenü Ausführungsfehler verursachen können (das ist der Grund, warum diese Eigenschaft normalerweise deaktiviert ist). Im Internet Explorer können Sie das Standardbrowser-Kontextmenü auch anzeigen, wenn die „DebugSource“-Eigenschaft nicht eingestellt ist. Drücken Sie hierzu die STRG-Taste, während Sie mit der rechten Maustaste klicken.

DebugTrace

Veranlasst die Web-Engine, Trace-Informationen in die Datei "tdlog" zu schreiben.

Wichtig! Diese Eigenschaft sollten Sie für eine normale Verwendung *nicht* einstellen. Sie sollten sie nur verwenden, wenn es der CA Support verlangt.

EmpPrio

Gibt gültige Prioritäten für Anforderungen an, die über die Mitarbeiter-Web-Schnittstelle erstellt werden. Benutzer der Mitarbeiterschnittstelle können nur eine der Prioritäten in der "EmpPrio"-Liste für ihre Anfragen angeben. Außerdem können sie die Priorität einer Anfrage nicht aktualisieren, wenn ein Analyst sie in einen Wert geändert hat, der nicht in der Liste enthalten ist.

Einträge in der Prioritätenliste werden durch Leerzeichen getrennt. Jeder Eintrag muss entweder eine Zahl zwischen 1 und 5 sein oder „keiner“ lauten (ohne Anführungszeichen). Die Standardpriorität für Anfragen, die über die Mitarbeiterschnittstelle erstellt werden, sollte zuerst angegeben werden (und kann in der Liste wiederholt werden).

Standard: keine, 3, 4, 5

Die gültigen Werte für „EmpPrio“ entsprechen den symbolischen Namen der Prioritäten, wie verteilt. Sie können den Java-Client verwenden, um diese symbolischen Namen anzupassen. Dies beeinflusst jedoch nicht die Angabe für „EmpPrio“, die weiterhin auf Prioritäten durch ihre Standardnamen verweisen muss, wobei 1 der höchsten Priorität entspricht.

ExclLockSeconds

Gibt die maximale Anzahl der Sekunden an, für die ein Benutzer eine exklusive Sperre für einen Datensatz erhält, nachdem er auf "Bearbeiten" geklickt hat. Nachdem diese Zeit abgelaufen ist, hebt die Web-Engine die Sperre auf, und andere Benutzer können den Datensatz aktualisieren. Die Web-Engine versucht eine Neuaufnahme der Sperre, wenn ein Benutzer eine Speicherung anfordert, nachdem „ExclLockSeconds“ abgelaufen ist. Dieser Versuch ist nur erfolgreich, wenn kein anderer Benutzer den Datensatz aktualisiert hat, während die Sperre ausgesetzt war. Wenn der Versuch, die Sperre wiederaufzunehmen, scheitert, muss der Benutzer die Aktualisierungen erneut eingeben.

Standard: 120 (zwei Minuten)

Dieses Argument ist optional. Wenn Sie keinen Wert angeben, wird der Standardwert verwendet.

Hinweis: Die Einstellung "ExclLockSeconds" muss kürzer als die Einstellung für die Zeitüberschreitung (Timeout) sein. ExclLockSeconds ist in Sekunden angegeben, das Timeout in Minuten.

FormCacheMax

Gibt die Höchstzahl von Formularen an, die im Speicher der Web-Engine für jeden Benutzer beibehalten werden. Die Web-Engine behält immer die letzten „FormCacheMax“-Formulare bei, die von jedem Benutzer verwendet werden. Auf Formulare mit höheren Zeitangaben kann die Zeitüberschreitungsfunktion angewendet werden. Auf Formulare, für die eine Zeitüberschreitung erfolgte, kann mit den Schaltflächen „Zurück“ oder „Vor“ auf der Hauptseite nicht zugegriffen werden, und sie können nicht mehr in einem Popup-Formular abgesendet werden.

Standard: 10

Formulare, für die eine Zeitüberschreitung erfolgte, entlasten den Speicher der Web-Engine. Es ist aber möglich, dass Benutzer sie bisweilen manuell aktualisieren müssen. Sie können "FormCacheMax" auf -1 einstellen, um die Zeitüberschreitungsfunktion für Formulare zu deaktivieren.

FormTimeout

Gibt die Mindestzahl von Sekunden an, die ein Formular in der Web-Engine beibehalten wird, bevor es aus dem Cache gelöscht werden kann. Für die Benutzer ist immer mindestens die Sekundenzahl in diesem Parameter definiert, um ein Formular vor dem Absenden zu bearbeiten. Zudem behält die Web-Engine immer die zuletzt verwendeten „FormCacheMax“-Formulare für jeden Benutzer bei.

Mit der Eigenschaft „StayCacheList “ können Sie verhindern, dass die Zeitüberschreitung für die angegebenen Formulare gilt.

Standard: 180 (3 Minuten)

FormTitle

Gibt eine Zeichenfolge an, die in die Titelleiste eines Webbrowsers eingefügt wird und die ein CA SDM-Webformular anzeigt. Der Wert von „FormTitle“ ergänzt den Titel des betreffenden angezeigten Formulars.

Standard: CA SDM

Wenn z. B. der Standardwert beibehalten wird und Microsoft Internet Explorer zum Anzeigen des Formulars "Ankündigungsdetails" verwendet wird, zeigt die Titelleiste Folgendes an:

"Ankündigungsdetails – CA SDM - Microsoft Internet Explorer"

Diese Eigenschaft ist optional. Wenn keine Angabe erfolgt, verwendet die Analytiker-Web-Schnittstelle keinen konstanten Wert im Titel. Die Kunden und die PDA-Web-Schnittstellen werden auf den Standardwert zurückgesetzt.

HitTrackFile

Gibt den vollständigen Pfad zu einer Datei an, die ein Protokoll aller verwendeten Webseiten empfängt. Jedes Mal, wenn ein Benutzer eine Seite anfordert, wird eine Zeile in diese Datei eingetragen. Die Datei kann unbegrenzt wachsen; verwenden Sie diese Eigenschaft somit mit Vorsicht.

Hinweis: Datensätze, die einen Zeitstempel, eine Benutzer-ID, eine Datenbankdatensatz-ID und einen HTML-Formularnamen enthalten, werden an diese Datei angehängt. Das Format der Datensätze kann sich ändern. Sie müssen diese Datei regelmäßig pflegen, damit sie nicht zu groß wird.

Diese Eigenschaft ist optional. Wenn keine Angabe erfolgt, wird keine Trefferverfolgungsdatei erstellt.

HtmlpCacheSize

Gibt die Größe des HTML-Caches an. Wenn die Größe überschritten wird, wird das am wenigsten verwendete Formular aus dem Cache gelöscht.

Standard: 1000

ListAllMaximum

Gibt die maximale Anzahl der Datensätze in einer Liste an, bevor eine Anfrage zur Anzeige der gesamten Liste eine Warnmeldung ausgibt, die den Benutzer darauf hinweist, dass die Anfrage die Leistung beeinträchtigt und nicht zulässig ist.

Standard: 2500

ListAllWarn

Gibt die maximale Anzahl der Datensätze in einer Liste an, bevor eine Anfrage zur Anzeige der gesamten Liste eine Warnmeldung ausgibt, die den Benutzer darauf hinweist, dass die Anfrage die Leistung beeinträchtigen kann und eine Bestätigung erfordert.

Standard: 1000

ListBottomMaximum

Gibt die maximale Anzahl der Datensätze in einer Liste an, bevor eine Anfrage zum Blättern ans Ende der Liste eine Warnmeldung ausgibt, die den Benutzer darauf hinweist, dass die Anfrage die Leistung beeinträchtigt und nicht zulässig ist.

Standard: 2500

ListBottomWarn

Gibt die maximale Anzahl der Datensätze in einer Liste an, bevor eine Anfrage zum Blättern ans Ende der Liste eine Warnmeldung ausgibt, die den Benutzer darauf hinweist, dass die Anfrage die Leistung beeinträchtigt und eine Bestätigung erfordert.

Standard: 1000

ListPageLength

Gibt die maximale Anzahl der gefundenen Datensätze an, die nach Durchführen einer Suche auf einer Listenseite angezeigt werden.

Standard: 10

LogoutURL

Gibt die vollständige URL einer Webseite an, die angezeigt wird, nachdem Sie sich aus CA SDM abgemeldet haben. Diese Eigenschaft ist optional. Wenn keine Angabe erfolgt, kehrt das System nach Abmeldung des Benutzers zum Anmeldeformular zurück.

Lr_Refresh

Gibt das Aktualisierungsintervall in Sekunden für den Log-Reader an. Wenn diese Eigenschaft ungleich null ist, aktualisiert sich der Reader für Benachrichtigungsprotokoll automatisch im angegebenen Intervall (mindestens alle dreißig Sekunden).

Diese Eigenschaft ist optional. Wenn keine Angabe erfolgt, aktualisiert sich der Reader für Benachrichtigungsprotokoll alle 5 Minuten (Standardwert von 300 Sekunden). Wenn für diese Eigenschaft null angegeben wird, aktualisiert sich der Reader für Benachrichtigungsprotokoll nicht automatisch.

MacroPath

Gibt eine Liste der Verzeichnispfade an, die die Web-Engine durchsucht, um vom PDM_MACRO-Tag angeforderte Dateien zu finden. Sie können mehrere Verzeichnisse durch Leerzeichen getrennt angeben. Sie können Umgebungsvariablen in den Verzeichnisnamen einschließen, indem sie ihnen ein Dollarzeichen voranstellen (zum Beispiel \$NX_ROOT). Trennen Sie sowohl in Windows als auch in UNIX die Pfadkomponenten mit einem Schrägstrich(/); verwenden Sie nicht den umgekehrten Schrägstrich (\). Diese Eigenschaft ist erforderlich. Sie wird normalerweise folgendermaßen eingestellt:

```
$NX_ROOT/site/mods/macro $NX_ROOT/bopcfg/www/macro
```

MatchesFound

Gibt den Text der Meldung an, die in einem Feld angezeigt wird, wenn der Schlüssel eines Benutzers für ein Suchfeld nicht eindeutig ist, und das Bearbeitungsformular mit einer Dropdown-Auswahlliste erneut angezeigt werden muss. Diese Eigenschaft ist optional. Wenn keine Angabe erfolgt, wird die Standardmeldung "Mehrere Übereinstimmungen" verwendet.

MaxRecordsAutoSuggest

Legt die Anzahl von Datensätzen fest, die durch Suche während der Eingabe oder automatische Empfehlung als Vorschläge unter einem Suchfeld angezeigt werden.

Standard: 25

MaxSelectList

Gibt die maximale Anzahl der Übereinstimmungen an, die in der Dropdown-Auswahlliste angezeigt werden, wenn der Schlüssel eines Benutzers für ein Suchfeld nicht eindeutig ist und das Bearbeitungsformular erneut angezeigt werden muss. Wenn mehr als diese Übereinstimmungen gefunden werden, wird die Meldung "Zu viele Übereinstimmungen" angezeigt.

MinCharsAutoSuggest

Legt die Mindestanzahl von Zeichen fest, die in ein Suchfeld eingegeben werden, bevor die Ergebnisse der Suche während der Eingabe bzw. der automatischen Empfehlung angezeigt werden.

Standard: 3

MouseoverPreviewDelayTime

Legt die Zeitverzögerung (in Millisekunden) zwischen dem Bewegen des Mauszeigers über eine Verknüpfung und der Anzeige der QuickInfo-Vorschau fest.

Wenn der Mauszeiger von der Verknüpfung entfernt wird, bevor diese Zeit abgelaufen ist, wird die Vorschau nicht angezeigt.

Standard: 1000

NoMatchesFound

Gibt den Text der Meldung an, die in einem Feld angezeigt wird, wenn der Schlüssel eines Benutzers für ein Suchfeld nicht korrekt ist und das Bearbeitungsformular erneut angezeigt werden muss. Diese Eigenschaft ist optional. Wenn keine Angabe erfolgt, wird die Standardmeldung "Keine Übereinstimmungen gefunden" verwendet.

PreLogin Timeout

Gibt die maximale Anzahl von Minuten an, für die die Web-Engine eine Sitzung vor der Anmeldung aktiv hält. Die Web-Engine startet automatisch eine Sitzung, wenn ein Benutzer ein Anmeldeformular anfordert. Dabei wird vorweggenommen, dass der Benutzer die Anmeldung abschließt. Wenn der Benutzer sich nicht innerhalb der angegebenen Zeitspanne anmeldet, verwirft die Web-Engine die Sitzung. Wenn sich der Benutzer anschließend anmeldet, erstellt die Web-Engine eine neue Sitzung, die für den Benutzer transparent ist.

Diese Eigenschaft hat keine Auswirkung auf den Endbenutzer. Ihr einziger Zweck ist die Leistung – Ausgleich der Speichernutzung der Web-Engine im Vergleich zum Aufwand für das Verwerfen und Neuerstellen einer Sitzung. Diese Eigenschaft ist optional. Wenn keine Angabe erfolgt, wird der Standardwert von einer Minute verwendet.

RedirectingURL

Gibt den URL an, den der WebDirector verwenden soll, um dieser Web-Engine Anforderungen zu senden. Diese Eigenschaft gibt den vollständigen URL der Web-Engine an, einschließlich http. Diese Eigenschaft ist erforderlich, wenn Sie WebDirector verwenden. Die Eigenschaft wird ignoriert, wenn Sie Webdirector nicht verwenden.

SchedExpMaximum

SchedExpMaximum

Gibt die maximale Anzahl an Ablaufplanereignissen an, die gleichzeitig exportiert werden können.

Standard: 1000

Wichtig! Die Standardeinstellung ist die größtmögliche Anzahl an Exporten, die CA SDM gleichzeitig bearbeiten kann. Eine Erhöhung des Standardwerts könnte zu einer Instabilität des Systems führen. Wenn Sie versuchen, mehr als den in "SchedExpMaximum" angegebenen Wert zu exportieren, erscheint die Meldung, dass Ihre Exportanfrage abgelehnt wird.

SellListCacheExclude

SellListCacheExclude

Gibt die Namen der Factorys (Objekte) an, die von der Zwischenspeicherung für <PDM_SELECT>-Listen ausgeschlossen werden sollen. Zur Verbesserung der Leistung speichert die Web-Engine den Inhalt kleiner Tabellen, die in <PDM_SELECT>-Listen (Dropdown-Listen) und hierarchischen Suchlisten verwendet werden, normalerweise in ihrem eigenen Speicher zwischen. Unter Umständen möchten Sie die Zwischenspeicherung für eine Tabelle unterdrücken, wenn Sie mit Hilfe von Datenaufteilungsbedingungen angeben, dass verschiedene Benutzer verschiedene Ansichten der Tabelle erhalten sollen. Zusätzlich erübrigt der Einschluss von Tabellen in den Wert dieser Eigenschaft, dass die Web-Engine die Datensatzzählung für diese Tabellen beim Start abfragt, was die Startleistung leicht verbessert. Diese Eigenschaft ist optional. Wenn diese Eigenschaft angegeben wird, sollte sie einen oder mehrere Objektnamen durch Leerzeichen getrennt enthalten.

SellListCacheMax

SellListCacheMax

Definiert die maximale Anzahl von Datensätzen in einer Tabelle, die in der Web-Engine zwischengespeichert werden können. Die Web-Engine speichert den gesamten Inhalt von Tabellen bis zur Cachegröße im eigenen Speicher. Dadurch verbessert die Web-Engine ihre Leistung, indem sie <PDM_SELECT>-Listen unter Verwendung dieser Tabellen erstellt. Durch Angabe eines höheren Wertes für diese Eigenschaft können Sie die Leistung verbessern, was auf Kosten des Speicherverbrauchs geht.

Standard: 10

"SelListCacheMax" wird für Tabellen ignoriert, die in hierarchischen Suchenlisten benutzt werden, wie zum Beispiel Kategorien für Anfragen, Issues und Changes. Die Web-Engine speichert den gesamten Inhalt von Tabellen, die in hierarchischen Suchlisten verwendet werden, stets im eigenen Speicher. Wenn Sie eine große Anzahl von Werten in diesen Tabellen haben, können Sie die Eigenschaft „SelListCachePreload“ angeben.

SelListCachePreload

Gibt an, dass eine oder mehrere Tabellen beim Starten in den ausgewählten Cache der Web-Engine geladen werden sollen. Nicht in dieser Eigenschaft angegebene Tabellen werden das erste Mal dann geladen, wenn sie verwendet werden. Wenn "SelListCacheMax" einen großen Wert hat oder wenn eine große Zahl von Datensätzen in einer hierarchischen Suchliste (zum Beispiel Kategorie) vorhanden ist, können Sie die Tabelle in "SelListCachePreload" angeben. Dies vermeidet eine Verzögerung der Antwortdauer, wenn ein Benutzer das erste Mal auf ein Formular zugreift, das die Tabelle benutzt.

Die Werte für die Eigenschaft „SelListCachePreload“ geben Sie in Form einer durch Leerzeichen getrennten Liste von Objektnamen an. Jedem Objektnamen kann eine optionale Liste mit Attributnamen in Klammern folgen. Die in der Liste angegebenen Attribute werden in die Web-Engine geladen. Wenn keine Attribute angegeben sind, werden nur der allgemeine Name und der „rel attr“-Wert des Objekts geladen. Dies ist für Dropdown-Auswahllisten ausreichend, für hierarchische Suchen aber unter Umständen nicht. Wenn Sie die Formulare für hierarchische Suchen (hiersel_xx.html, wobei xx ein Objektnamen ist) ändern, stellen Sie sicher, dass die Eigenschaft „SelListCachePreload“ alle im Formular verwendeten Attribute angibt. Wenn Sie ein Attribut auslassen, wird bei Verwendung des Formulars der Cache neu geladen.

Die Eigenschaft „SelListCachePreload“ ist optional. Wenn Sie diese Eigenschaft nicht angeben, werden Daten erst dann in den Selekt-Cache geladen, wenn ein Benutzer ein Formular anfordert, das eine Dropdown-Auswahlliste oder eine hierarchische Suche verwendet.

```
chgcac(description owning_contract) chgstat crs isscat(description  
owning_contract) issstat pcat(description cr_flag in_flag pr_flag  
owning_contract) pri tskstat urg pcat_cr(description cr_flag in_flag pr_flag  
owning_contract) pcat_pr(description cr_flag in_flag pr_flag owning_contract)  
pcat_in(description cr_flag in_flag pr_flag owning_contract)
```

StayCacheList

Gibt die Namen der Formulare an, die niemals aus dem Formular-Cache entfernt werden, unabhängig davon, wie lange sie angezeigt werden. Diese Eigenschaft stellt sicher, dass die festen Frames in einer Frame-Anzeige für die gesamte Dauer einer Sitzung beibehalten werden. Sie kann verwendet werden, damit andere Formulare permanent in den Cache-Speicher aufgenommen werden. Verwenden Sie diese Eigenschaft mit Vorsicht. Der Standardwert ist wie folgt:

```
scoreboard.html top_splash.html buttons.html hiersel_admin_tree.html
```

SuppressHtmlCache

Gibt an, dass die Web-Engine alle Dateien, die den Inhalt einer Seite definieren, jedes Mal neu lesen soll, wenn die Seite angefordert wird. Die Analyse einer HTML-Datei nimmt einen beträchtlichen Teil der Verarbeitungszeit der Web-Engine in Anspruch und beinhaltet normalerweise das Lesen mehrerer physischer Dateien (da die meisten Seiten PDM_INCLUDE-Tags benutzen). Die Web-Engine legt analysierte Dateien normalerweise im eigenen Speicher ab, damit zukünftige Anfragen für die gleiche Seite sofort erfüllt werden können. Dadurch wird die Leistung deutlich verbessert. Dieses Verhalten kann jedoch für Benutzer, die neue Seiten entwickeln oder Seiten aktualisieren, ungünstig sein, da die Web-Engine aktualisiert werden muss, damit die Änderungen wirksam werden.

Diese Eigenschaft ist optional und erfordert keinen Wert. Wenn sie angegeben wird, speichert die Web-Engine analysierte Dateien nicht im Cache, und Änderungen für HTML-Dateien werden sofort wirksam. Wegen ihrer Auswirkung auf die Leistung sollte diese Eigenschaft nicht in einer Produktionsumgebung angegeben werden.

SuppressLoginAndLogoutMsg

Gibt an, dass die Web-Engine keine Meldung in der CA SDM-Protokolldatei speichern soll, wenn ein Benutzer sich in der Web-Schnittstelle anmeldet oder von ihr abmeldet.

Diese Eigenschaft ist optional. Wenn sie nicht angegeben wird, protokolliert die Web-Engine jedes Mal eine Meldung, wenn sich ein Benutzer an- oder abmeldet.

SuppressMacroCache

Gibt an, dass die Web-Engine bei jeder Anfrage einer neuen Seite alle gespeicherten Makros verwerfen soll. Die Web-Engine legt analysierte Makros normalerweise im eigenen Speicher ab, damit zukünftige Anfragen für das Makro sofort erfüllt werden können. Dadurch wird die Leistung verbessert. Dieses Verhalten kann jedoch für Benutzer, die neue Makros entwickeln oder Makros aktualisieren, ungünstig sein, da die Web-Engine aktualisiert werden muss, damit die Änderungen wirksam werden.

Diese Eigenschaft ist optional. Wenn sie angegeben wird, speichert die Web-Engine analysierte Makros nicht im Cache, und Änderungen für Makros werden sofort wirksam. Wegen ihrer Auswirkung auf die Leistung sollte diese Eigenschaft nicht in einer Produktionsumgebung angegeben werden.

Timeout

Gibt die Anzahl der Minuten an, für die eine Benutzersitzung inaktiv sein kann, bevor sie automatisch beendet wird und alle Serverressourcen freigegeben werden.

Hinweis: Für "Timeout" muss eine längere Dauer angegeben werden als für "ExclLockSeconds". ExclLockSeconds ist in Sekunden angegeben, das Timeout in Minuten.

TooManyMatches

Gibt den Text der Meldung an, die in einem Feld angezeigt wird, wenn der Schlüssel eines Benutzers für ein Suchfeld nicht eindeutig ist und die Anzahl der Übereinstimmungen für den Schlüssel den Wert von "MaxSelectList" überschreitet. Diese Eigenschaft ist optional. Wenn keine Angabe erfolgt, wird die Standardmeldung "Zu viele Übereinstimmungen" verwendet.

UpdatedAnnouncementsPopup

Gibt das Intervall an, in dem der Browser prüft, ob neue Ankündigungen vorhanden sind. Wenn eine neue Ankündigung gefunden wird, zeigt der Browser die Ankündigung automatisch in einem Popup-Fenster an. Das Intervall wird in Minuten angegeben. Um eine Beeinträchtigung der Browser-Leistung zu verringern, wird empfohlen für diese Variable einen Wert größer als 5 (Minuten) einzustellen.

UseDirector

Gibt an, wann der WebDirector diese Web-Engine kontrolliert. Die folgende Tabelle definiert die möglichen Werte:

Wert	Beschreibung
Nein	Die Web-Engine ist vom WebDirector unabhängig. Dies ist der Standardwert.
Ja	Der WebDirector muss alle Sitzungen starten, einschließlich des Anmeldeformulars. Wenn ein Benutzer eine direkte Verbindung zur Web-Engine versucht, bittet die Web-Engine den WebDirector um eine Verweisung.
AfterLogin	Die Web-Engine verweist eine Sitzung nach Authentifizierung des Benutzers an den WebDirector. Eine mit „UseDirector AfterLogin“ konfigurierte Web-Engine ist einzig für die Authentifizierung zuständig und ist dadurch ein Kandidat für die Verwendung von Secure Sockets (SSL) für maximale Sicherheit.
BeforeLogin	Die Web-Engine verweist eine Sitzung vor Authentifizierung des Benutzers an den WebDirector. Eine mit „UseDirectory BeforeLogin“ konfigurierte Web-Engine zeigt nie eine Anmeldungsseite an und akzeptiert nie ein Anmeldekennwort.

Diese Eigenschaft ist optional. Wenn keine Angabe erfolgt, verwendet die Web-Engine den WebDirector nicht.

UseNestedTabs

Gibt an, ob die Steuerung für verschachtelte Registerkarten auf Detailformularen angezeigt werden soll.

Standard: Aktiviert

WebDirectorSlumpName

Gibt den Namen des WebDirectors an, der mit dieser Web-Engine verbunden ist. Diese Eigenschaft ist nur notwendig, wenn Sie mehrere WebDirectors verwenden oder wenn Sie für den WebDirector einen anderen Slump-Namen als den Standardnamen „web:director“ festgelegt haben.

Diese Eigenschaft ist optional, wenn Sie Webdirector verwenden. Die Eigenschaft wird ignoriert, wenn Sie Webdirector nicht verwenden.

WillingnessValue

Gibt basierend auf einer Skala von 0 bis 10 die Bereitschaft dieser Web-Engine an, Sitzungen zu akzeptieren. Diese Eigenschaft ist nur verfügbar, wenn Sie WebDirector verwenden. Dieser Wert hat nur eine Bedeutung im Vergleich mit der Bereitschaft anderer mit demselben WebDirector verbundener Web-Engines. Der WebDirector überträgt Sitzungen an Web-Engines entsprechend ihres „Willingness“-Wertes. Eine Web-Engine mit einem doppelt so hohen „Willingness“-Wert wie eine andere Web-Engine bedient durchschnittlich die doppelte Anzahl von Sitzungen.

Der „WillingnessValue“ null bedeutet, dass die Web-Engine keine Sitzungen annimmt. Dieser Wert kann nützlich sein, wenn "UseDirector" auf "AfterLogin" eingestellt ist.

Diese Eigenschaft ist optional, wenn Sie Webdirector verwenden. Die Eigenschaft wird ignoriert, wenn Sie Webdirector nicht verwenden. Wenn keine Angabe erfolgt, wird der „Willingness“-Wert einer Web-Engine auf 5 eingestellt.

WorkFrameTimeout

Gibt die maximale Wartezeit (in Sekunden) an, die eine Web-Engine auf eine Antwort auf eine interne Serveranforderung wartet, bevor sie die Anforderung als fehlgeschlagen betrachtet. Der Workframe-Wert wird für Funktionen der Web-Schnittstelle von CA SDM verwendet, die andere Serverdaten als herkömmliche Webseiten erfordern. Hierzu zählen Funktionen wie automatisches Ausfüllen, Laden von Kategorieeigenschaften und Aktualisieren von Scoreboard-Zählungen. Workframe-Anforderungen an CA SDM schlagen in der Regel nicht fehl. Jedoch können Workframe-Anforderungen an andere Server (zum Beispiel integrierte Produkte wie Knowledge Management) fehlschlagen, wenn der Zielserver nicht aktiv ist oder ein Netzwerkproblem den Zugriff darauf verhindert. Die Eigenschaft „WorkFrameTimeout“ gibt die Zeitspanne an, nach deren Ablauf eine Anforderung als fehlgeschlagen betrachtet wird und der Workframe für andere Anforderungen verfügbar ist.

Hinweis: "WorkFrameTimeout" wird nur geprüft, wenn ein Workframe erforderlich ist und alle Workframes in Gebrauch sind. Daher ist es ziemlich wahrscheinlich, dass ein Remoteserver mehr Zeit für seine Antwort hat als für „WorkFrameTimeout“ angegeben. Der Wert von „WorkFrameTimeout“ ist ein Mindestwert.

Diese Eigenschaft ist optional. Wenn keine Angabe erfolgt, verwendet die Web-Engine einen „WorkFrameTimeout“-Wert von 30 Sekunden.

Kapitel 14: Verwenden der Text-API

Dieses Kapitel enthält folgende Themen:

[Text-API](#) (siehe Seite 579)

Text-API

Die *Text-API* ist eine Schnittstelle, über die Sie textbasierte Objekte in der CA SDM-Datenbank, zum Beispiel Issues, Anfragen, Kontakte und Assets, erstellen und aktualisieren können. Bei der Verwendung der Text-API können Sie den meisten Feldern Werte zuweisen, auf die Anwender zugreifen können.

Wichtig! Für CA SDM müssen alle Eingaben im UTF-8-Format vorliegen; andernfalls können Daten beschädigt werden. Mit dem [Dienstprogramm "pdm_unconv"](#) (siehe Seite 1196) können Sie Daten aus einem lokalen Zeichensatz in UTF-8- und von UTF-8 in einen lokalen Zeichensatz konvertieren.

Sie können über folgende Schnittstellen auf die Text-API zugreifen:

- Befehlszeile
- E-Mail
- CA NSM

Hinweis: Eine Alternative zur Text-API für die anwendungsübergreifende Integration sind Webservices.

Weitere Informationen:

[Konvertierungsmethoden](#) (siehe Seite 591)

Befehlszeilenschnittstelle

Mit dem Befehl *pdm_text_cmd* können Sie die Befehlszeilenschnittstelle der Text-API aktivieren. Sie geben bestimmte Informationen, zum Beispiel die zu verarbeitende Tabelle und die auszuführende Operation, mit Hilfe von Parametern für den Befehl "pdm_text_cmd" an.

Die Eingabe in die Text-API wird an den Befehl "pdm_text_cmd" in Form einer Eingabedatei oder direkt von STDIN übergeben.

Hinweis: Wenn Sie Parameter über die Eingabeaufforderung weitergeben, verwenden Sie STRG+Z in Windows und STRG+D in POSIX.

Wichtig! Sie können einzelne oder doppelte Anführungszeichen nicht als Parameter für die Befehle *bop_cmd* und *pdm_text_nxd* verwenden.

Weitere Informationen:

[pdm_text_cmd – Befehlszeilenschnittstelle für Text-API](#) (siehe Seite 1192)

CA Network and Systems Management-Schnittstelle

Wenn CA NSM und CA SDM integriert sind und Sie Anfragen von CA NSM-Ereignissen erstellen, wird der Parameter "user_parms" in den Erstellerregeldefinitionen an die Text-API übergeben. Der CA SDM-Erstellerprozess (tngwriter) definiert seine eigenen Ersetzungsparameter zum Ändern des Textes, bevor dieser an die Text-API gesendet wird. Das Schlüsselwort LOG_AGENT wird zum Ende der Eingabe hinzugefügt, um das "log_agent" für die Anfrage zu setzen.

Hinweis: Sie müssen das die Datei "Text_API.cfg" für alle Felder aktualisieren, die von CA NSM-Alert Management Systemen an CA SDM weitergegeben werden. Diese Datei wird für Integrationen in Webservices, E-Mail und AHD.DLL. verwenden.

Weitere Informationen:

[Schlüsselwörter](#) (siehe Seite 582)

Eingabeformat

Die Eingabe in die Text-API geschieht folgendermaßen:

- In der Befehlszeilenschnittstelle wird geschieht die Eingabe typischerweise in einer Textdatei, die an den Befehl "pdm_text_cmd" übergeben wird.
- In der E-Mail-Schnittstelle geschieht die Eingabe im Text der E-Mail. Sie geben einen regulären Ausdruck an, um die Zielobjektkennungen zu suchen.

Sie formatieren die Text-API-Eingabe auf die gleiche Weise unabhängig von der verwendeten Schnittstelle.

Das grundlegende Format für die Eingabe sieht wie folgt aus:

`%keyword=value`

oder

`%PROPERTY={{property_label}}value`

Das normale Verhalten von Text-API-Befehlen hat die folgenden Ausnahmen, wobei der zuletzt angezeigte von zwei oder mehreren, in Konflikt stehenden Befehlen Vorrang hat:

- Wenn eine Meldung mehrere gültige Ticket-ID-Artefakte, die mit der Filterzeichenfolge der Postfachregel übereinstimmen, oder mehrere Text-API-Ticket-ID-Befehle enthält, wird die erste Übereinstimmung verwendet. Ebenso überschreibt ein Ticket-ID-Artefakt, das unter Verwendung der Filterzeichenfolge der Postfachregel identifiziert wird, einen beliebigen Text-API-Ticket-ID-Befehl, unabhängig davon, welcher zuerst angezeigt wird.
- Wenn eine Meldung mehrere Protokollkommentar-Text-API-Befehle enthält, werden alle Kommentare bereitgestellt, obwohl die Reihenfolge, in der sie im Ticket-Aktivitätsprotokoll erscheinen, variieren kann.

Alle Ticket-ID-Artefakte, die mit dem Filter übereinstimmen - gültig oder anderweitig - und Text-API-Ticket-ID-Befehle innerhalb der Meldung - anwendbar oder anderweitig, angewandt oder anderweitig - werden auskommentiert, bevor die Meldung bereitgestellt wird. Die Ticket-ID-Artefakte, die durch die Postfachregelfilter identifiziert werden, werden als `-(...)-` angezeigt. Vorangestellte Prozentzeichen (%) in Text-API-Ticket-ID-Befehlen werden in zwei Klammer-auf-Symbole vor und zwei Klammer-zu-Symbole nach dem Befehl konvertiert. Wenn ein Text-API-Ticket-ID-Befehl nach einem anderen Text-API-Befehl mit einem Protokollkommentar (`%LOG=...`) erscheint, dann wird der auskommentierte Text-API-Ticket-ID-Befehl zu einem separaten Protokollkommentar.

Hinweis: Der Protokollkommentar ist der einzige Text-API-Befehl, der mehrmals in einer Meldung erscheinen kann und trotzdem bei jedem Vorkommen angewendet wird. Bei allen anderen Befehlen verwendet die Text-API nur den letzten vorkommenden Befehl, da mehrmals vorkommende Befehle zueinander in Konflikt stehen. Mehrere Protokollkommentarbefehle stellen separate Protokollkommentarmeldungen im Ticket bereit; dies geschieht nicht notwendigerweise in einer besonderen Reihenfolge.

Wenn ein Text-API-Ticket-ID-Befehl in der Meldung entweder am Anfang der Meldung oder zwischen zwei anderen Text-API-Befehlen erscheint, wird er zusätzlich in einen Protokollkommentar konvertiert. Wenn der vorherige Befehl ein Protokollkommentar (%LOG=...) oder eine Aktualisierungsbeschreibung (%DESCRIPTION=...) ist, wird er an diesen Befehl angehängt und wird nicht zu einem separaten Protokollkommentar.

Eingehende Meldungen, die als HTML ohne eingeschlossene Klartextversion gesendet werden, geben ihren Meldungstext ab. Wenn die Meldung mit einem beliebigen Postfachregelfilter mit einem leeren Meldungstext übereinstimmt, kann ein Ticket mit einer leeren Beschreibung oder mit dem zitierten Nachrichtenbetreff als Gesamtheit der Ticket-Beschreibung erstellt werden.

Schlüsselwörter

Sie können zwei Arten von Schlüsselwörtern als Eingabe in der Text-API verwenden.

- Definitionen im Abschnitt [KEYWORDS] der Datei "text_api.cfg": Dieser Typ ist eine Gruppe von Schlüsselwörtern, die sich direkt auf die Felder der verschiedenen Tabellen beziehen, die Sie aktualisieren können. Zum Beispiel sind hier die meisten der Felder im Formular "Issue – Detail" definiert. Mit diesen Schlüsselwörtern können Sie Werte für Felder in dem Datensatz festlegen, den Sie aktualisieren oder erstellen. Zum Beispiel stellt die folgende Zeile die Priorität des Issue auf 5 ein:

```
%PRIORITY=5
```

Der Abschnitt [KEYWORDS] der Datei "text_api.cfg" listet alle Schlüsselwörter auf. Sie können zusätzliche Schlüsselwörter definieren (zum Beispiel, um Text-API-Zugriff auf Felder zu gewähren, die Sie beim Anpassen Ihres Datenbankschemas hinzugefügt haben).

- Die folgenden besonderen Schlüsselwörter werden immer folgendermaßen definiert, ungeachtet der Inhalte der Datei "text_api.cfg":

Schlüsselwort	Beschreibung
ASSET	Wird verwendet, um einem Ticket ein Element anzuhängen (gültig für Anfragen, Issues und Changes). Der angegebene Wert ist der Elementname, der bereits existieren muss. Sie können dieses Schlüsselwort mehrmals angeben, da einem Ticket mehrere Elemente angehängt werden können.
ATTACHMENT	Wird intern von der E-Mail-Schnittstelle verwendet, um einem Ticket E-Mail-Anhänge hinzuzufügen.

Schlüsselwort	Beschreibung
DESCRIPTION	Gibt den Wert an, der für das Beschreibungsfeld des Tickets verwendet werden soll. Dieses Schlüsselwort wird übernommen, wenn eine Eingabe an die Text-API ohne Angabe eines expliziten Schlüsselwortes gesendet wird. Dieses Schlüsselwort wird automatisch vom Post-Vernichter angewandt, wenn die Meldung mit keinem Schlüsselwort anfängt, aber ein Ticket-ID-Artefakt oder Schlüsselwort enthält. Sie können die Art und Weise ändern, wie das Schlüsselwort DESCRIPTION für Aktualisierungen behandelt wird. Verwenden Sie hierzu den folgenden Eintrag im Abschnitt [OPTIONS] der Datei "text_api.cfg": UPDATE_DESC_IS_LOG Wenn diese Option auf YES eingestellt ist, wird der Wert zur Erstellung eines Protokollkommentars verwendet. Wenn der Wert NO lautet, überschreibt der Wert das vorhandene Beschreibungsfeld.
FROM_EMAIL FROM_EMAIL_OVERRIDE	Wird von der E-Mail-Schnittstelle für den Abgleich mit dem Feld für die E-Mail-Adresse im ca_contact-Datensatz verwendet. Er wird auch als "log_agent" für das Ticket verwendet. Wenn beides angegeben wird, wird FROM_EMAIL ignoriert. Hinweis: FROM_EMAIL wird automatisch vom Post-Vernichter mit der Absenderadresse der Meldung gesetzt.
FROM_PERSID	Wird von der Befehlszeilenschnittstelle verwendet, um "log_agent" für eine Operation zu definieren (wenn zum Beispiel ein ca_contact-Datensatz keine Anwender-ID enthält). Dieses Schlüsselwort wird automatisch von pdm_text_cmd weitergegeben, wenn der -Parameter "p" angegeben wird. Der Wert wird mit der persistent_id eines ca_contact-Datensatzes abgeglichen.
FROM_USERID	Wird nur in der Befehlszeilenschnittstelle verwendet, um log_agent für eine Operation zu definieren. Dieses Schlüsselwort wird automatisch von "pdm_text_cmd" weitergegeben, wenn der -Parameter "u" angegeben wird. Der Wert wird mit der Anwender-ID eines Kontakts abgeglichen.
LOG	Wird zur Erstellung eines Protokolleintrags verwendet (gültig für Anfragen, Changes, Issues und Kontakte). Dieses Schlüsselwort wird automatisch vom Post-Vernichter angewandt, wenn die Meldung ohne ein Schlüsselwort anfängt, aber entweder ein Ticket-ID-Artefakt oder Schlüsselwort, oder ein DESCRIPTION-Schlüsselwort enthält.
LOG_AGENT	Wird von der CA NSM-Schnittstelle verwendet, um log_agent für eine Operation zu definieren. Der Wert wird mit dem ID-Feld eines Kontaktdatenatzes abgeglichen.

Schlüsselwort	Beschreibung
PROPERTY	Wird zur Einstellung des Wertes für eine Eigenschaft verwendet (gültig nur für Anfragen, Changes und Issues). Im Gegensatz zu anderen Schlüsselwörtern, die von einem Gleichheitszeichen und einem Wert gefolgt werden, muss die PROPERTY-Schlüsselwortsyntax die Eigenschaft folgendermaßen angeben: PROPERTY={{property_label}}value Sie müssen <i>property_label</i> genauso angeben, wie es in der Datenbank angezeigt wird.
SEARCH	Wird nur in der Befehlszeilenschnittstelle und der CA NSM-Schnittstelle verwendet und liefert eine Liste von Schlüsselwörtern zur Verwendung in einer Abfrage, um mehrere Tickets für ein Asset zu aktualisieren. Der Wert besteht aus einer Liste von Schlüsselwörtern, die in der Suche verwendet werden. Das Schlüsselwort SEARCH wird von der CA NSM-Schnittstelle automatisch festgelegt.
SEARCH_EXPLICIT	Wird nur in der CA NSM-Schnittstelle verwendet, um das von der CA NSM-Schnittstelle gelieferte Schlüsselwort SEARCH zu überschreiben. Die Werte werden auf dieselbe Weise bereitgestellt wie für das Schlüsselwort SEARCH.

Weitere Informationen:

[pdm text cmd – Befehlszeilenschnittstelle für Text-API](#) (siehe Seite 1192)

Eingabekonventionen für Schlüsselwörter

Die folgenden Konventionen beziehen sich auf die Formatierung bei der Schlüsselworteingabe:

- Setzen Sie vor jedes Schlüsselwort (einschließlich PROPERTY) ein Prozentzeichen (%). Das Prozentzeichen muss in Spaltenposition eins stehen. Wenn die erste nichtleere Zeile der Eingabe kein Prozentzeichen am Anfang der Zeile hat, wird entweder %DESCRIPTION= oder %LOG= als das Präfix für die eingehenden Daten benutzt, je nachdem, ob ein Ticket-ID-Artefakt oder ein Schlüsselwort gefunden wurde. Wenn %DESCRIPTION gesetzt wird, wird der Inhalt der Meldung bis zum ersten Schlüsselwort als Ticket-Beschreibung bereitgestellt. Wenn %LOG= gesetzt wird, wird der Inhalt der Meldung bis zum ersten Schlüsselwort als Protokollkommentar bereitgestellt.
- Verwenden Sie innerhalb des Schlüsselwortes keine Leerzeichen zwischen dem %-Zeichen und dem Schlüsselwort oder zwischen dem Schlüsselwort und dem Gleichheitszeichen (=).

- Setzen Sie Werte nicht in Anführungszeichen; alle Daten nach dem Gleichheitszeichen werden als Werte interpretiert.
- Bei Schlüsselwörtern wird nicht zwischen Groß- und Kleinschreibung unterschieden.
- Wenn die Eingabe doppelte Schlüsselwörter enthält, wird das letzte Schlüsselwort verwendet; ansonst ist die Reihenfolge, in der Sie die Schlüsselwort-/Wertpaare angeben, unwichtig.
- Geben Sie Schlüsselwortwerte genauso an wie für das entsprechende Feld in der Web-Schnittstelle. Um zum Beispiel einen Analysten-Kontakttyp anzugeben, verwenden Sie %CONTACT_TYPE=Analyst, auch wenn in der Datenbank dieser Wert als Ganzzahl gespeichert ist. Das Schlüsselwort CONTACT_TYPE ist in "text_api.cfg" definiert und [konvertiert den angegebenen Wert](#) (siehe Seite 591) gemäß dem gespeicherten Wert.
Hinweis: Ob beim Wert zwischen Groß- und Kleinschreibung unterschieden wird, hängt vom zugrunde liegenden DBMS ab.
- Zeichenfolgendaten können sich über mehrere Zeilen erstrecken.

Formatieren von E-Mail-Nachrichten zum Aktualisieren eines Tickets

Benutzer können E-Mail-Nachrichten formatieren, um Tickets zu erstellen oder zu aktualisieren.

So können Sie E-Mail-Nachrichten durch Ändern der folgenden Felder formatieren, um Tickets zu erstellen oder zu aktualisieren:

Bis

Gibt den Mailboxnamen an, der dem für den berechtigten Benutzer eingerichteten CA SDM-Kontakt zugewiesen ist.

Von:

Gibt die Person an, die die E-Mail versendet. Die Person muss in der Tabelle "ca_contact" definiert sein, oder die Option "Anonymen Zugang erlauben" ist in der anzuwendenden Postfachregel angegeben.

Hinweis: Der Absenderadresse wird i. d. R. der Konfiguration Ihres E-Mail-Clients entnommen und braucht daher nicht für einzelne Nachrichten angegeben zu werden.

Anhänge

Ermöglicht das Anhängen von Dokumenten und anderen Dateien an die E-Mail-Nachricht, um auf diese Weise Anhänge an das Text-API zu übermitteln.

Betreff

Führt einen Abgleich mit Schlüsselwörter in einer Postfachregel-Filterzeichenfolge durch, insbesondere bei der Erstellung von Tickets.

Text

Legt den Nachrichtentext der E-Mail unter Verwendung des Text-APIs fest. Sie können eines der Schlüsselwörter `ISSUE_ID`, `REQUEST_ID` oder `CHANGE_ID` angeben, um ein entsprechendes Ticket zu erstellen oder zu aktualisieren.

Start- und Endtrennzeichen in E-Mail-Nachrichten

Einige E-Mail-Schnittstellen fügen Informationen am Anfang oder Ende von E-Mail-Nachrichten hinzu, die eine Fehlfunktion der E-Mail-Schnittstelle verursachen können (zum Beispiel MIME-Codierung). Wenn Ihre E-Mail-Schnittstelle Informationen hinzufügt, können Sie die folgenden Begrenzer benutzen: `start-request` und `end-request`. Die E-Mail-Schnittstelle ignoriert Informationen vor `"start-request"` und nach `"end-request"`.

Hinweis: Der Mail Eater unterstützt keine E-Mails im RTF- oder Nur-HTML-Format.

Beispiel: Verwendung der Begrenzer `start-request` und `end-request`

```
"start-request"  
message_body  
"end-request"
```

Text-API und Artefakte

Mit der Text-API wird der Betreff oder Text von E-Mail-Benachrichtigungen verarbeitet. Mit Postfachregeln können Sie Artefakte und Werte identifizieren, die die Text-API benutzt. Zum Beispiel können Sie die Regel für Incidents als `"Incident:{{object_id}}"` definieren. `"Suche Incident:1234"` wird für die Text-API als `"%INCIDENT_ID=1234"` übersetzt. 1234 ist die `Ref_Num` für den Incident. Weil das Artefakt in der E-Mail eindeutig und leicht zu finden sein muss, können Sie das Artefakt ausgeprägter machen, wie z. B. `"%Incident:{{object_id}}%"`.

Das Zeichen nach dem Schlüsselwort `{{object_id}}` darf kein Buchstabe, keine Zahl, kein Komma, kein Schrägstrich (`/`), kein Pluszeichen (`+`) und kein Gleichheitszeichen (`=`) sein, weil diese Zeichen innerhalb eines Artefakts erscheinen können. Anderenfalls können Zeichen, die dem Artefakt folgen, als Teil des Wertes des Artefakts missverstanden werden, oder ein Zeichen innerhalb des Wertes des Artefakts kann als Zeichen, das dem Wert folgt, missverstanden werden.

Die Komponente "Mail Eater" führt folgende Schritte aus:

1. Sucht das Artefakt in einer E-Mail (wie `"Incident:1234"`), das dem entsprechenden Ticket oder einem anderen von der Text-API unterstützten Objekt zugeordnet ist.
2. Übersetzt das Artefakt in ein Text-API-Token (wie etwa `"%INCIDENT_ID=1234"`).

- Die Komponente "Mail Eater" sendet die markierte Nachricht an die Text-API. Die Text-API verarbeitet die E-Mail, wendet den Text, Befehle oder beides auf das entsprechende Ticket an und erzeugt eine automatische Antwort-E-Mail, die zeigt, ob die erhaltene E-Mail-Nachricht erfolgreich angewendet wurde. Je nach den ausgeführten Aktionen wird eine Benachrichtigungs-E-Mail-Nachricht auch separat verschickt, um bestimmte Ereignisse, wie die Erstellung eines Tickets, anzuzeigen.

Einrichten von Benachrichtigungsantworten zum Aktualisieren von Tickets

Der Text-API-Dämon (pdm_text_nxd) erstellt und aktualisiert Tickets mit Informationen von externen Schnittstellen, wie beispielsweise Befehlszeile und E-Mail. Sie können Post für die Verwendung der Text-API einrichten, so dass Anwender (Kontakte) Tickets aktualisieren können, indem sie auf E-Mail-Benachrichtigungen antworten. Der Text der Antwort wird dem Ticket als Protokollkommentaraktivität hinzugefügt.

So richten Sie Benachrichtigungsantworten ein, um Tickets zu aktualisieren:

- Setzen Sie die Benachrichtigungsmethode, die der Kontakt verwendet, auf "pdm_mail -T *Antwort-E-Mail-Adresse*" oder "pdm_mail -F *Antwort-E-Mail-Adresse*". Die *Antwort-E-Mail-Adresse* gibt die Eingangsadresse für das Postfach an. Wenn der Kontakt bei einer E-Mail auf "Antwort" klickt, wird diese Adresse mit dem Feld "Von" oder der Antwortadresse der Nachricht ausgefüllt, auf die er antwortet.

-T legt die Antwortadresse fest. -F legt die Adresse "Von" fest, die als Antwortadresse benutzt wird, wenn keine andere Adresse angegeben ist.

Hinweis: Nicht alle E-Mail-Programme können eine Antwortadresse verarbeiten.

- Erstellen oder aktualisieren Sie eine Postfachregel mit Hilfe eines Text-API-Schlüsselwortes.

Die benutzerdefinierten Artefakte in den Postfachregelfiltern ersetzen die folgenden Text-API-Schlüsselwörter:

Objekt	Text-API-Schlüsselwort	Kennung
Incident (Störung)	%INCIDENT_ID	Ref_num
Problem	%PROBLEM_ID	Ref_num
Request	%REQUEST_ID	Ref_num
Chg_ref_num	%CHANGE_ID	Chg_ref_num
Issue	%ISSUE_ID	Ref_num

3. Erstellen oder aktualisieren Sie eine Benachrichtigungswortfolge, die der Regel entspricht.
4. Erstellen oder aktualisieren Sie eine Meldungsvorlage, die die Benachrichtigungswortfolge verwendet.
5. Aktualisieren Sie die in Schritt 2 erstellte Postfachregel, um die in Schritt 4 erstellte oder aktualisierte Meldungsvorlage festzulegen.

Hinweis: Informationen zum Ausführen der einzelnen Schritte finden Sie in der *Online-Hilfe*.

Nachdem der Anwender die Benachrichtigung erhalten und darauf geantwortet hat, werden die folgenden Aktionen automatisch ausgeführt:

1. Wenn die Filterzeichenfolge gefunden wird, werden das dazugehörige Ticket-ID-Schlüsselwort und der vom Platzhalter angezeigte Wert an die Nachricht angehängt.
2. Wenn ein passendes Ticket-ID-Artefakt gefunden wird, wird das entsprechende Ticket mit einem Protokollkommentar, einer neuen Beschreibung oder mit anderen Werten in Übereinstimmung mit dem Text, den Schlüsselwörtern und Befehlen in der Nachricht aktualisiert.
3. Wenn kein passendes Ticket-ID-Artefakt gefunden wird, wird ein Ticket mit einer Beschreibung und mit anderen Parametern in Übereinstimmung mit dem Text, den Schlüsselwörtern und Befehlen in der Nachricht erstellt.

Einrichten einer Antwort auf eine Incident-Benachrichtigung – Beispiel

Dieses Beispiel zeigt, wie eine Antwort auf eine Incident-Benachrichtigung eingerichtet wird.

So richten Sie eine Antwort auf eine Incident-Benachrichtigung ein:

1. Erstellen Sie eine Postfachregel mit den folgenden Feldern und Werten:
 - Filter – Text enthält
 - Filterzeichenfolge – %Incident:{{object_id}}%
 - Fall ignorieren – JA
 - Aktion – Objekt aktualisieren
 - Aktionsobjekt – Incident
2. Erstellen Sie eine Benachrichtigungszeichenfolge, die folgende Regel enthält:
 - Symbol – IncidentReply
 - Code – IncidentReply

- Aktiv – Aktiv
- Beschreibung – Kommentar, der die Antwort für einen Incident / ein Problem / eine Anfrage einbettet.
- Wortfolge – Um @`{call_req_id.type.sym}` einen Kommentar hinzuzufügen, antworten Sie einfach auf diese E-Mail oder fügen die Zeile unten ein (in einer separaten Zeile).

`%Incident:{call_req_id.ref_num}%`

Hinweis: Lassen Sie im Text einer automatischen Antwort der Postfachregel das Präfix "call_req_id." weg. Dieses Präfix wendet einen Kontext an, in dem sich der Postfachregeltext schon befindet, und solch eine Kontextänderung ist nicht gültig, wenn schon innerhalb dieses Kontextes gehandelt wird.

3. Erstellen oder aktualisieren Sie eine Meldungsvorlage, die die Benachrichtigungszeichenfolge folgendermaßen verwendet:
 - Benachrichtigungstext

Dies ist eine einfache Benachrichtigung.
`@{notification_phrase[IncidentURL1].phrase}`
4. Aktualisieren Sie die in Schritt 1 erstellte Postfachregel, um die in Schritt 3 erstellte Meldungsvorlage folgendermaßen festzulegen:

Meldungsvorlage – *Postfachregelname*

Aktualisieren von Tickets durch Endbenutzer – Beispiel

Das folgende Beispiel zeigt, wie ein Endbenutzer (Johann Schmid) auf eine E-Mail-Benachrichtigung antwortet, um ein Incident-Ticket zu aktualisieren.

Der Text oder Betreff der E-Mail enthält die Objektkennung. Der Platzhalter "`{{object_id}}`" in der Filterzeichenfolge steht für die Objektkennung.

1. Eine Benachrichtigung mit den folgenden Anweisungen wird an Johann Schmid gesendet:

Um dem Incident einen Kommentar hinzuzufügen, antworten Sie einfach auf diese E-Mail oder fügen die Zeile unten ein (in einer separaten Zeile).
`%Incident:1234%`
2. Johann Schmid antwortet auf die Benachrichtigung folgendermaßen:

Meine Antwort...

3. Die Komponente "Mail Eater" empfängt die folgende Textversion der E-Mail von Johann Schmid:

Meine Antwort...

Von: Service Desk

Gesendet: Mittwoch, 18. September 2009 10:22

An: Schmid, Johann

Betreff: Einfache Benachrichtigung

Dies ist eine einfache Benachrichtigung.

Um dem Incident einen Kommentar hinzuzufügen, antworten Sie einfach auf diese E-Mail oder fügen die Zeile unten ein (in einer separaten Zeile).

%Incident:1234%

4. Die Komponente "Mail Eater" verarbeitet Regeln in der entsprechenden Reihenfolge und findet das Artefakt "%Incident:1234%":

Meine Antwort...

Von: Service Desk

Gesendet: Mittwoch, 18. September 2009 10:22

An: Schmid, Johann

Betreff: Einfache Benachrichtigung

Dies ist eine einfache Benachrichtigung.

Um dem Incident einen Kommentar hinzuzufügen, antworten Sie einfach auf diese E-Mail oder fügen die Zeile unten ein (in einer separaten Zeile).

%INCIDENT_ID=1234

5. Die Komponente "Mail Eater" fügt die Text-API-Schlüsselwörter und den Wert "{{object_id}}" einer Anweisung "%INCIDENT_ID=" hinzu und fügt eine Markierung an der Stelle ein, wo der Wert "{{object_id}}" gefunden wurde. Der folgende Text zeigt die Daten, die an die Text-API gesendet werden. Der fett formatierte Text zeigt Werte, die von der Komponente "Mail Eater" hinzugefügt werden.

%LOG=Meine Antwort...

Von: Service Desk

Gesendet: Mittwoch, 18. September 2009 10:22

An: Schmid, Johann

Betreff: Einfache Benachrichtigung

Dies ist eine einfache Benachrichtigung.

Um dem Incident einen Kommentar hinzuzufügen, antworten Sie einfach auf diese E-Mail oder fügen die Zeile unten ein (in einer separaten Zeile).

%Incident:-((...))-%

%FROM_EMAIL=johann.schmid@company.com

%INCIDENT_ID=1234

6. Die Text-API fügt einen Protokollkommentar für Incident 1234 hinzu.

Konvertierungsmethoden

Viele der in "text_api.cfg" definierten Schlüsselwörter enthalten eine zugehörige Methode, um den angegebenen Wert in einen Wert zu konvertieren, der sich für die Speicherung in der Datenbank eignet. Mit dieser Funktion können Benutzer Werte genau wie in der Web-Schnittstelle festlegen. Sie benötigen keinerlei Wissen über die Implementierung, die im Hintergrund läuft.

In der Konfigurationsdatei finden Sie verschiedene Beispiele für diese Art der Schlüsselwort-Definition (z. B. ISSUE.PRIORITY und CONTACT.CONTACT_TYPE). Möchten Sie zusätzliche Schlüsselwörter definieren, beispielsweise weil Sie Text-API-Zugriff auf benutzerdefinierte Felder in Ihrem Datenbankschema einrichten möchten, können Sie eine der folgenden vordefinierten Methoden nutzen:

Methode	Ausgabetyt
lookup_actbool	INTEGER
lookup_asset_by_name	UUID
lookup_asset_by_persid	UUID
lookup_chg_category	STRING
lookup_chg_status	STRING
lookup_cnt_by_email	UUID
lookup_cnt_by_last_first_middle	UUID
lookup_cnt_by_logonid	UUID
lookup_cnt_by_persid	UUID
lookup_cnt_meth	INTEGER
lookup_cnt_type	INTEGER
lookup_company	UUID
lookup_cr_status	STRING
lookup_cr_template	STRING
lookup_domain	INTEGER
lookup_grc	INTEGER
lookup_group	UUID
lookup_impact	INTEGER
lookup_iss_category	STRING
lookup_iss_status	STRING

Methode	Ausgabetyp
lookup_loc	UUID
lookup_mfr_model	UUID
lookup_nr_family	INTEGER
lookup_org	UUID
lookup_person_contacting	INTEGER
lookup_position	INTEGER
lookup_priority	INTEGER
lookup_prob_category	STRING
lookup_product	INTEGER
lookup_resource_status	INTEGER
lookup_service_lvl	STRING
lookup_severity	INTEGER
lookup_state	INTEGER
lookup_timezone	STRING
lookup_type_of_contact	INTEGER
lookup_urgency	INTEGER
lookup_workshift	STRING

Wenn der Wert, den Sie konvertieren müssen, nicht durch eine dieser vordefinierten Methoden abgedeckt ist, müssen Sie eine benutzerdefinierte Methode erstellen. Die Methode sollte einen STRING-Wert als Eingabe verwenden und einen Wert (INTEGER, STRING oder UUID) als Ausgabe zurückgeben. Geben Sie den Wert -1 (oder „-1“) zurück, um anzugeben, dass der Wert nicht ermittelt werden kann und somit nicht eingestellt wird. Geben Sie für UUID “(uuid) NULL” zurück.

Zum Beispiel können Sie eine Methode entwerfen, um eine Benutzer-ID in einen ca_contact-Tabellenverweis zu konvertieren. Der eingehende Wert, zum Beispiel "Administrator", wird dann an die Methode übergeben, und die Methode gibt die ca_contact-Tabellen-ID für die Benutzer-ID "Administrator" zurück.

Die Art und Weise, in der Sie Schlüsselwörter in der Konfigurationsdatei definieren, bietet Ihnen den Vorteil, abhängig vom angegebenen Wert mehrere Schlüsselwortzuordnungen für das gleiche Feld zu definieren, einschließlich verschiedener Konvertierungsmethoden. Zum Beispiel kann ein Zuständiger mehrere verschiedene Schlüsselwortzuordnungen haben, die festlegen, wie sein Wert abhängig von den verschiedenen Eingabewerten eingestellt wird. Eine Eingabe könnte die Benutzer-ID, eine andere der Nachname, der Vorname und der zweite Vorname und wiederum eine andere Eingabe könnte die eigentliche ca_contact-ID sein (z. B. 793ED69B4E87A545BD8E911834D829FC). Jedes Schlüsselwort wird einer anderen Konvertierungsmethode zugeordnet, mit Ausnahme des letzten, das nicht konvertiert werden muss.

Die Konfigurationsdatei

Die Datei "text_api.cfg" definiert die Schlüsselwörter, die sich direkt auf die Felder der verschiedenen Tabellen beziehen, die Sie aktualisieren können. Sie verwenden diese Datei sowohl als Referenz für die Suche bestimmter vordefinierter Werte, wie zum Beispiel Schlüsselwörter, als auch als Mechanismus, um Text-API zu konfigurieren; die Standardkonfigurationsdatei funktioniert allerdings für die meisten Installationen ohne Änderung.

Die Datei "text_api.cfg" befindet sich in folgendem Verzeichnis:

- UNIX-\$NX_ROOT/Standort
- Windows-Installationsverzeichnis\Standort. Zum Beispiel:
C:\Programme\CA\Service Desk\Standort

Die Konfigurationsdatei unterteilt sich in Abschnitte, wobei innerhalb jedes Abschnitts bestimmte Attribute definiert werden. Attributdefinitionen haben folgende Form:

keyword=value

Keines der Schlüsselwörter unterscheidet zwischen Groß- und Kleinschreibung, während alle Werte (außer im Abschnitt [OPTIONS]) zwischen Groß- und Kleinschreibung unterscheiden.

Hinweis: Sie können die Datei "text_api.cfg" mit Hilfe eines beliebigen Texteditors anzeigen und ändern.

Wichtig! Wenn Sie eine Integration in die CA NSM-Komponente Alert Management Systems durchführen, müssen Sie "text_api.cfg" für zusätzliche Felder aktualisieren, die an CA SDM übergeben werden.

Weitere Informationen:

[Schlüsselwörter](#) (siehe Seite 582)

Options

Der Abschnitt [OPTIONS] der Datei "text_api.cfg" definiert Verarbeitungsoptionen, die sich von Standort zu Standort unterscheiden können. Zum Beispiel gibt es Optionen, die bestimmen, welches eingehende Datumsformat verwendet wird, für welche Felder Zeilenvorschübe beibehalten werden und ob Issues, Anfragen oder Changes über die E-Mail-Schnittstelle aktualisiert werden können. Alle Optionen in diesem Abschnitt sind konfigurierbar. Beachten Sie, dass Sie zwar Tabellennamen aus VALID_TABLE_LIST entfernen können, wenn Sie den Text-API-Zugriff auf diese Tabellen nicht unterstützen möchten, dass Sie aber keine Tabellennamen zu dieser Liste hinzufügen können.

Standardeinstellungen

Verwenden Sie den Abschnitt [XX_DEFAULTS] in der Datei text_api.cfg für alle Schnittstellen, die die Text-API verwenden (zum Beispiel [EMAIL_DEFAULTS] für die E-Mail-Schnittstelle und [CMD_DEFAULTS] für die Befehlszeilenschnittstelle). Der Abschnitt [XX_DEFAULTS] definiert die Standardwerte für Felder und Eigenschaften, die erforderlich sind, wenn sie der Anwender nicht direkt angibt. XX bezieht sich auf den Schnittstellentyp wie CMD oder E-MAIL.

Standardwerte können Sie in einem der folgenden Formate festlegen:

- table_name.keyword=value

Das Schlüsselwort (*keyword*) muss entweder im Abschnitt [KEYWORDS] oder als Eigenschaften in Ihrer Datenbank definiert werden. Jede mit dem Schlüsselwort verbundene Methode gilt automatisch für den Wert (*value*). Beispiel:

ISSUE.PRIORITY=1

Das Schlüsselwort PRIORITY wird in der Datei "text_api.cfg" definiert, damit eine Suche durchgeführt wird, um den angegebenen Wert mit dem entsprechenden, in der Datenbank gespeicherten Wert abzugleichen. In diesem Beispiel wird der Wert "1" in den Wert "5" geändert. Dies ist der Basis-Datenbankwert für das Prioritätssymbol 1. Mit dieser Funktion können Anwender den Wert angeben, genauso wie sie dies in der Web-Schnittstelle tun würden.

- table_name.PROPERTY={{property_label}}value

property_label muss als Eigenschaft in Ihrer Datenbank definiert sein.

Bei beiden Formaten muss *Tabelle_Name* einer der Werte sein, die von VALID_TABLE_LIST im Abschnitt [OPTIONS] definiert werden, wie zum Beispiel Issue, Request oder Kontakt.

Weitere Informationen:

[Konvertierungsmethoden](#) (siehe Seite 591)

Eingehende ignorieren

Es gibt mehrere Abschnitte [..._IGNORE_INCOMING] in der Datei "text_api.cfg", einen für jede Schnittstelle, die die Text-API verwendet (zum Beispiel [TNG_IGNORE_INCOMING] für die CA NSM-Schnittstelle und [EXT_IGNORE_INCOMING] für die von anderen CA-Produkten verwendete externe Schnittstelle). Diese Abschnitte definieren Felder und Eigenschaften, die in der Eingabe ignoriert werden (das Format ist dasselbe wie für Standardwerte beschrieben, außer das kein „=value“ angegeben wird). Mit dieser Funktion können Sie verhindern, dass Benutzer bestimmte Werte festlegen. Das wiederum gibt Ihnen mehr Sicherheit, wenn Kunden die E-Mail-Schnittstelle verwenden dürfen.

Diese Abschnitte IGNORE eignen sich gut bei ihrer Verwendung in Verbindung mit den entsprechenden Abschnitten [..._DEFAULTS]. Auf diese Weise können Sie verhindern, dass Benutzer einen bestimmten Wert festlegen, und Sie können gleichzeitig einen Standardwert liefern. Wenn Sie zum Beispiel verhindern möchten, dass Benutzer der E-Mail-Schnittstelle die Priorität eines Issue einstellen, können Sie die folgenden Werte festlegen:

```
[EMAIL_DEFAULTS]
ISSUE.PRIORITY=2
[EMAIL_IGNORE_INCOMING]
ISSUE.PRIORITY
```

In diesem Fall wird jede Priorität, die der Benutzer im Text der E-Mail-Nachricht angibt, ignoriert, und allen von der E-Mail-Schnittstelle erstellten Issues wird automatisch die Priorität 2 zugewiesen.

Beispieleingabe

Die folgenden Beispiele zeigen Informationen, die Sie in den Text einer E-Mail-Nachricht oder in eine Datei eingeben können und die als Eingabe für die Befehlszeilenschnittstelle fungieren soll.

Beispiel: Die erste Zeile enthält kein Schlüsselwort

Da in der ersten Spalte der ersten Zeile ein %keyword fehlt, wird in diesem Beispiel am Anfang der Meldung das Literal %DESCRIPTION= hinzugefügt. Das Beschreibungsfeld ist nun auf "Der gesamte Text erscheint im Beschreibungsfeld" eingestellt. (Der Zeilenumbruch bleibt erhalten, da ISSUE.DESCRPTION in der Liste der Felder für den Eintrag LINEFEEDS_ALLOWED im Abschnitt [OPTIONEN] der Datei "text_api.cfg" enthalten ist).

```
This entire text goes
into the description field
%PRIORITY=None
```

Beispiel: Die erste Zeile enthält ein Schlüsselwort

In diesem Beispiel wird das Schlüsselwort **PRIORITY** in der Datei "text_api.cfg" definiert, damit eine Suche durchgeführt wird, um den angegebenen Wert mit dem entsprechenden, in der Datenbank gespeicherten Wert zu vergleichen. Hier wurde der Wert **Keiner** in den Wert **"0"** geändert. Dies ist der Basis-Datenbankwert für das Prioritätssymbol 1. Mit dieser Funktion können Benutzer den Wert angeben, genauso wie sie dies in der Web-Schnittstelle tun würden.

```
%description=This is my description
%priority=None
%CATEGORY=Upgrade.PC
%PROPERTY={{Current CPU}}266 mhz
%PROPERTY={{Current Harddrive}}1 gig
%PROPERTY={{Requested Upgrade}}4 gig harddrive
```

Die angegebenen Werte werden für die Einstellung des Beschreibungs- und Prioritätsfeldes für das Ticket verwendet, ähnlich wie im vorherigen Beispiel (beachten Sie, dass Schlüsselwörter nicht zwischen Groß- und Kleinschreibung unterscheiden).

Der Wert für „Upgrade.PC“ wird gesucht, und das Kategoriefeld für das Ticket wird entsprechend eingestellt.

Durch Vergleich der folgenden Labels werden die drei Eigenschaftswerte eingestellt:

- Current CPU
- Current Hard drive
- Requested Upgrade

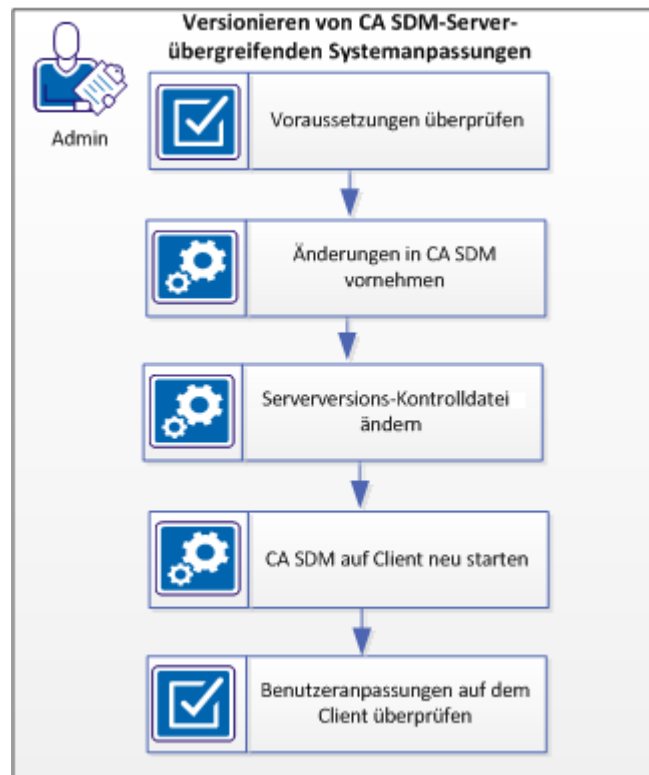
Kapitel 15: So führen Sie eine Versionskontrolle der Systemanpassungen auf CA SDM-Servern durch

Mit der CA SDM-Versionskontrolle können Sie die Systemanpassungen auf allen CA SDM-Servern (Client und Server) verwalten. Abhängig von der CA SDM-Konfiguration werden folgende Clients und Server verwendet:

- Konventionelle Konfiguration,
 - Client: Sekundärserver
 - Server: Primärserver
- Konfiguration für erweiterte Verfügbarkeit,
 - Client: Anwendungsserver und Standby-Server
 - Server: Hintergrundserver

Beispiel: Als Systemadministrator haben Sie ein Feld auf der Seite "detail_usp_server.html" von CA SDM hinzugefügt. Jetzt möchten Sie diese Änderung auf den Clients und den Servern synchronisieren. Dieses Beispiel wird im Szenario verwendet, um zu erläutern, wie die Anpassung synchronisiert wird.

Folgendes Diagramm zeigt, wie eine Versionskontrolle der Systemanpassungen auf CA SDM-Servern durchgeführt wird:



Gehen Sie wie folgt vor:

1. [Überprüfen Sie die Voraussetzungen](#) (siehe Seite 599).
2. Nehmen Sie Änderungen in CA SDM vor. Fügen Sie in diesem Beispiel das neue Feld auf der CA SDM-HTML-Seite hinzu.
3. [Ändern Sie die Versionskontrolldatei des Servers](#) (siehe Seite 599).
4. Führen Sie CA SDM auf den Client zurück.
5. [Überprüfen Sie die Anpassungen auf dem Client](#) (siehe Seite 607).

Überprüfen der Voraussetzungen

Überprüfen Sie folgende Voraussetzungen:

- Stellen Sie sicher, dass die Option "ver_ctl" auf den Wert "**Aktualisieren**" festgelegt ist. Wenn ein Versionsunterschied erkannt wird, dann wird versucht, die betroffenen Komponenten auf dem Client zu aktualisieren. Wenn das Upgrade erfolgreich ist, bleibt die Client-Verbindung mit dem Server bestehen. Anderenfalls wird die Verbindung getrennt. Weitere Informationen zur Option "ver_ctl" finden Sie in der Online-Hilfe.
- Stellen Sie sicher, dass die Datei "server_secondary_custom.ver" im Verzeichnis "\$NX_ROOT\site\mods" vom Primärserver oder Hintergrundserver (abhängig von der CA SDM-Konfiguration) erstellt wird. Alle Anpassungen einer Versionskontrollkomponente müssen in dieser Datei vorgenommen werden. Wenn die Datei nicht vorhanden ist, stellen Sie sicher, dass Sie sie am gleichen Speicherort erstellen.

Ändern der Versionskontrolldatei des Servers

Nachdem Sie die Anpassung abgeschlossen haben (zum Beispiel ein Feld auf der HTML-Seite hinzugefügt), müssen Sie die Versionskontrollkomponenten der Versionskontrolldatei des Servers hinzufügen oder aktualisieren. Eine Versionskontrollkomponente kann eine Datei, ein Verzeichnis oder die Umgebungsvariablendatei "client_nx.env" darstellen.

Gehen Sie wie folgt vor:

1. Melden Sie sich abhängig von Ihrer CA SDM-Konfiguration auf folgendem Server an:
 - Konventionell: Primärserver
 - Erweiterte Verfügbarkeit: Hintergrundserver
2. Wechseln Sie in das folgende Verzeichnis:
`$NX_ROOT\site\mods`
3. Öffnen Sie die Datei "server_secondary_custom.ver".

4. Fügen Sie folgende Komponenten hinzu:

```
[ MY_USP_SERVERS_HTML ]  
directory="$NX_ROOT/site/mods/www/html/web/analyst/Analyst"  
filename="detail_usp_servers.html"  
version="2.0 , 20121119"  
o_mode="RW"  
g_mode="RW"  
w_mode="RW"  
file_ctl
```

Hinweis: Weitere Informationen über das Hinzufügen oder Aktualisieren von Versionskontrollkomponenten finden Sie im Abschnitt ["Versionskontrollkomponenten"](#) (siehe Seite 600).

5. Speichern Sie die Datei "server_secondary_custom.ver".

Die Versionskontrollkomponente wird der Versionskontrolldatei hinzugefügt.

Versionskontrollkomponenten

So definieren Sie eine neue Komponente,

- Verwenden Sie folgende Syntax. Elemente in *Kursivschrift* entsprechen Daten, die Sie bereitstellen. Die Parameter *component-name* und Versionsparameter sind immer erforderlich. Andere Parameter sind abhängig vom Wert für "*control-type*" erforderlich. Alle anderen Elemente sind Schlüsselwörter, die Sie genau wie in folgenden Beispiel gezeigt eingeben müssen:

```
[ component-name ]  
version = "x.x, yyyymmdd"  
control-type  
filename = "filename"  
directory = "directory"  
link = "link-directory"  
source = "source-directory"  
effectivity = "effect-spec"  
checksum  
min_release = "release"  
max_release = "release"  
component_type = "file-type"
```

```
o_mode = "owner-mode"
```

```
g_mode = "group-mode"
```

```
w_mode = "world-mode"
```

Hinweis: Weitere Informationen zu den Parametern finden Sie unter "[Versionskontrollparameter](#)" (siehe Seite 601)". Weitere Informationen zur Struktur und Syntax der Versionskontrolldateien finden Sie in den ".ver"-Dateien, die im Verzeichnis "\$NX_ROOT/site" installiert sind. Diese Dateien enthalten nützliche Kommentare und Beispielseinstellungen, die Ihnen helfen können.

So aktualisieren Sie einen vorhandenen Komponenteneintrag,

- Ändern Sie den Parameter. Ändern Sie zum Beispiel die Versionsnummer.

So entfernen Sie das Steuerelement aus einer Komponente,

- Bearbeiten Sie die Komponente folgendermaßen:

```
! uncontrol component-name
```

Versionskontrollparameter

Für die Versionskontrolle gelten die folgenden Parameter:

[component-name]

Gibt den Namen eines Elements unter Versionskontrolle an. Der Name muss eindeutig sein und in eckigen Klammern angegeben werden. Bei *component-name* muss nicht auf Groß- und Kleinschreibung geachtet werden. Dieser Parameter ist für eine Komponentendefinition erforderlich.

version="x.x. yyymmdd"

Gibt eine Versionsnummer (x.x) und ein Datum (yyymmdd) an, die die Version der Komponente definieren. Dieser Parameter ist erforderlich und muss in Anführungszeichen eingeschlossen werden. Die Versionskontrolle prüft die Version einer Komponente, indem sie die Versionsnummer und das Datum auf dem Server mit der Versionsnummer und dem Datum auf dem Client vergleicht. Sowohl die Versionsnummer als auch das Datum müssen übereinstimmen, damit die Komponente als synchron zwischen Client und Server betrachtet wird. Wenn die Prüfsummeneigenschaft aktiviert ist, wird die Datei vor ihrer Aktualisierung durch eine Prüfsummenverifizierung geprüft.

control-type

Gibt den Typ der Versionskontrolle für diese Komponente an. Die folgenden Einstellungen sind für "Kontrolle-Typ" gültig:

Einstellung	Beschreibung
dir_ctl	Gibt an, dass die Komponente ein Verzeichnis darstellt. Sie müssen den Verzeichnisparameter liefern, um den Pfad zum Verzeichnis anzugeben. Sie können auch den Dateinamenparameter angeben, um eine Gruppe von Dateien im Verzeichnis zu filtern. Unterverzeichnisse werden weder unter UNIX noch unter Windows aufgerüstet.
file_ctl	Gibt an, dass die Komponente eine Datei darstellt. Sie müssen den Verzeichnis- und Dateinamenparameter liefern, um den Pfad zur Datei anzugeben.
Nxenv_ctl	Gibt an, dass diese Komponente die Datei "client_nx.env" darstellt, in der interne CA SDM-Umgebungsvariablen gespeichert werden. CA SDM-Versionskontrolle und der Optionsmanager pflegen diese Datei automatisch. Es gibt genau eine nxenv_ctl-Komponente, und ihr Komponentenname muss CLIENT_NXENV lauten.
ver_ctl	Dies ist der Standardkontrolltyp. Er gibt an, dass die Komponente generisch ist; d. h. sie ist nicht mit einem bestimmten externen Objekt verbunden. Mit einer generischen Komponente können Sie eine Versionskontrolle für den Client als Ganzes oder für eine Datei oder ein Verzeichnis zur Verfügung stellen, die bzw. das für eine automatische Aktualisierung zu groß ist. Komponenten mit dem Kontrolltyp „ver_ctl“ können nicht aufgerüstet werden. Ein Versionsunterschied bei einer ver_ctl-Komponente bewirkt einen Abbruch der Clientverbindung, wenn der Server den Modus UPGRADE hat.

filename="filename"

Gibt den Namen einer Datei unter Versionskontrolle an. Dieser Parameter enthält keine Angaben zum Verzeichnis. Er ist für file_ctl-Komponenten erforderlich, ist aber für Komponenten mit Verzeichniskontrolle (dir_ctl) optional. Wenn der Dateinamenparameter zusammen mit Verzeichniskomponenten verwendet wird, fungiert er als Dateimaske, um die mit der dir_ctl-Komponente verbundenen Dateien einzuschränken. Wenn zum Beispiel der Dateiname für eine dir_ctl-Komponente *.README lautet, dann schließt ein Upgrade dieses Verzeichnisses nur Dateien ein, die mit „.README“ enden.

directory="directory"

Gibt den Pfad zum Verzeichnis für dir_ctl-Komponenten oder zu dem Verzeichnis an, das die Datei für file_ctl-Komponenten enthält. Dieser Parameter wird für ver_ctl- und nxenv_ctl-Komponenten ignoriert. Der Verzeichnispfad muss in Anführungszeichen eingeschlossen werden und kann Verweise auf Umgebungsvariablen enthalten, wobei \$ vorangestellt werden muss.

Note: Um Unterverzeichnisse im Pfadnamen zu trennen, verwenden Sie immer den Schrägstrich (nicht den umgekehrten Schrägstrich), auch auf einem Windows-Server.

link="link-directory"

Gibt ein Link-Verzeichnis auf dem Client im gleichen Format an, das zuvor für Verzeichnisparameter beschrieben wurde. Dieser Parameter ist optional für file_ctl- und dir_ctl-Komponenten und wird für ver_ctl- und nxenv_ctl-Komponenten ignoriert. Wenn er angegeben wird, dann wird bei einem Upgrade auf einem Linux-Client ein symbolischer Link ins Link-Verzeichnis gestellt. Dieser verweist auf die eigentliche Datei, die in die im Verzeichnisparameter angegebene Position kopiert wurde. Bei einem Upgrade auf einem Windows-Client wird die eigentliche Datei sowohl in den Link- als auch in den Verzeichnisspeicherort kopiert.

source="source-directory"

(Optional) Gibt ein anderes Verzeichnis auf dem Server an, aus dem der Server Dateien zur Bereitstellung abrufen kann. Dieser Parameter hat das gleiche Format, das zuvor für den Verzeichnisparameter beschrieben wurde. Er ist nützlich, wenn die dem Client bereitzustellenden Dateien sich von den gleichen Dateien im Verzeichnisspeicherort auf dem Server unterscheiden. Dieser Parameter wird verwendet, um dem Server mitzuteilen, dass die Datei aus dem *source-directory* abgerufen und an dem im Verzeichnisparameter angegebenen Speicherort auf dem Client bereitgestellt werden soll. Der Verzeichnisparameter ist erforderlich, wenn Sie den Quellparameter angeben.

effectivity="effect-spec"

(Optional) Gibt an, ob der Client diese Komponente erhalten soll. Hiermit können Sie den Download zu einigen Clients ausschließen. Wenn ein Client in die Effektivitätsangabe nicht eingeschlossen ist, erhält er die Komponente nicht. Wenn dieser Parameter nicht angegeben wird, erhalten alle Clients die Komponente. Die Effektivitätsangabe verwendet die folgenden Symbole:

+ (Pluszeichen)

Gibt an, dass eine Clientgruppe hinzugefügt werden soll.

- (Minusvorzeichen)

Gibt an, dass eine Clientgruppe ausgeschlossen werden soll.

Die folgenden Clientgruppen sind gültig:

- SUN4SOL
- AIX
- LINUX
- LINUX390
- HP
- WINDOWS_CLIENTS
- UNIX_CLIENTS

Zum Beispiel gibt Folgendes an, dass nur UNIX-Clients die Dateien erhalten:
effectivity = "+ UNIX_CLIENTS"

checksum

Weist die Komponente zur Aktualisierung an, wenn die Prüfsumme der Komponente auf dem Client nicht mit der entsprechenden Prüfsumme auf dem Server übereinstimmt. Wenn der Parameter für ein Verzeichnis gilt, wird die Prüfsumme auf jede Datei angewandt.

min_release="release" und max_release="release"

Gibt den ältesten und neuesten Client an, an den diese Komponente verteilt werden soll. Versionen werden durch Anweisungen in der Datei "server_default.ver" definiert. Diese Parameter haben folgende Form, wobei Gaxx die Version angibt und die folgenden Werte mit der Version verbundene „genlevels“ sind.

! Release GA50 50MvV000900 50w7T000900
! Release GA45 45Mw000900 50wTT000900

Die Reihenfolge gibt an, dass GA50 neuer ist als GA45.

component_type

Gibt den Typ der verwendeten Komponente an. Folgende Typen von Komponenten werden verwendet:

Einstellung	Beschreibung
file	Dies ist der Standardkomponententyp. Er gibt an, dass auf den Client zu kopierende Dateien direkt von dem Speicherort auf dem Server abgerufen werden, der im Verzeichnisparameter angegeben ist.

Einstellung	Beschreibung
exe_file	Gibt an, dass auf den Client zu kopierende Dateien von einem Speicherort auf dem Server abgerufen werden, der vom Betriebssystem des Client abhängt, zum Beispiel: ■ windows (Windows) ■ sun4Sol (Solaris) ■ hp (HP-UX) ■ aix (AIX) ■ linux (Linux) ■ linux390 (Linux390) Die Speicherorte für diese Unterverzeichnisse hängen von der Einstellung des Verzeichnisparameters ab. Wenn dieser Parameter eingestellt ist, befinden sich Unterverzeichnisse unter dem angegebenen <i>Verzeichnis</i>. Andernfalls befinden sie sich unter dem Verzeichnis "bin" des Installationshauptverzeichnisses von CA SDM.

o_mode="owner-mode"

Gibt die Dateizugriffsberechtigungen für den Eigentümer der Datei an.

g_mode="group-mode"

Gibt Dateizugriffsberechtigungen für Anwender in der Dateieigentümergruppe an (wird nur für UNIX-Clients verwendet).

w_mode="world-mode"

Gibt Dateizugriffsberechtigungen für Anwender an, die nicht in der Dateieigentümergruppe enthalten sind (wird nur für UNIX-Clients verwendet).

Mit den drei mode-Parametern können verschiedene Versionen derselben ausführbaren Datei auf dem Server verwaltet werden. Sie geben Zugriffssteuerungen für die Datei an, wenn diese auf den Client kopiert wird. Diese Parameter werden nur während eines Upgrades verwendet. Sie bestehen aus einem bis drei Zeichen, die folgende Bedeutung haben:

Einstellung	Beschreibung
R	Gelesen
W	Schreiben
X	Ausführen

PC-Clients ignorieren die Schreib- und Ausführungsberechtigungen.

Sie können jede Kombination eines oder mehrerer Dateizugriffsmodi angeben. Auf UNIX-Clients erhält die Datei den angegebenen Zugriffsmodus. Auf PC-Clients ist die Datei beschreibbar oder schreibgeschützt, abhängig davon, ob w_mode angegeben wurde.

Neustarten von CA SDM auf dem Client.

Sie starten CA SDM auf den Client-Servern neu, um die Versionskontrolldateien des Clients mit den Anpassungen zu aktualisieren.

Hinweis: Wählen Sie "Start" > "Einstellungen" > "Systemsteuerung" > "Verwaltung" > "Dienste". Klicken Sie mit der rechten Maustaste auf den CA SDM-Server, und wählen Sie "Starten", um einen Server zu starten oder neu zu starten.

Gehen Sie wie folgt vor:

1. Starten Sie für die konventionelle Konfiguration den sekundären Server neu.
2. Führen Sie für die Konfiguration für erweiterte Verfügbarkeit folgende Schritte aus:
 - a. Starten Sie alle Standby-Server neu.
 - b. [Wählen Sie einen Anwendungsserver aus, der wenig aktiv ist](#) (siehe Seite 36).
 - c. Starten Sie den Anwendungsserver neu, der wenig aktiv ist.
 - d. [Halten Sie den anderen Anwendungsserver an](#) (siehe Seite 37).
 - e. Starten Sie den Anwendungsserver.
 - f. Führen Sie die Schritte "d" und "e" für weitere Anwendungsserver aus.

Der Client stellt eine Verbindung mit dem Server her, um eine Liste der gesteuerten Komponenten zu senden. Der Server vergleicht die Liste mit seiner eigenen Hauptliste. Die betroffenen Komponenten auf dem Client werden aktualisiert.

Auswählen des Anwendungsservers, der wenig aktiv ist

Sie wählen einen Anwendungsserver mit der geringsten Anwenderaktivität aus. Führen Sie folgenden Befehl auf jedem Anwendungsserver aus, um den Server auszuwählen, der keine oder nur wenige aktive Sitzungen hat.

```
pdm_webstat
```

Hinweis: Dieser Befehl erfasst nicht die SOAP- oder REST-Webservice-Sitzungen.

Anhalten der anderen Anwendungsserver

Sie benachrichtigen alle aktiven Anwender auf einem Anwendungsserver darüber, auf den am wenigsten aktiven Anwendungsserver zu wechseln, bevor Sie ihn anhalten. Stellen Sie sicher, dass Sie den Anwendungsserver, der am wenigsten aktiv ist, neu gestartet haben, bevor Sie alle Anwender dorthin verschieben.

Gehen Sie wie folgt vor:

1. (Empfohlen) Fordern Sie alle aktiven Support-Automatisierung-Analysten auf dem Anwendungsserver, den Sie anhalten möchten, dazu auf, ein Ticket in CA SDM mit ihren Sitzungsinformationen zu erstellen. Dieser Vorgang stellt sicher, dass die Sitzungsinformationen nicht verloren gehen. Zum Beispiel ist der Support-Automatisierung-Analyst in einer Sitzung mit einem Kunden, um einen Hardware-Issue zu lösen. In diesem Fall kann der Support-Automatisierung-Analyst einen Issue in CA SDM mit den Sitzungsinformationen erstellen, bevor der Anwendungsserver heruntergefahren wird.
2. Senden Sie eine Benachrichtigung (zum Beispiel eine E-Mail-Benachrichtigung) an alle aktiven Anwender auf dem Anwendungsserver, in der die Anwender aufgefordert werden, zum Anwendungsserver, der am wenigsten aktiv ist und den Sie gerade neu gestartet haben, zu wechseln. Diese Benachrichtigung kann die Details des aktualisierten Anwendungsservers enthalten.
3. Führen Sie folgenden Befehl auf dem Anwendungsserver aus:

```
pdm_server_control [-h] -q interval -s server_name
```

-h

Zeigt die Hilfeseite an.

-q interval -s server_name

Benachrichtigt einen lokalen Anwendungsserver oder einen Remote-Anwendungsserver, eine Stilllegung in einem angegebenen Zeitintervall durchzuführen. Dieses Intervall ist die Anzahl der Sekunden, bevor der Server offline geschaltet wird. Wenn man diese Option ohne server_name verwendet wird, dann wird der lokale Server zur Stilllegung benachrichtigt. Diese Option kann für einen Hintergrundserver oder einen Standby-Server nicht verwendet werden.

Eine Pop-up-Meldung wird allen aktiven Anwendern auf dem Anwendungsserver angezeigt. Die Meldung weist auf das Herunterfahren des Servers und auf die verbleibende Zeit bis zum Herunterfahren hin. Die Anwender müssen ihre Arbeit speichern und sich innerhalb dieser Zeit abmelden. Der Anwendungsserver wird nach der angegebenen Zeit angehalten. Die Anwender melden sich auf dem anderen Anwendungsserver an, um ihre Arbeit fortzusetzen. Der Support-Automatisierung-Analyst kann sich auf das Ticket beziehen und seine Arbeit fortsetzen.

Der Anwendungsserver wird erfolgreich angehalten.

Überprüfen der Anpassungen auf dem Client

Sie überprüfen die Versionskontrolldatei auf dem Client, um zu überprüfen, ob alle Anpassungen synchronisiert wurden.

Gehen Sie wie folgt vor:

1. Melden Sie sich abhängig von Ihrer CA SDM-Konfiguration auf folgendem Client an:
 - Konventionell: Sekundärserver
 - Erweiterte Verfügbarkeit: Standby-Server und Anwendungsserver
2. Öffnen Sie die Datei "stdlog" vom folgenden Speicherort:
`$NX_ROOT\log`
3. Finden Sie heraus, ob alle auf dem Server vorgenommenen Anpassungen auf dem Client angewendet wurden.

Kapitel 16: Verwalten von Konfigurationselementen

Dieses Kapitel enthält folgende Themen:

[Verwenden der Web-Schnittstelle](#) (siehe Seite 609)
[Configuration Items: Kontakt, Standort und Organisation](#) (siehe Seite 614)
[CI Relationships](#) (siehe Seite 617)
[Versionskontrolle](#) (siehe Seite 626)
[Anzeigen von CI-Attributen in anderen CA-Produkten](#) (siehe Seite 654)
[Verwenden des CMDBf-Viewers](#) (siehe Seite 655)
[CMDB Visualizer](#) (siehe Seite 655)
[Hinzufügen von ermittelten Assets](#) (siehe Seite 659)
[Asset- und CI-Markierungen](#) (siehe Seite 660)
[Abstimmung von CIs](#) (siehe Seite 661)
[Verwalten bereitgestellter Transaktionen](#) (siehe Seite 682)
[CA CMDB-Datenwartung](#) (siehe Seite 707)
[Configuration Audit and Control Facility \(CACF\)](#) (siehe Seite 722)

Verwenden der Web-Schnittstelle

Je nach Ihrer Rolle können Sie unter Verwendung der folgenden Funktionen Anwender- und Administrationsaufgaben auf Configuration Items (CIs) ausführen:

- Sie können über Scoreboards Anwenderprozesse ausführen und CIs und Relationen zwischen CIs verwalten.
- Die Registerkarte "Administration" dient der Durchführung von Administrationsaufgaben in Zusammenhang mit CIs und Relationen zwischen CIs.
- CMDB Visualizer dient der Durchführung von Anwender- und Administrationsaufgaben zur Anzeige von CIs und Relationen zwischen CIs

Weitere Informationen:

[Anzeigen von Configuration Items](#) (siehe Seite 610)
[Erstellen von Configuration Items](#) (siehe Seite 610)
[Aktualisieren von Configuration Items](#) (siehe Seite 611)
[Zuordnen eines Wartungsfensters zu einem CI](#) (siehe Seite 612)
[Anzeigen von zugeordneten Change-Fenstern](#) (siehe Seite 612)
[Anzeigen des Configuration Item-Verlaufs](#) (siehe Seite 613)
[Deaktivieren von Konfigurationselementen](#) (siehe Seite 613)
[Neu aktivieren von Konfigurationselementen](#) (siehe Seite 614)

Anzeigen von Configuration Items

Mit dem Scoreboard können Sie ein Configuration Item öffnen und Informationen darüber anzeigen.

So öffnen Sie ein Configuration Item und zeigen es an:

1. Klicken Sie im Scoreboard auf "Suchen" > "Configuration Items".
Das Configuration Item-Suchfenster wird angezeigt.
2. Geben Sie die Suchkriterien ein, und klicken Sie auf "Suchen".
Die Configuration Item-Liste erscheint und zeigt eine Liste der Suchergebnisse an.
3. (Optional) Klicken Sie auf ein Configuration Item in der Spalte "Name", um es zu öffnen und detaillierte Informationen anzuzeigen.
Es werden Configuration Item-Details angezeigt.

Hinweis: Nachdem Sie ein CI erstellt haben, zeigt die CI-Detailseite einige identifizierende Attribute nicht an, wenn sie unbeschrieben sind (keinen Wert enthalten) und nicht für die CI-Familie gelten. Allerdings werden identifizierende Attribute mit nicht-leeren Werten immer angezeigt.

Erstellen von Configuration Items

Mit dem Scoreboard können Sie ein Configuration Item erstellen.

So erstellen Sie ein Configuration Item

1. Klicken Sie im Scoreboard auf "Datei" > "Neues Configuration Item".
Die Seite "Neues Configuration Item erstellen" wird angezeigt.
2. Geben Sie im Feld "Name" einen eindeutigen Namen für das Configuration Item ein.
3. Geben Sie im Feld "Klasse" eine Klasse für das Configuration Item ein, oder klicken Sie auf das Suchsymbol über dem Feld, um eine Klasse zu suchen.
4. Füllen Sie die verbleibenden Felder aus, die auf das neue Configuration Item zutreffen.

Hinweis: Für das Erstellen eines Configuration Item werden nur die Werte "Name" und "Klasse" benötigt.

5. Klicken Sie auf "Fortsetzen".

Auf der Seite "Neues Configuration Item erstellen" werden zusätzliche Registerkarten und Felder angezeigt.

6. Geben Sie bei Bedarf Daten in die entsprechenden Felder auf der Registerkarte "Attribute" ein.

Die Attribute auf der Registerkarte werden durch die Familie der Klasse bestimmt, die Sie für das Configuration Item ausgewählt haben. Welche Informationen Sie hier eintragen, hängt von Ihren Geschäftsprozessen und den Informationen ab, die Sie für ein Configuration Item speichern und anzeigen möchten.

7. Klicken Sie auf "Speichern".

Eine Meldung wird angezeigt, die die Erstellung des Configuration Items bestätigt.

Aktualisieren von Configuration Items

Mit dem Scoreboard können Sie ein Configuration Item ändern.

So ändern Sie ein Configuration Item:

1. Suchen Sie im Scoreboard das Configuration Item, und öffnen Sie es.

Die Seite "Configuration Item – Detail" wird angezeigt.

2. Klicken Sie auf "Bearbeiten".

Die Seite "Configuration Item aktualisieren" wird angezeigt.

3. Ändern Sie die Informationen des Configuration Items, indem Sie die entsprechenden Registerkarten auf der Seite auswählen und neue Daten in die Felder eingeben. Klicken Sie auf "Speichern".

Eine Meldung wird angezeigt, die die Änderung des Configuration Items bestätigt.

Hinweis: Wenn ein Configuration Item über die -a-Option aktualisiert wird, werden das Datum der letzten Änderung sowie der entsprechende Benutzer in der Configuration Item-Liste angezeigt, auch wenn keine Attribute geändert wurden. Diese Aktualisierung wird stets vorgenommen, egal ob ein Configuration Item in der Benutzeroberfläche bearbeitet (und ohne Änderungen gespeichert) oder mit GRLoader aktualisiert wurde.

Zuordnen eines Wartungsfensters zu einem CI

Um den Wartungszugriff auf ein CI zu steuern, können Sie ein CI einem oder mehreren nichtglobalen Wartungsfenstern zuordnen.

So ordnen Sie einem CI ein Wartungsfenster zu:

1. Navigieren Sie zur Detailseite des CI.
2. Klicken Sie auf die Registerkarte "Wartungsfenster".
Die Liste "Wartungsfenster" wird angezeigt.
3. Klicken Sie auf "Wartungsfenster aktualisieren".
Die Wartungsfenster-Such-Seite wird angezeigt.
4. Geben Sie Informationen für erforderliche Wartungsfenster ein.
5. Klicken Sie auf "Suchen".
Die Seite "Verfügbare Fenster" wird angezeigt.
6. Verschieben Sie wie gewünscht die benötigten Wartungsfenster aus der Liste "Verfügbare Änderungsfenster" in die Liste "Zugeordnete Änderungsfenster".
7. Klicken Sie auf "OK".
Das CI, die Change-Fenster, und neue Fensterzuordnungen werden gespeichert.

Anzeigen von zugeordneten Change-Fenstern

Um festzulegen, auf welche Weise ein CI während bestimmter Zeiträume betroffen sein kann, können Sie die Wartungsfenster anzeigen, die einem CI zugeordnet sind.

So zeigen Sie die einem CI zugeordneten Change-Fenster an:

1. Navigieren Sie zur Detailseite des CI.
2. Klicken Sie auf die Registerkarte "Wartungsfenster".
Die zugeordneten Wartungsfenster werden gezeigt.

Anzeigen des Configuration Item-Verlaufs

Sie können den Verlauf eines Configuration Item anzeigen.

So zeigen Sie den Verlauf eines Configuration Item an

1. Suchen Sie nach dem Configuration Item, und öffnen Sie es.

Die Seite "Configuration Item – Detail" wird angezeigt.

2. Klicken Sie auf die Registerkarte "Versionskontrolle".

Die Seite "Versionskontrolle" wird angezeigt.

3. Klicken Sie auf "Protokoll anzeigen".

Der Verlauf des Configuration Item wird aufgelistet.

Hinweis: "Protokoll anzeigen" ignoriert die Auswahl im linken Bereich.

Deaktivieren von Konfigurationselementen

Wenn ein Configuration Item nicht mehr verwendet wird, können Sie seine Details bearbeiten, um es zu deaktivieren. Durch einen inaktiven Status wird das Configuration Item aus der Configuration Item-Liste auf dem Scoreboard entfernt. Sie können kein Configuration Item löschen.

Hinweis: Wenn Sie eine Familie oder Klasse deaktivieren, hat dies keinen Einfluss auf vorhandene CIs in dieser Familie oder Klasse. Es bedeutet lediglich, dass in dieser Familie oder Klasse keine neuen CIs mehr erstellt werden können.

So deaktivieren Sie ein Konfigurationselement:

1. Suchen Sie nach dem Configuration Item, und öffnen Sie es.

Die Seite "Configuration Item – Detail" wird angezeigt.

2. Klicken Sie auf "Bearbeiten".

Die Seite "Configuration Item aktualisieren" wird angezeigt.

3. Wählen Sie in der Dropdown-Liste "Aktiv" die Option "Inaktiv" aus. Klicken Sie auf "Speichern".

Ein Meldungsfenster wird angezeigt, das die Statusänderung bestätigt. Das Konfigurationselement wird nicht länger in der Liste der aktiven Konfigurationselemente angezeigt. Das Konfigurationselement erscheint weiterhin in allen bestehenden Beziehungen, bis die Beziehungen deaktiviert werden.

Neu aktivieren von Konfigurationselementen

Wenn Sie ein inaktives Konfigurationselement benötigen, können Sie es neu aktivieren.

So aktivieren Sie ein Konfigurationselement neu:

1. Suchen Sie nach dem Configuration Item, und öffnen Sie es.
Die Seite "Configuration Item – Detail" wird angezeigt.
2. Klicken Sie auf "Bearbeiten".
Die Seite "Configuration Item aktualisieren" wird angezeigt.
3. Wählen Sie "Aktiv" in der Drop-down-Liste "Aktiv" aus. Klicken Sie auf "Speichern".
Ein Meldungsfenster wird angezeigt, das die Statusänderung bestätigt. Das Konfigurationselement wird in der Liste der aktiven Konfigurationselemente angezeigt.

Configuration Items: Kontakt, Standort und Organisation

Eine CA CMDB-Installation kann für *Basisobjekte* folgende CIs definieren: Kontakte, Lokationen und Organisationen. Diese Configuration Items können entsprechend verwaltet werden. Zudem können ggf. Beziehungen mit anderen CIs erstellt werden. Bei einigen Kunden unterstützt dieses Modell den Configuration Management-Prozess besser, als wenn Basisobjekte nur als CI-Attribute bereitgestellt werden.

Weitere Informationen:

[Erstellen eines CI auf der Grundlage eines Basisobjekts](#) (siehe Seite 614)

[Wählen eines Basisobjekts für ein CI](#) (siehe Seite 615)

[Bearbeiten von Configuration Item-Details für ein Basisobjekt](#) (siehe Seite 616)

[Bearbeiten von CI-Attributen für ein Basisobjekt](#) (siehe Seite 616)

[Erstellen eines Basisobjekt-CI mit Hilfe von GRLoader](#) (siehe Seite 617)

Erstellen eines CI auf der Grundlage eines Basisobjekts

Mit dem Scoreboard können Sie ein Configuration Item aus einem Basisobjekt erstellen.

So erstellen Sie ein CI aus einem Basisobjekt:

1. Wählen Sie unter "Datei" die Option "Neues Configuration Item" aus.
Die Seite "Neues Configuration Item erstellen" wird angezeigt.

2. Füllen Sie die verschiedenen Felder für das CI aus. Name und Klasse sind erforderlich. Klicken Sie auf "Fortsetzen".

Hinweis: Die allgemeinen CI-Attribute Hostname, Seriennummer, MAC-Adresse und DNS-Name sind irrelevant für ein Configuration Item für ein Basisobjekt.

Die Seite "Neues Configuration Item erstellen" wird angezeigt.

3. Klicken Sie auf die Verknüpfung des Basisobjekts, um das Objekt zu definieren, das dieses CI darstellt.
4. Wählen Sie das Objekt. Sie können nach einem bereits bestehenden Objekt suchen oder auf "Neu erstellen" klicken, um ein Objekt zu erstellen. Wenn Sie ein Objekt erstellen möchten, klicken Sie auf "Speichern", um fortzufahren.

Das ausgewählte Objekt wird oben auf der Seite "Configuration Item-Details" angezeigt.

5. Klicken Sie auf "Speichern".

Die Hauptattribute des ausgewählten Objekts werden auf der Seite "Configuration Item – Detail" auf der Registerkarte "Attribute" angezeigt.

Wählen eines Basisobjekts für ein CI

Sie können ein Basisobjekt für ein Configuration Item wählen.

So wählen Sie ein Basisobjekt für ein CI:

1. Wählen Sie ein CI in der Familie des Basisobjekts ("Kontakt", "Standort" oder "Organisation").

Die Seite "Configuration Item – Detail" wird angezeigt.

2. Klicken Sie auf "Bearbeiten".

Die Seite "Configuration Item aktualisieren" wird angezeigt.

3. Füllen Sie im oberen Abschnitt die erforderlichen Felder für das Basisobjekt aus. Sie können direkt einen Wert eingeben oder auf das Lupensymbol klicken, um nach dem Objekt zu suchen. Wenn Sie beispielsweise einen Kontakt suchen, füllen Sie eines oder mehrere Suchfelder im Fenster "Kontaktsuche" aus, und klicken Sie auf "Suchen". Wählen Sie anschließend einen Kontakt aus der angezeigten Liste.

4. Klicken Sie auf "Speichern".

Wenn das ausgewählte Objekt bereits durch ein anderes CI in derselben Familie dargestellt wird, wird eine Fehlermeldung angezeigt. Sie müssen ein anderes Objekt auswählen, bevor Sie das CI ändern können.

Bearbeiten von Configuration Item-Details für ein Basisobjekt

Sie können die Attribute des Basisobjekts, das durch das CI dargestellt wird, z. B. "Alternative CI-ID" und "Hinweise", auf die gleiche Weise wie auf allen anderen Seiten vom Typ "Configuration Item - Detail" bearbeiten.

So bearbeiten Sie die Attribute des Basisobjekts, das durch das CI dargestellt wird:

1. Wählen Sie ein Configuration Item in der Familie des Basisobjekts.
Die Seite "Configuration Item – Detail" wird angezeigt.
2. Klicken Sie oben auf der Seite auf die Verknüpfung des Objekts.
Die Seite "CI – Detail" wird angezeigt.
3. Klicken Sie auf "Bearbeiten".
Die Seite "Aktualisieren" wird für das Objekt angezeigt.
4. Bearbeiten Sie die Felder wie gewünscht, und klicken Sie auf "Speichern".
Das Fenster "Aktualisieren" wird geschlossen.
Wenn Sie eines der Attribute bearbeitet haben, die in der Registerkarte "Attribute" im Fenster "Configuration Item - Detail" angezeigt werden, wird die Änderung dort erst angezeigt, nachdem das Fenster aktualisiert wurde.

Bearbeiten von CI-Attributen für ein Basisobjekt

Sie können die Configuration Item-Attribute für ein Basisobjekt bearbeiten.

So bearbeiten Sie die Attribute für ein CI:

1. Wählen Sie ein CI in der Familie des Objekts ("Kontakt", "Standort" oder "Organisation").
Die Seite "Configuration Item – Detail" wird angezeigt.
2. Klicken Sie auf "Bearbeiten".
Die Seite "Configuration Item aktualisieren" wird angezeigt.
3. Klicken Sie in der Registerkarte "Attribute" auf "Bearbeiten".
Die Seite "Aktualisierung" wird angezeigt.
4. Bearbeiten Sie die Felder wie gewünscht, und klicken Sie auf "Speichern".
Das Fenster "Aktualisieren" wird geschlossen.
5. Klicken Sie auf "Speichern".
Das Fenster "CI - Detail" zeigt das bearbeitete CI an.

Erstellen eines Basisobjekt-CI mit Hilfe von GRLoader

Sie können GRLoader verwenden, um ein Basisobjekt-CI anhand eines bestehenden Basisobjekts zu erstellen.

So erstellen Sie mit Hilfe von GRLoader ein Basisobjekt-CI anhand eines bestehenden Basisobjekts:.

1. Erstellen Sie den benötigten XML-Code mit folgenden Daten:

- CI Name
- Familie
- Klasse

2. Übertragen Sie den XML-Code.

Das Basisobjekt wird erstellt. Der GRLoader zeigt an, das ein CI gelesen und eingefügt worden ist.

Beispiel: Erstellen eines CI aus einem vorhandenen Kontakt

Im folgenden Beispiel wird ein CI aus dem vorhandenen Kontakt **Gibbs, Keith** erstellt.

```
<GRLoader>
<ci>
  <name>Gibbs, Keith</name>
  <family>Kontakt</family>
  <class>Techniker</class>
  <base_contact>Gibbs, Keith</base_contact>
</ci>
</GRLoader>
```

CI Relationships

Die Funktionen von CA SDM hängen von den Beziehungen zwischen Configuration Items ab. CI Beziehungen besitzen die folgenden Merkmale:

- Der *Beziehungstyp* definiert, wie zwei Configuration Items in Beziehung stehen.
- Hierarchische Beziehungstypen werden als *Übergeordnetes/Untergeordnetes Element* gepaart. Zum Beispiel ist A (übergeordnetes Element) *Host für* B; B (untergeordnetes Element) wird von A *gehostet*.
- Nichthierarchische Beziehungstypen werden als *Peer-to-Peer* definiert. Zum Beispiel *ist verbunden mit*, welcher in jeder Richtung gleich ist.

Sie können durch Verwendung der Registerkarte "CMDB-Beziehungen" folgende Beziehungsfunktionen vornehmen:

- Anzeigen von aktiven oder inaktiven Beziehungen durch Suchen im "Aktiv?"- Feld.
- In der "CI-Beziehungen - Liste" können Sie auf eine beliebige Verknüpfungen für eine Beziehung klicken, um deren Seite "CI-Beziehung - Detail" zu starten.

Weitere Informationen:

[CI-Beziehungstypen](#) (siehe Seite 618)

[Erstellen eines Beziehungstyps](#) (siehe Seite 619)

[Verwalten von CI-Beziehungen](#) (siehe Seite 620)

[Erstellen von CI-Beziehungen](#) (siehe Seite 620)

[Anzeigen von Beziehungen für ein CI](#) (siehe Seite 621)

[Deaktivieren von CI-Beziehungen](#) (siehe Seite 621)

[Neuaktivieren einer CI-Beziehung](#) (siehe Seite 622)

[Deaktivieren von CI-Beziehungen \(Listebearbeitung\)](#) (siehe Seite 622)

[Deaktivieren von CI-Beziehungen mit Hilfe von GRLoader](#) (siehe Seite 623)

[Erneutes Aktivieren von CI-Beziehungen mit Hilfe von GRLoader](#) (siehe Seite 624)

[Löschen von CI-Beziehungen aus der Datenbank](#) (siehe Seite 625)

[CI-Beziehungs-Verlauf und -Vergleich](#) (siehe Seite 626)

CI-Beziehungstypen

CA SDM bietet eine Liste mit vordefinierten Beziehungstypen, die zum Beschreiben einer Beziehung oder Zuordnung von CIs benutzt werden kann. Wie die Beziehung angegeben wird, hängt davon ab, auf welchem CI sich konzentriert wird. Zum Beispiel *unterstützt* ein übergeordnetes Element ein untergeordnetes CI, aber das untergeordnete Element *wird unterstützt vom* übergeordneten Element. Diese unterschiedlichen Angaben beziehen sich auf dieselbe Beziehung, und der Beziehungstyp, den Sie sehen, hängt davon ab, ob Sie eine Beziehung: "Übergeordnet -> Untergeordnet" oder eine Beziehung: "Übergeordnet -> Untergeordnet" anzeigen.

Hinweis: Weitere Informationen über die von CA CMDB bereitgestellten Beziehungstypen finden Sie im *technischen CA CMDB-Referenzhandbuch*.

Erstellen eines Beziehungstyps

Sie können Beziehungstypen erstellen und sie für das Erstellen und Aktualisieren von Beziehungen verfügbar machen.

So erstellen Sie einen Beziehungstyp:

1. Erweitern Sie in der Registerkarte "Administration" im linken Ausschnitt den Ordner CA CMDB.
2. Klicken Sie auf "CI-Beziehungstypen".

Im rechten Fensterbereich wird die CI-Beziehungstypen-Liste angezeigt.

3. Klicken Sie auf "Neu erstellen".

Die Seite "Neuen CI-Beziehungstyp erstellen" wird angezeigt.

4. Füllen Sie die folgenden Felder aus:

Bezeichnung der Beziehung zwischen Anbieter und Abhängigem

Bezeichnet die Beziehung zwischen dem Anbieter und dem Abhängigen. Dies ist der Name, der in der Liste der Beziehungstypen angezeigt wird. Beispiele für Beziehungen zwischen dem Anbieter und dem Abhängigen wären "wartet" oder "verwaltet".

Bezeichnung der Beziehung zwischen Abhängigem und Anbieter

Bezeichnet die Beziehung zwischen dem Abhängigen und dem Anbieter. Dies ist der Name, der in der Liste der Beziehungstypen angezeigt wird. Beispiele für Beziehungen zwischen dem Abhängigen und dem Anbieter wären "wird gewartet" oder "wird verwaltet".

Gleichrangig?

Gibt an, dass die Beziehung nicht über einen Anbieter-CI und einen Abhängigen-CI verfügt, sondern über zwei gleichrangigen CIs besteht. Beispiele für gleichrangige Beziehungen wären "stellt eine Verbindung her zu" und "ist Ausfallsicherung für".

Aktiv?

Macht den Beziehungstyp für die Auswahl in CI-Beziehungen und die Anzeige in Listen verfügbar.

5. Klicken Sie auf "Speichern".

Der Beziehungstyp wird erstellt und Sie können ihn verwenden, um Beziehungen zu erstellen oder zu aktualisieren.

Verwalten von CI-Beziehungen

Die Seite "Configuration Item-Beziehung" enthält alle erforderlichen Einstellungen konzentriert an einer einzelnen Stelle, um die Verwaltung von CI-Beziehungen zu vereinfachen.

Sie können mit Hilfe der Seite die folgenden Funktionen ausführen:

- Umkehren der Beziehung "übergeordnet/untergeordnet" zwischen zwei CIs
Klicken Sie auf "Umkehren", um "Übergeordnetes CI" und "Untergeordnetes CI" für die Beziehung umzukehren. Das Fokus-CI wird geändert. Wenn die umgekehrte Beziehung nicht gültig ist, wird der Inhalt des Felds "Beziehung" mit Klicken auf "Rückgängig machen" gelöscht.
- Festlegen optionaler Felder wie Symbol, Beschreibung und Kosten.
Klicken Sie auf "Optional", um optionale Felder festzulegen.
Wenn ein Symbol nicht angegeben ist, wird automatisch ein eindeutiges Symbol mit dem Präfix **cmdb bmhier:** und einer eindeutigen Nummer generiert, wenn die Beziehung erstellt wird.
Hinweis: Wenn Ihre Installation in CA Network and Systems Management (CA NSM) integriert ist, werden Sie aufgefordert, das CA NSM-Repository und die Kosten anzugeben.

Erstellen von CI-Beziehungen

Sie können Beziehungen ausgehend von einem Fokus-CIs hinzufügen.

So fügen Sie eine Beziehung ausgehend von einem Fokus-CIs hinzu:

1. Wählen Sie das CI, zu dem Sie eine Beziehung hinzufügen möchten.
Die Seite "CI - Detail" wird angezeigt.
2. Klicken Sie auf "Bearbeiten".
Die Seite "CI aktualisieren" wird angezeigt.
3. Klicken Sie auf die Registerkarte "CMDB-Beziehungen" und klicken Sie dann auf "Neu erstellen".
Die Seite "Neue CI-Beziehung erstellen" wird angezeigt.

4. Geben Sie das übergeordnete CI an. Wenn Sie auf das Lupensymbol klicken, können Sie nach dem CI suchen.

Hinweis: Je nach Art der benötigten Beziehung, können Sie auf "Umkehren" klicken, um die Positionen von Anbieter bzw. Abhängige zu tauschen.

5. Geben Sie einen Beziehungstyp an. Wenn Sie auf das Lupensymbol klicken, können Sie nach dem Beziehungstyp suchen.
6. Geben Sie das andere CI an (standardmäßig das abhängige CI). Wenn Sie auf das Lupensymbol klicken, können Sie nach dem CI suchen.
7. Klicken Sie auf "Speichern".

Die Beziehung wird erstellt.

Anzeigen von Beziehungen für ein CI

Sie können Beziehungen für CIs anzeigen.

So zeigen Sie die Beziehungen für ein Configuration Item an.

1. Navigieren Sie zu dem gewünschten Configuration Item.
Die Seite "Configuration Item – Detail" wird angezeigt.
2. Wählen Sie die Registerkarte "CMDB-Beziehungen".
Eine Liste der Beziehungen für das Configuration Item wird angezeigt.

Deaktivieren von CI-Beziehungen

Sie können eine CI-Beziehung deaktivieren, indem Sie den Status auf "Inaktiv" setzen.

So deaktivieren Sie eine Beziehung:

1. Navigieren Sie zu der CI-Detailseite, klicken Sie auf die Registerkarte "CMDB-Beziehungen", und klicken Sie auf "Bearbeiten".
Die Registerkarte "CMDB-Beziehungen" zeigt den Bearbeitungsmodus an.
2. Wählen Sie eine Beziehung aus und klicken Sie auf eine beliebige Verknüpfung in der entsprechenden Zeile.
Die Detailseite "CI-Beziehung" Detail wird angezeigt.
3. Klicken Sie auf "Bearbeiten".
4. Setzen Sie das Attribut "Aktiv?" auf "Inaktiv". Klicken Sie auf "Speichern".
Die Beziehung wurde deaktiviert. Auf der Detailseite "CI-Beziehung" zeigt das Attribut "Aktiv?" den Attributwert "Inaktiv" an.

Neuaktivieren einer CI-Beziehung

Sie können eine gelöschte CI-Beziehung neu aktivieren.

So aktivieren Sie eine gelöschte CI-Beziehung:

1. Navigieren Sie zur Detailseite des CI.
Die Detailseite des CI wird im schreibgeschützten Modus angezeigt.
2. Klicken Sie auf "Bearbeiten".
Die Detailseite des CI wird im Bearbeitungsmodus angezeigt.
3. Klicken Sie auf die Registerkarte "CMDB-Beziehungen".
4. Klicken Sie auf einen Link in einer Zeile, um die zugehörige Detailseite "CI-Beziehungen" aufzurufen.
5. Klicken Sie auf "Bearbeiten".
Die Seite zur Aktualisierung der CI-Beziehungen wird angezeigt.
6. Setzen Sie das Attribut "Aktiv?" auf "Aktiv". Klicken Sie auf "Speichern".
Die Beziehung wird neu aktiviert.

Deaktivieren von CI-Beziehungen (Listenbearbeitung)

Sie können CI-Beziehungen unter Verwendung der Listenbearbeitung deaktivieren.

So deaktivieren Sie CI-Beziehungen:

1. Öffnen Sie in der Registerkarte "Administration" im linken Ausschnitt den Ordner CA CMDB.
Der Ordner CA CMDB wird erweitert, so dass Unterordner angezeigt werden.
2. Klicken Sie auf den Ordner "CI-Beziehungen - Liste".
3. (Optional) Geben Sie Suchfilter an.
4. Klicken Sie auf "Suche".
Im rechten Bereich werden die Beziehungen der Configuration Items angezeigt.
Hinweis: Standardmäßig werden alle Beziehungen angezeigt.
5. Klicken Sie auf die Schaltfläche "In Liste bearbeiten" oben rechts in der Liste.
Die Steuerelemente für "Beziehung in Liste bearbeiten" werden angezeigt.

6. Wählen Sie die Zeile aus, in der sich die Beziehung befindet, die Sie ändern möchten.

Die Zeile wird angezeigt, und die Steuerelemente werden mit den Werten der Beziehung aufgefüllt.

7. Setzen Sie das Attribut "Aktiv?" auf "Inaktiv".

Klicken Sie auf "Speichern", wenn Sie nur die ausgewählte Beziehung deaktivieren möchten oder klicken Sie auf "Alle ändern", um alle Beziehungen in der gefilterten Suche zu deaktivieren.

Deaktivieren von CI-Beziehungen mit Hilfe von GRLoader

Sie können CI-Beziehungen unter Verwendung von GRLoader deaktivieren, indem Sie geeigneten XML-Code übermitteln.

So deaktivieren Sie eine Beziehung unter Verwendung von GRLoader:

1. Erstellen Sie den benötigten XML-Code mit den folgenden Daten unter Verwendung eines Tags "Relation":
 - Übergeordnetes CI
 - Untergeordnetes CI
 - Beziehungstyp
2. Legen Sie für das Flag "delete_flag" den Wert "true" (oder "yes" bzw. 1) fest.
3. Übertragen Sie den XML-Code.

Die CI-Beziehung wird gelöscht.

Hinweis: Weitere Informationen zu GRLoader finden Sie im *technischen CA CMDB-Referenzhandbuch*.

Beispiel: Entfernen einer CI-Beziehung unter Verwendung von GRLoader

Im folgenden XML-Beispiel wird die Beziehung "stellt eine Verbindung her zu" zwischen ci_1 und ci_2 gelöscht.

```
<GRLoader>
  <relation>
    <dependent>
      <name>ci_2</name>
    </dependent>
    <type>stellt eine Verbindung her zu</type>
    <provider>
      <name>ci_1</name>
    </provider>
    <delete_flag>wahr</delete_flag>
  </relation>
</GRLoader>
```

Erneutes Aktivieren von CI-Beziehungen mit Hilfe von GRLoader

Sie können CI-Beziehungen unter Verwendung von GRLoader erneut aktivieren, indem Sie geeigneten XML-Code übermitteln.

So aktivieren Sie eine CI-Beziehung unter Verwendung von GRLoader erneut:

1. Erstellen Sie den benötigten XML-Code mit den folgenden Daten unter Verwendung eines Tags "Relation":
 - Beziehungstyp
 - Untergeordnetes CI
 - Übergeordnetes CI
2. Legen Sie für das Flag "delete_flag" den Wert "false" (oder "no" bzw. 0) fest.
3. Übertragen Sie den XML-Code.

Die CI-Beziehung wird erneut aktiviert.

Hinweis: Weitere Informationen zu GRLoader finden Sie im *technischen CA CMDB-Referenzhandbuch*.

Beispiel: Erneutes Aktivieren einer CI-Beziehung

Im folgenden XML-Beispiel wird die Beziehung "stellt eine Verbindung her zu" zwischen "ci_1" und "ci_2" erneut aktiviert.

```
<GRLoader>
  <relation>
    <dependent>
      <name>ci_2</name>
    </dependent>
    <type>stellt eine Verbindung her zu</type>
    <provider>
      <name>ci_1</name>
    </provider>
    <delete_flag>falsch</delete_flag>
  </relation>
</GRLoader>
```

Löschen von CI-Beziehungen aus der Datenbank

Sie können eine CI Beziehung löschen, so dass diese nicht nur deaktiviert, sondern dauerhaft aus der Datenbank entfernt wird.

So löschen Sie eine Beziehung aus der Datenbank:

1. Navigieren Sie zur CI-Klassenliste.

Die Seite "CI-Beziehungen - Liste" wird angezeigt.

2. Klicken Sie mit der rechten Maustaste auf eine Beziehungszeile und wählen Sie aus dem Kontextmenü den Befehl "Löschen".

Die Beziehung wird aus der Datenbank entfernt.

Achtung: Wenn für die gelöschte Beziehung ein definiertes Symbol vorhanden ist, dann werden alle Beziehung mit dem gleichen Symbol ebenfalls aus der Datenbank gelöscht.

CI-Beziehungs-Verlauf und -Vergleich

Die Registerkarte "Versionskontrolle" zeigt CI-Beziehungen an und ermöglicht Ihnen Folgendes:

- Anzeigen des Beziehungsverlaufs für ein CI in der CMDB. Änderungen an einer Beziehung werden automatisch protokolliert, wenn die Beziehung erstellt, aktualisiert oder gelöscht wird. Sie können alle gegenwärtigen und historischen Beziehungen für ein CI anzeigen.

Hinweis: Beziehungen, die mit früheren Versionen von CA CMDB erstellt wurden, enthalten keine Informationen zum Auditverlauf.

- Vergleichen von Beziehungen bei einem beliebigen Snapshot oder Meilenstein.

Versionskontrolle

Die Versionskontrolle ermöglicht Ihnen die Kontrolle über die IT-Infrastruktur durch Nachverfolgen und Verwalten der Lebenszyklen aller CIs, aus denen sich der autorisierte Status der CMDB zusammensetzt. Versionskontrolle kommt auch bei der Überwachung des Verlaufs eines Objekts zum Einsatz. Die Versionskontrolle bietet folgende Funktionen zur Steuerung der IT-Infrastruktur:

Snapshots

Automatisch für Änderungen aufgenommen, die Sie im Zuge von CI-Aktualisierungen am Wert von Objektaktualisierungen vorgenommen haben., Die Versionskontrolle erstellt einen Snapshot, der den vollständigen Zustand des Hardware-CI aufzeichnet, wenn die Speichergröße eines Computers geändert worden ist. Die Versionskontrolle kann den Snapshot anzeigen und kann zeigen, welche CI-Attribute geändert wurden. Die Versionskontrolle kann es auch mit allen anderen historischen Snapshots dieses CI vergleichen. Sie benötigen diese äußerst wichtigen Informationen, wenn Sie die Auswirkung von Änderungen auf die Verfügbarkeit und Leistungsfähigkeit eines CI verstehen möchten.

Meilensteine

Werden als Snapshots mit besonderem Zweck mit einer anwenderspezifischen Beschriftung wie beispielsweise "Erster Tag", "Produktion" oder "Baseline Januar" aufgezeichnet. Diese Bezeichnungen können zum schnelleren Auffinden spezifischer Snapshots beitragen.

Wichtig! Meilensteine beziehen sich *nicht* auf Change-Spezifikationen, Verifizierungsrichtlinien, verwaltete Change-Zustände und verwaltete Attribute.

Vergleiche

Vergleichen eines CI mit einem anderen CI, das als Standard fungiert. Für den Vergleich kann jedes CI als Standard verwendet werden. Es wird jedoch empfohlen, spezifische CIs als *Standard-CIs* festzulegen. Ein Standard-CI ermöglicht Ihnen die Definition einer Standardkonfiguration, mit der andere Betriebs-CIs in derselben Familie verglichen werden können. Beispielsweise könnte eine Organisation Server groß als Standard-CI bestimmen, um die Attributwerte für diese Art von Server zu definieren. Das Standard-CI für eine Familie kann zum Attribut eines Betriebs-CI in dieser Familie gemacht werden, mit dessen Hilfe Sie den aktuellen Status oder einen historischen Zustand eines CI mit der zugehörigen Standardkonfiguration vergleichen können. Wie andere Vergleiche können Sie diese Information drucken oder als Datei mit durch Komma getrennten Werten exportieren.

Während Meilensteine als nicht freigegebene, nicht veränderbare Baselines verwendet werden, stellen Standard-Configuration Items freigegebene, dynamische Baselines für Ihre Configuration Items dar.

Wichtig! Ein Standard-CI darf niemals Werte für ein Attribut enthalten, das zur CI-Abstimmung verwendet wird.

Change-Spezifikationen

Zeigen Sie geplante oder nicht geplante Change-Spezifikationen an, die Anwender für Changes für das CI angegeben haben. Sie können die Change-Spezifikation mit dem aktuellen Zustand des CI vergleichen. Vergleichen Sie zum Beispiel einen geplanten Wert mit dem aktuellen Zustand eines CI. Dieser Vergleich kann Konflikte mit Changes zeigen, Change-Überschneidungen im Ablaufplan identifizieren usw..

Mit Versionskontrolle können Sie die folgenden Aufgaben durchführen:

- Automatische Erfassung aller Änderungen an CIs
 - Snapshots eines CI zu einem beliebigen Zeitpunkt anhand von Datums- oder Attribut-Changes
 - Verschiedene Anzeigeebenen wie die ausführliche Protokollansicht, die einfache und die erweiterte Ansicht
 - Mehrere Attributvergleiche mit anderen Snapshots, anwenderspezifischen Meilensteinen oder Standard-CIs
 - Automatische Snapshots, wenn CA SDM-Change-Tickets ihren Status ändern
- Hinweis:** Dieser automatische Snapshot bezieht sich nicht auf Change-Spezifikationen, Verifizierungsrichtlinien, verwaltete Change-Zustände und verwaltete Attribute.
- Erweiterte Filter- und Vergleichsfunktion mit Druck- und CSV-Export-Unterstützung

Weitere Informationen:

[Verwenden von Versionskontrolle](#) (siehe Seite 628)

[Datensätze für gemeinsame Assets und CI-Audit-Kontrolle](#) (siehe Seite 629)

[Terminologie der Versionskontrolle](#) (siehe Seite 629)

[Datenquellen für Versionskontrollen](#) (siehe Seite 633)

[CA SDM Change Management-Integration](#) (siehe Seite 634)

[CA APM-Integration](#) (siehe Seite 635)

[CI-Versionsmanagement](#) (siehe Seite 636)

[CA SDM Change Management](#) (siehe Seite 653)

[Configuration Audit and Control Facility \(CACF\)](#) (siehe Seite 722)

[CI-Versionskontrolle und zukünftiger Zustand](#) (siehe Seite 747)

Verwenden von Versionskontrolle

Die Versionskontrolle schließt die folgenden Verwendungen ein:

Problembestimmung

Um ein Problem mit einem CI zu beheben, *müssen* Sie verstehen, was sich in der Umgebung des CI geändert hat. Die Versionskontrolle zeigt den aktuellen defekten Zustand sowie einen früheren Zustand an, sodass Sie die beiden Zustände vergleichen können, um potenzielle Probleme zu identifizieren.

Leistungs- und Kapazitätsplanung

Durch Überprüfen des Verlaufs eines CI kann ein Leistungs- oder Kapazitätsplaner die Gründe für Leistungsengpässe besser bestimmen und besser für einen zukünftigen Systemzuwachs planen.

Konformität

Sie können den Zustand eines CI mit dem Standard-CI seiner Familie vergleichen. Vergleichen Sie den Zustand an einem beliebigen Punkt in seinem Change-Management-Lebenszyklus, um dabei zu helfen, sicherzustellen, dass sich das CI in Compliance befindet sowie Attribute zu identifizieren, die Korrekturen benötigen.

Change-Verifizierung

Sie können den Audit-Verlauf des Objekts anzeigen, beispielsweise welcher Anwender eine Verifizierungsrichtlinie geändert hat, an welchem Datum der Request erstellt wurde, welche Attributen und Werte der Anwender geändert hat usw.. Sie können die Änderungen für spezifische Zeiträume vergleichen einander gegenüberstellen.

Datensätze für gemeinsame Assets und CI-Audit-Kontrolle

Die Funktion zur Versionskontrolle umfasst an CA APM vorgenommene Audit-Pfadänderungen. Diese Funktion unterstützt ferner den kontextuellen Start von CA CMDB an CA APM direkt von einem beliebigen Attributprotokolleintrag, der mit einer CA APM-Änderung verknüpft ist. Die CA APM-Audit-Kontrollinformationen sind nur für CIs/Assets aus CA CMDB-Familien verfügbar, für die CA APM-Audit-Protokollierung aktiviert ist.

Die Registerkarte "Versionskontrolle", welche die Informationen über den CA APM Audit-Pfad enthält, unterstützt alle Familien, vorausgesetzt die Familie kann sich beim System anmelden.

Standardmäßig protokolliert CA APM keine Änderungen an Assetattributen. Um die CA CMDB-Versionskontrolle mit einem von CA APM verwalteten Asset/CI verwenden zu können, muss für jedes Assetattribut, das protokolliert werden soll, das Kontrollkästchen zum Speichern der Audit-Pfaddaten aktiviert sein.

Hinweis: Weitere Informationen zum Aktivieren von Audit-Protokollen finden Sie in der CA APM-Dokumentation.

Wenn Assetattribute in CA APM geändert werden, kann es aufgrund der Zwischenspeicherung vorkommen, dass die Daten auf der Registerkarte "Versionskontrolle" auf der Seite "CI - Detail" vor den Daten auf der Registerkarte "Attribute" aktualisiert werden. Klicken Sie auf die Schaltfläche "Bearbeiten", um die Werte neu zu synchronisieren.

Terminologie der Versionskontrolle

Mit der Versionskontrolle werden *Dienstübergänge* dargestellt und verfolgt. Die Versionskontrolle verwendet normalerweise eine Namenskonvention, um Daten, Sequenzen und Bedeutungen dieser Übergänge zu identifizieren. Mit diesen Aufzeichnungen kann man bestimmte Statuswerte eines Configuration Item identifizieren und vergleichen.

Beispiel: Versionsvergleich

Bei einem CI für Lohn- und Gehaltslisten ergibt ein Vergleich zwischen Version 3 und Version 2, dass die neuere Version verbesserte Funktionen und andere Unterschiede zur alten Version aufweist.

Weitere Informationen:

[Zustände](#) (siehe Seite 630)

[Versionen](#) (siehe Seite 630)

[Snapshots](#) (siehe Seite 630)

[Kategorien](#) (siehe Seite 631)

[Meilensteine](#) (siehe Seite 631)

[Standard-Configuration Items](#) (siehe Seite 632)

Zustände

Im Kontext der Versionskontrolle stellt der *Zustand* eines Configuration Item alle Attributwerte dieses CI zu einem bestimmten Zeitpunkt dar. Der Zustand eines CI kann das Ergebnis von Änderungen an Attributen durch mehrere MDRs sein.

Versionen

Eine *Version* ist eine identifizierte Instanz eines CI innerhalb einer Produkt- oder Konfigurationsstruktur. Versionen werden dazu genutzt, um den Change-Verlauf zu verfolgen und zu protokollieren.

Snapshots

Ein *Snapshot* stellt einen vollständigen Status eines CI zu einem bestimmten Zeitpunkt dar. Mit einem typischen CI sind viele Snapshots verknüpft. Ein Snapshot vereint alle Änderungen an einem CI, die innerhalb einer Minute vorgenommen wurden. Wenn ein CI beispielsweise innerhalb einer Minute mehrere Male aktualisiert (bearbeitet und gespeichert) wird, erstellt CA SDM einen einzigen Snapshot, der alle Aktualisierungen während dieser Minute darstellt.

"Snapshot" ist ein allgemeiner Begriff, der sich auf zeit- und datenbasierte Snapshots ebenso bezieht wie auch auf Meilensteine oder Standard-CIs. Um relevante Zeitpunkte einfacher zu finden, können Sie in CA SDM Snapshots beschriften. Diese benannten Snapshots heißen Meilensteine.

Jede Mal, wenn eine Änderung an einem CI vorgenommen wird, erstellt CA SDM automatisch einen Snapshot, ohne, dass manuell eingegriffen werden muss. Die Versionskontrolle erfasst alle Änderungen am Objekt. Dies umfasst Snapshots, die über die Benutzeroberfläche erstellt wurden, ebenso wie solche, die aus einem MDR stammen und über GRLoader oder CA CMDB-Webservices in die CMDB gelangt sind.

Kategorien

Eine *Kategorie* identifiziert eine Klasse von Attributen. Die Kategorie ist in der Regel der Name der Registerkarte, auf der die Attribute angezeigt werden.

Hinweis: Elemente, die nicht in der Registerkarte stehen (zum Beispiel Name, Seriennummer, aktive Markierung) werden einer Kategorie zugeteilt, die einen anderen Namen als eine Registerkarte hat.

Beispiele: Registerkarten und Kategorien

Die folgenden Beispiele veranschaulichen, wie Kategorien Registerkarten entsprechen:

- Da *Speicherplatz* auf der Registerkarte "Attribute" angezeigt wird, ist die Kategorie ebenfalls *Attribute*.
- Da *IP-Adresse* in der Registerkarte "Inventar" angezeigt wird, ist die Kategorie ebenfalls *Inventar*.
- *Meilenstein* wird in der Kategorie *Allgemein* angezeigt.
- Ein *Standard-CI* wird in der Kategorie "Klassifikation" angezeigt.
- *Beziehungen* werden in der Kategorie "Beziehung" angezeigt.

Meilensteine

Als *Meilenstein* wird der Snapshot eines Configuration Item bezeichnet, der auf Wunsch benannt wird. Er wird erstellt, um ein Event, einen logischen Messpunkt oder eine Ansammlung von Änderungen zu kennzeichnen. Der Meilenstein enthält den aktuellen Status des Configuration Item zu dem Zeitpunkt, an dem der Snapshot erstellt wurde. Mit Meilensteinen können Sie schnell bedeutende Events im Verlauf eines CI identifizieren und zu ihnen navigieren. Bei der Erstellung eines Meilensteins wird auch ein entsprechender "Datum"-Snapshot erstellt.

Meilensteine sind CI-spezifisch und werden nicht gemeinsam genutzt. Wenn Sie einen Meilenstein für ein Objekt einer hohen Ebene, zum Beispiel einen Service, erstellen, erstellen die Unterkomponenten dieses Objekts Meilensteine nicht automatisch. Um einen Meilenstein für ein Objekt mit mehreren Unterkomponenten zu übernehmen, können Sie mehrere unabhängige Meilensteine erstellen.

Meilensteine sind statisch und können niemals verändert oder gelöscht werden. Wenn Sie einen Meilenstein erstellen, hat der Snapshot den aktuellen Status des CI. Wenn sie später angezeigt oder für einen Vergleich herangezogen werden, verweisen die Meilensteine immer auf einen Zeitpunkt in der Vergangenheit. Eine gute Namenskonvention für Ihre Meilensteine hilft Ihnen dabei, kritische Punkte während der Lebensdauer eines CIs leicht zu identifizieren.

Wichtig! Meilensteine beziehen sich *nicht* auf Change-Spezifikationen, Verifizierungsrichtlinien, verwaltete Change-Zustände und verwaltete Attribute.

Standard-Configuration Items

Ein *Standard-CI* ist eine abstrahierte Konfiguration für eine CI-Familie. Sie können damit grundlegende Vergleiche zu "richtigen" CI-Instanzen in derselben Familie aufstellen. Ein Standard-CI kann ein richtiges CI sein; dann stellt es ein physisches Objekt dar oder kann nur für Vergleichszwecke existieren. Standard-CIs können die folgenden Zuordnungen haben:

- Ein Standard-CI kann von mehreren CIs gemeinsam genutzt werden.
- Ein CI kann immer nur mit jeweils einem Standard-CI verknüpft sein. Wenn das Standard-CI verändert wird, zeigt sich diese Veränderung auch dann, wenn man die verknüpften CIs mit dem Standard-CI vergleicht.
- Eine Familie kann mehrere Standard-Configuration Items besitzen. Eine Familie verfügt beispielsweise über Standard-Configuration Items namens "Standard-Testserver", "Standard-Produktionsserver", "Standard-Annahmeserver". Es ist empfehlenswert, dass Sie Ihre Standard-Configuration Items so benennen, dass Sie sie leicht suchen und als Standard-Configuration Items identifizieren können.

Da ein Standard-CI auch selbst ein CI ist, kann es verwaltet werden. Wie jedes andere CI auch verfügt es über einen Audit-Pfad, Sicherheit, einen Änderungsverlauf usw. Nachdem Sie für ein bestimmtes CI ein Standard-CI definiert haben, können Sie mit ihm die Compliance mit Unternehmensstandards überprüfen.

Die Konzepte "Datum" oder "Zeit" gelten nicht für den Vergleich zwischen einem Standard-CI und einem Snapshot oder Meilenstein. Nur die Attributwerte des Standard-CI werden zu Vergleichszwecken herangezogen. Snapshots und Meilensteine, die spezifisch für das Standard-CI sind, gelten nicht.

Beispiel: Verwenden von Standard-CI

Ein Unternehmen definiert eine Konfiguration **Mitarbeiter-Workstation** als Standard-CI, um damit die tatsächlichen Desktop-Rechner in der Familie "Hardware.Workstation" zu vergleichen. Ein solcher Vergleich zeigt, dass ein bestimmter PC nur über 1 GB RAM verfügt, obwohl das Standard-CI einen Speicherwert von 2 GB vorsieht.

Datenquellen für Versionskontrollen

Versionskontrolldaten werden immer generiert, wenn Sie ein Objekt mithilfe von Komponenten, die die ändern, die die Audit-Protokoll-Funktion unterstützen, erstellen oder ändern. Snapshots, die aus mehreren Quellen generiert wurden, sind voneinander nicht zu unterscheiden. Wenn die Umgebung richtig konfiguriert ist, werden Snapshots automatisch immer dann angezeigt, wenn Configuration Items und ihre Beziehungen verändert wurden.

Bei allen CA CMDB-Familien ist die Versionskontrolle aktiviert. CIs in Basisfamilien von CA Service Desk müssen in CA CMDB-Familien konvertiert werden, damit die Versionskontrolle angewendet werden kann.

Die Daten der Versionskontrolle enthalten die folgenden Quellen:

- **CA CMDB-CI-Aktualisierungen:** Aktualisierungen von allgemeinen CI-Attributen und familienspezifischen CI-Attributen mit Hilfe der Benutzeroberfläche.
- **Aktualisierungen von CA CMDB-Beziehungen:** Aktualisierungen von Beziehungen auf der Registerkarte "Beziehungen" und in der CI-Beziehungsliste mit Hilfe der Funktionen "Bearbeiten" und "In Liste bearbeiten".
- **GRLoader:** Aktualisierungen von eingefügten CIs und Attributen, Aktualisierungen von Beziehungen, Zuweisungen von Standard-CIs und mit Hilfe von GRLoader importierte Meilensteine. Wenn Aktualisierungen von einem MDR mit Hilfe von GRLoader gesendet werden, wird die MDR-Quelle ebenfalls aufgezeichnet. So können Sie Attributänderungen direkt bis zu ihrer Quelle zurückverfolgen.
Hinweis: Weitere Informationen finden Sie im *technischen Referenzhandbuch*.
- **CA SDM-Change-Verlauf:** Ein Snapshot wird automatisch für alle CIs erstellt, die einem Change-Ticket zugeordnet sind. Wenn das Configuration Item geöffnet, geschlossen, aktiv oder abgeschlossen ist, werden bis zu vier Snapshots aufgezeichnet.
- **CA Asset Portfolio Management (CA APM) CI-Änderungen:** Changes, die von CA APM an CIs bei aktivierter Protokollierung vorgenommen wurden.
- **Change-Verifizierung:** Aktualisierungen an Change-Spezifikationen, Verifizierungsrichtlinien, verwalteten Change-Zuständen und verwalteten Attributen.

Hinweis: Bei CIs, die in CA SDM oder früheren CA CMDB-Versionen erstellt wurden, werden nur Modifikationsänderungen angezeigt. Ursprüngliche Attributwerte wie Name, Familie und Klasse wurden nicht protokolliert und werden in Snapshots nicht angezeigt. Außerdem verfügen Beziehungen, die mit CA Service Desk oder früheren CA CMDB-Versionen erstellt wurden, über keinerlei Informationen zum Prüfungsverlauf.

CA SDM Change Management-Integration

Für jedes CI, das mit einem CA SDM-Change-Ticket verknüpft ist, werden Daten der Versionskontrolle erzeugt. Während sich der Status des Change-Tickets von "Offen" in "Aktiv", "Gelöst" und dann in "Geschlossen" ändert, wird für jedes zugehörige CI ein Snapshot angefertigt. Damit werden Snapshots für Status vom Typ "Geöffnet", "Geschlossen", "Aktiv" und "Gelöst" erstellt. Wenn mit einem Change Request keine CIs verknüpft sind, werden keine Snapshots erstellt.

Hinweis: Die Funktion "Versionskontrolle" erfordert keine spezielle Konfiguration und wird in integrierten Installationen automatisch unterstützt.

Die Funktion "Versionskontrolle" wirkt sich wie folgt auf das Change-Ticket aus:

1. Sie vergleicht den Status des CI beim Öffnen des Tickets mit seinem aktuellen Status.
2. Sie überprüft, ob alle erforderlichen Changes richtig ausgeführt worden sind und keine zusätzlichen Changes eingeführt wurden.
3. Sie schließt das Ticket, nachdem die Änderungen bestätigt worden sind.

Zu Prüfzwecken können Sie den CI-Status vor und nach jeder Änderung vergleichen. Diese Vergleichsinformationen helfen, verschiedene Fragen (z. B. zum Status eines CIs vor und nach einem Change Request) zu beantworten, wie z. B.:

- Wurde die korrekte Änderung wie gewünscht ausgeführt?
- Welche anderen Änderungen betrafen das CI, die nicht mit dem Change-Ticket verknüpft waren?
- Wann wurden die Änderungen ausgeführt?
- Wie verhält sich das Configuration Item im Vergleich zur Standardkonfiguration – jeweils vor und nach der Änderung?

CA APM-Integration

Die Versionskontrolle zeigt Änderungen an, die von CA APM an den CIs vorgenommen wurden. Die Versionskontrolle unterstützt auch den Start im Zusammenhang von CA CMDB zu CA APM direkt von einem beliebigen Attributprotokolleintrag, der einer Änderung von CA APM zugeordnet ist. CA APM-Audit-Informationen sind nur für CIs aus CA CMDB-Familien verfügbar, wenn die CA APM-Audit-Protokollierung aktiviert ist.

Hinweis: Wenn CI-Attribute in CA APM geändert werden, können aufgrund der Zwischenspeicherung die Daten auf der Registerkarte "Versionskontrolle" auf der Seite "Configuration Item - Detail" vor den Daten auf der Registerkarte "Attribute" aktualisiert werden. Klicken Sie auf die Schaltfläche "Bearbeiten", um die Werte neu zu synchronisieren.

Standardmäßig protokolliert CA APM keine Änderungen an CI-Attributen. Um die Versionskontrolle mit einem von CA APM verwalteten CI verwenden zu können, muss für jedes Assetattribut, das protokolliert werden soll, das Kontrollkästchen "Audit-Pfaddaten speichern" aktiviert sein.

Hinweis: Standardmäßig ist eine zehnminütige Verzögerung zwischen der Aktualisierung eines CI in CA APM und dem Zeitpunkt, an dem es in CMDB für die Versionskontrolle verfügbar ist, eingestellt. Sie können diese Verzögerung durch die Veränderung der @NX_DBMONITOR_TIMER_MINUTES-Variablen in einer integrierten Installation ändern.

Hinweis: Informationen zur Aktivierung der Attributprotokollierung für Assets finden Sie in der CA APM-Dokumentation.

Weitere Informationen:

[CA APM-Integrationsfunktionen](#) (siehe Seite 635)

CA APM-Integrationsfunktionen

CA SDM bietet die folgenden Integrationsfunktionen in CA APM:

- Freigegebene Datensätze und ein Audit-Protokoll, die zwischen CA APM-CIs und -Assets unterscheiden
- CA CMDB und CA APM starten im Kontext mit CI-/Asset-Informationen
- Freigegebene Erweiterungstabellenfelder
- Ein CA SDM-Kontakt wird aktualisiert, wenn CA APM einen ersten Kontakt ändert
- Änderung der CA APM-Assettypen, um CI-Familien zu benutzen

CI-Versionsmanagement

Sie können den Verlauf des CI, zugehörige Snapshots, Meilensteine, ungeplante Changes und andere Ansichten anzeigen. Der linke Bereich dient zum Navigieren, der rechte Fensterbereich zum Anzeigen der CI-Details und des Audit-Protokolls.

Hinweis: Die Funktionsweise der Versionskontrolle ist für den Verlauf des verwalteten Attributs und des verwalteten Change-Zustans sehr ähnlich. Zum Beispiel werden auf der Registerkarte "Verlauf des verwalteten Attributs" Versionskontrollinformationen zu einem verwalteten Attribut angezeigt.

Verwenden Sie Versionskontrollinformationen, um Change-Spezifikationen und die zugeordneten Changes zu identifizieren. Die Versionskontrolle identifiziert ungeplante Änderungen in den Change-Spezifikationen in der Snapshot-Ansicht, die Changes ohne geplantem Startdatum entspricht. Sie können den Snapshot und das Protokoll einer Change-Spezifikation in CACF anzeigen.

Beispiel: Ungeplanter Change

In diesem Beispiel versucht ein Anwender, den Wert eines verwalteten Attributs zu ändern. Sie zeigen die Registerkarte "Versionskontrolle" auf der CI-Detailseite an, auf der ein Snapshot des ungeplanten Change angezeigt wird. Dieser Snapshot zeigt Informationen zum Change wie Datum, Uhrzeit, Anwendername und Attributwert, an.

Wenn Sie eine Momentaufnahme oder einen Meilenstein in der linken Fensterhälfte auswählen, zeigt die rechte Fensterhälfte die Attributwerte dieses CI-Status, -Events oder -Vergleichs an. Der linke Bereich kann CI-Momentaufnahmen oder Meilensteine nach Datum und Uhrzeit (Grundmodus) oder nach CI-Merkmalen (Fortgeschrittener Modus) anzeigen, und schließt die folgenden Verknüpfungen ein, um Sie bei der Verwaltung eines CI zu unterstützen:

Meilenstein erstellen

Bezeichnet den Status eines CI.

Protokoll anzeigen

Zeigt einen ungefilterten CI-Verlauf.

Erweitert/Grundlegend

Schaltet zwischen Ansichten für Snapshots um.

Leere Werte ausblenden

Ermöglicht das Filtern leerer Datenfelder. Ist diese Option nicht aktiviert, werden alle CI-Attribute angezeigt.

Drucken und Exportieren

Drucken Sie oder schneiden und fügen Sie ein, um die angezeigten Daten der Versionskontrolle zu speichern.

Protokoll anzeigen

Im Protokoll können Sie den Verlauf eines CIs anzeigen. Mit der Option "Filter" können Sie nach Protokollzeilen filtern. Mit "Drucken" und "Exportieren" können Sie drucken oder ausschneiden und einfügen, um die angezeigten Daten der Versionskontrolle zu speichern.

Der Informationsbereich der Versionskontrolle zeigt folgende Felder an:

- Kategorie
- Datum
- Protokoll
- Attribut
- Neuer Wert
- Alter Wert
- Geändert von
- MDR

Hinweis: Das Protokoll zeigt nur *Aktualisierungen* von Attributen für CIs an, die in Vorversionen von CA SDM bzw. CA CMDB erstellt wurden. Ihre ursprünglichen CI-Attributwerte werden nicht angezeigt. Beziehungen, die mit die in Vorversionen von CA SDM bzw. CA CMDB erstellt wurden, enthalten keine Informationen zum Prüfungsverlauf und sind auch nicht im Protokoll aufgeführt.

Protokollfilterung

Sie können das Protokoll filtern, indem Sie eine einfache Zeichenfolge in das Feld "Filter" eingeben. Beim Filter wird nicht zwischen Groß- und Kleinschreibung unterschieden. Wenn die Zeichenfolge des Filters an einer beliebigen Stelle der Protokollzeile auftaucht, wird die Zeile angezeigt. Im Filter werden keine speziellen Zeichen oder Platzhalter verwendet. Protokollzeilen, auf die die Filterkriterien zutreffen, werden angezeigt, und Zeilen, auf die die Kriterien nicht zutreffen, werden ausgeblendet.

Um die Anzeige zu aktualisieren, müssen Sie nicht die Eingabetaste oder auf Aktualisieren drücken. Die Ansicht des Protokolls wird sofort gefiltert, wenn eine Eingabe gemacht wird, und gilt für alle Felder: "Datum", "Protokoll", "Attribut", "Alter Wert", "Neuer Wert", "MDR" und "Name".

Anzeigen des Configuration Item-Verlaufs

Sie können den Verlauf eines Configuration Item anzeigen.

So zeigen Sie den Verlauf eines Configuration Item an

1. Suchen Sie nach dem Configuration Item, und öffnen Sie es.

Die Seite "Configuration Item – Detail" wird angezeigt.

2. Klicken Sie auf die Registerkarte "Versionskontrolle".

Die Seite "Versionskontrolle" wird angezeigt.

3. Klicken Sie auf "Protokoll anzeigen".

Der Verlauf des Configuration Item wird aufgelistet.

Hinweis: "Protokoll anzeigen" ignoriert die Auswahl im linken Bereich.

Drucken eines CI-Protokolls

So drucken Sie ein Protokoll für ein CI:

So drucken Sie ein Protokoll eines CI

1. Wählen Sie ein CI aus, und klicken Sie auf die Registerkarte "Versionskontrolle".

2. Klicken Sie auf den Link "Protokoll anzeigen".

3. (Optional) Geben Sie die gewünschten Filterkriterien ein, um Protokollzeilen aus- oder einzublenden.

4. Klicken Sie auf "Drucken".

Die Druckversion des Fensters wird geöffnet. Der Versionskontrollbericht für das CI wird angezeigt.

5. Klicken Sie in Ihrem Webbrowser auf "Datei", anschließend auf "Drucken", um den Bericht auszudrucken.

Der formatierte Text wird nun an den ausgewählten Drucker gesendet.

Unterstützung für CSV-Export

Sie können den CA CMDB-Protokollinhalt in eine Datei im CSV-Format (durch Kommata getrennten Werte) exportieren, die Berichts-Tools oder Anwendungen von Fremdanbietern importieren können. Der Export basiert auf dem, was aktuell dargestellt wird. Dies kann gefiltert oder ungefiltert sein.

Weitere Informationen:

[Exportieren von Daten](#) (siehe Seite 649)

Integrierte CA SDM- und CA APM-Protokolle

Neben solchen Änderungen, die mit Hilfe der CA CMDB-Funktionen gemacht wurden, enthält das CI-Protokoll auch Aktualisierungs-Events von CA SDM-Changeticket-Aktivitäten und von CA APM-Aktualisierungen.

Weitere Informationen:

[CA APM-Integration](#) (siehe Seite 635)

Starten von MDR im Kontext und Identifizierung von Quellen

In CA CMDB gibt es die Möglichkeit, im Kontext zu starten, direkt vom Protokoll zum MDR-Daten-Provider für einen bestimmten CI-Protokolleintrag. Sie können auch im Kontext der Change-Spezifikation starten. Mit dieser Startfunktion werden folgende Schritte ausgeführt:

- Attributänderungen werden zum Quell-MDR zurückverfolgt, wenn das MDR die Tags `<mdr_name>`, `<mdr_class>` und `<federated_asset_id>` in der GRLoader-Eingabe benutzt hat.

Hinweis: Weitere Informationen finden Sie im *technischen CA CMDB-Referenzhandbuch*.

- Aktualisierungen eines CI-Attributs durch mehr als ein MDR werden identifiziert. Dieser Fall kann eintreten, wenn mehrere MDRs unabhängig Daten zu einer CI-Definition beitragen.
- Es wird erkannt, welches MDR als maßgebliche Quelle dient.

Hinweis: Protokolleinträge, die in CA SDM oder früheren Versionen von CA CMDB erstellt wurden, enthalten die Informationen zum Starten von MDR im Kontext nicht. Des Weiteren kann CA Cohesion ACM Informationen zum Starten von MDR für die meisten, jedoch nicht alle Attribute und Beziehungen bieten.

Attributnamen

Attributnamen, die im Protokoll angezeigt werden, stimmen mit dem Attributnamen auf der Benutzeroberfläche überein. Sie tragen nicht den Namen des internen Objekts. Zum Beispiel zeigt CA CMDB "Wartungstyp" an Stelle von "mtce_type" an.

Protokollieren von anwenderspezifischen Familien und Attributen

Geben Sie neue MDR-Attribute und Audit-Auslöser an, um das Protokollieren angepasster Familien und Attribute zu aktivieren. Wenn Sie neue Familien oder Attribute erstellen, müssen Sie außerdem Metadatendateien erstellen, um lesbare Attributnamen anzugeben, die im Protokoll angezeigt werden sollen. Andernfalls wird der interne Objektname angezeigt.

Hinweis: Weitere Informationen finden Sie unter "Erweitern von CA CMDB" im *Administrationshandbuch*.

Erstellen eines Meilensteins

Sie können einen Meilenstein über die Benutzerschnittstelle oder mit GRLoader erstellen.

So erstellen Sie in der Benutzeroberfläche einen Meilenstein:

1. Wählen Sie ein CI aus, und klicken Sie auf die Registerkarte "Versionskontrolle".
2. Klicken Sie auf "Meilenstein erstellen".
3. Geben Sie eine Beschreibung für den Meilenstein ein. Klicken Sie auf "Speichern".

Die Seite "Meilenstein erstellen" wird geschlossen.

4. Wählen Sie "Ansicht" und anschließend "Aktualisieren".

In der Basisansicht wird ein neuer Snapshot mit dem aktuellen Datum und der Uhrzeit angezeigt, der den gerade erstellten Meilenstein darstellt. In der Meilensteinansicht werden nur die Snapshots mit zugewiesenen Namen angezeigt. Meilensteine werden nach Datum/Uhrzeit absteigend angezeigt, der aktuellste steht ganz oben.

So erstellen Sie einen Meilenstein mit Hilfe von GRLoader

1. Fügen Sie das Tag <milestone> in die XML-Datei für das CI ein.
2. Wenden Sie dieselben Abstimmungsregeln wie bei der Zuordnung eines Meilensteins zu einem Configuration Item an.

Hinweis: Der Wert eines Meilenstein-Tags ist die Bezeichnung, die mit diesem Meilenstein verknüpft ist.

3. Speichern und schließen Sie die XML-Datei für das CI.

Der Meilenstein wird erstellt.

Hinweis: Weitere Informationen finden Sie im *technischen CA CMDB-Referenzhandbuch*.

Beispiel: Verwenden von GRLoader zur Einrichtung eines Meilensteins

Das folgende GRLoader-Beispiel erstellt den Meilenstein **Geschäftsjahresende 2008**.

```
<ci>
<name>Server1 </name>
<milestone>Ende Geschäftsjahr 2008</milestone>
</ci>
```

Erstellen eines Standard-CI

Ein Standard-CI können Sie wie jedes andere CI erstellen.

So erstellen Sie in der Benutzeroberfläche ein Standard-CI:

1. Wählen Sie im Menü "Datei" die Option "Neues Configuration Item erstellen".
2. Wählen Sie die Familie aus, die Sie für das neue Standard-CI verwenden möchten.
3. Definieren Sie die Attribute wie bei einem normalen Configuration Item.

Das Standard-CI wird erstellt.

Hinweis: Jedes Configuration Item kann als Standard-Configuration Item eingesetzt werden, dabei sollte allerdings Folgendes bedacht werden:

- Ein Standard-Configuration Item sollte einer Namenskonvention folgen, damit es nicht mit normalen Configuration Items verwechselt werden kann.
- Ein Standard-Configuration Item darf nur als Ausgangselement für Configuration Items eingesetzt werden, die in derselben Familie wie das Standard-Configuration Item sind.
- Einem Standard-CI sollten *keine* Werte für CORA-Felder zugewiesen werden, z. B. "MAC-Adresse", "Seriennummer", "Alt. Configuration Item-ID", "DNS" usw.
- Da Standard-CIs nicht von normalen CIs zu unterscheiden sind, werden sie in Ihrem Scoreboard angezeigt und zur Gesamtanzahl der CIs hinzugezählt.
- Am besten ist es, wenn ein Standard-Configuration Item keine richtigen Instanzen eines Geschäftsobjekts repräsentiert.

Zuweisen eines Standard-CI zu einem CI

Sie können ein Standard-CI auf der CI-Detailseite einem Configuration Item zuordnen. Sie können ein Standard-CI einer Liste von CIs zuordnen oder "In Liste bearbeiten" verwenden.

So weisen Sie das Standard-CI einer Familie einem CI mit Hilfe der Detailseite des CI zu:

1. Wählen Sie ein CI aus, und klicken Sie auf "Bearbeiten".

Die Seite "Configuration Item aktualisieren" wird angezeigt.

2. Klicken Sie auf das Symbol neben dem Feld "Standard-CI".
Die CI-Liste wird angezeigt.
3. Legen Sie ein CI als Standard-CI fest. Klicken Sie auf "Speichern".
Das Standard-CI wurde zugewiesen.

So weisen Sie das Standard-CI einer CI-Liste mit Hilfe der Funktion "In Liste bearbeiten" zu:

1. Weisen Sie den Suchfilter im Scoreboard oder in der Registerkarte "Administration" an, ein einziges oder mehrere Configuration Items in der Detailliste anzuzeigen, und klicken Sie auf "Suchen".
Die Configuration Items, auf die die ausgewählten Suchkriterien zutreffen, werden aufgelistet.
2. Klicken Sie auf die Schaltfläche "In Liste bearbeiten" oben rechts in der Liste mit den Ergebnissen.
Das Steuerelement "In Liste bearbeiten" für Configuration Items wird angezeigt.
3. Wählen Sie in einer Zeile ein CI aus, das Sie als Standard-CI festlegen möchten.
Die Zeile wird nun farbig hervorgehoben.
4. Klicken Sie auf das Symbol neben dem Feld "Standard-CI".
Die CI-Liste wird angezeigt.
5. Legen Sie ein CI als Standard-CI fest. Klicken Sie auf "Speichern". Das CI wird aktualisiert. Möchten Sie alle Configuration Items in der Liste aktualisieren, klicken Sie auf "Alle ändern".
Sie können das Standard-CI entweder einem einzelnen CI zuweisen ("Speichern"), oder es allen CIs in der Liste zuweisen ("Alle ändern").

Hinweis: Jedes Configuration Item kann als Standard-Configuration Item eingesetzt werden, dabei sollte allerdings Folgendes bedacht werden:

- Ein Standard-Configuration Item sollte einer Namenskonvention folgen, damit es nicht mit normalen Configuration Items verwechselt werden kann.
- Ein Standard-Configuration Item darf nur als Ausgangselement für Configuration Items eingesetzt werden, die in derselben Familie wie das Standard-Configuration Item sind.
- Einem Standard-CI sollten *keine* Werte für CORA-Felder zugewiesen werden, z. B. "MAC-Adresse", "Seriennummer", "Alt. Configuration Item-ID", "DNS" usw.
- Da Standard-CIs nicht von normalen CIs zu unterscheiden sind, werden sie in Ihrem Scoreboard angezeigt und zur Gesamtanzahl der CIs hinzugezählt.

Am besten ist es, wenn ein Standard-Configuration Item keine richtigen Instanzen eines Geschäftsobjekts repräsentiert.

Zuweisen eines Standard-CI zu einem CI mit GRLoader

Um einem CI ein Standard-CI zuzuordnen, schließen Sie das Tag `<standard_ci>` in die Beschreibung des CI ein.

Hinweis: Weitere Informationen finden Sie im *technischen CA CMDB-Referenzhandbuch*.

Beispiel: Zuweisen eines Standard-CI zu einem CI

Haben Sie eine Standardkonfiguration Ihrer Workstation in einem CI mit der Bezeichnung **Standardkonfiguration Workstation** gespeichert, können Sie dieses Standard-CI der Workstation des Anwenders Joe zuweisen. Laden Sie hierzu mit GRLoader folgenden XML-Code:

```
<ci>
    <name>Joes Workstation</name>
    <class>Server</class>
    <standard_ci>Standardkonfiguration Workstation</standard_ci>
</ci>
```

Verwenden der Basisansicht

Sie können Snapshots sowohl in der Basisansicht als auch in der erweiterten Ansicht auswählen. In beiden Modi können dieselben Daten der Versionskontrollen angezeigt werden. In der Basisansicht können Sie den Status eines CI einsehen.

So verwenden Sie die Basisansicht zur Anzeige des Status eines CI:

1. Öffnen Sie das CI auf der Benutzerschnittstelle, und klicken Sie auf die Registerkarte "Versionskontrolle".

Vorhandene Snapshots werden links auf der Seite aufgelistet.

2. Wählen Sie einen Snapshot-Typ aus der Dropdown-Liste "Snapshot-Typ" aus.

Hinweis: Wenn Sie ein Standard-CI als Fokus-CI auswählen, wird es oben in der Liste der Snapshots oder Meilensteine angezeigt. Rechts neben dem CI-Namen wird außerdem der Indikator "Standard-CI" eingeblendet. Beim Klicken auf ein Standard-CI werden die Attribute für das Standard-CI und nicht für das Fokus-CI angezeigt.

Snapshot

Listet alle CI-Snapshots auf, die auf Basis des Datums/der Uhrzeit und des Standard-CI identifiziert werden. Dies ist die voreingestellte Option.

Meilenstein

Listet alle anwenderspezifischen Meilensteine und das Standard-CI auf.

Der Status des CI wird im rechten Fenster angezeigt.

Führen Sie den Mauszeiger in ein Element, werden Ihnen im Informationsbereich am unteren Rand der Seite nähere Informationen angezeigt. Wenn Sie den Mauszeiger in einen Snapshot, einen Meilenstein oder ein Standard-CI führen, werden Datum und Zeit der Erstellung und der Typ des Snapshots angezeigt.

Hinweis: Sie können zwei oder mehr Snapshots, Meilensteine oder Standard-CIs auswählen, um sie miteinander zu vergleichen.

Verwenden der erweiterten Ansicht

Sie können Snapshots sowohl in der Basisansicht als auch in der erweiterten Ansicht auswählen. In beiden Modi können dieselben Daten der Versionskontrollen angezeigt werden. In der erweiterten Ansicht können Sie Snapshots auf Basis des Attributtyps, Werts und Zeitstempels anzeigen. In dieser Ansicht können Sie außerdem beliebige Attribute, Meilensteine oder Standard-CIs miteinander vergleichen. Eine Strukturhierarchie zeigt einen Ordner für jedes Attribut des CI an, wobei jeder Attributordner den Verlauf der Werte für das Attribut enthält. Die Hierarchie ist folgendermaßen aufgebaut:

Stamm

Attributname

Attributwert 1

Attributwert 2

Mit dieser Hierarchie können Sie den Verlauf eindeutiger Werte für jedes Attribut auf einen Blick einsehen.

So verwenden Sie die erweiterte Ansicht:

1. Öffnen Sie das CI auf der Benutzerschnittstelle, und klicken Sie auf die Registerkarte "Versionskontrolle".

Vorhandene Snapshots werden links auf der Seite aufgelistet.

2. Klicken Sie auf "Erweitert".

Die erweiterte Auswahl zeigt eine Ordnerhierarchie an.

3. Navigieren Sie durch die Ordnerhierarchie, und klicken Sie auf den Ordner, der die gewünschten Informationen enthält:

Datum

Listet Snapshots auf Grundlage des Datums/der Uhrzeit auf, was der Basisansicht entspricht. Die Snapshots lassen sich weiter auf Grundlage des Jahres/Monats unterteilen, sofern das CI mindestens 30 Snapshots aufweist. Wurde dem Fokus-CI ein Standard-CI zugewiesen, können Sie dieses Standard-CI ebenfalls in diesem Ordner sehen.

Meilenstein

Listet alle anwenderspezifischen Meilensteine auf, was der Basisansicht entspricht. Wurde dem Fokus-CI ein Standard-CI zugewiesen, können Sie dieses Standard-CI ebenfalls in diesem Ordner sehen.

Die Attribute von Standard-CIs werden als Strukturknoten mit einem Marker "Standard-CI" dargestellt. Werte für Standard-Configuration Items werden nur für Attribute angezeigt, für die ein Standardwert für Configuration Items festgelegt wurde. Ist dies nicht der Fall, werden diese Werte nicht angezeigt.

Beziehung

Enthält alle Beziehungen (aktuelle und gegenwärtige) für das CI. Folgende Informationen finden Sie in der Ordnerhierarchie:

Beziehung
 Beziehungstyp.
 Partner-CI
 Status und Datum

Der Beziehungstyp definiert die Art der Beziehung, z. B. "wird enthalten von", "ist Host für" oder "kommuniziert mit".

Als Partner-CI wird der Name des CI angezeigt, das der Beziehung zugeordnet ist.

Status und Datum definieren den Status der Beziehung zum angegebenen Datum und Zeitpunkt. Statuswerte umfassen die folgenden:

- Beziehung erstellt: Status des CI zum Erstellungszeitpunkt der Beziehung
- Abgebrochene Beziehung: Das CI wird in der Beziehung nicht mehr verwendet. Für das Partnerelement ist die Beziehung noch aktiv, jedoch wird das Fokus-CI nicht mehr verwendet.
- Gelöschte Beziehung: Die Beziehung wurde als gelöscht gekennzeichnet.
- Geänderte Beziehung: Die Beziehung wurde nach der Löschung erneut aktiviert.
- Neuer Partner und Typ: Es wurde ein neues CI als Partner festgelegt. Gleichzeitig wurde der Beziehungstyp geändert.
- Neuer Beziehungstyp: Der Beziehungstyp zwischen zwei CIs hat sich geändert.
- Zugewiesenes Partner-CI: Für die Beziehung wurde ein neues Partnerelement festgelegt.

4. Klicken Sie auf einen Attributwert.

Der vollständige Status des CI zum Zeitpunkt der Attributwerteinstellung wird angezeigt.

Beispiel: Verwenden der erweiterten Ansicht zur Anzeige von Festplattenspeicherattributen

Im folgenden Beispiel wird in der erweiterten Auswahl angezeigt, dass der Festplattenspeicher von 10 GB auf 20 GB erweitert wurde.

Stamm
Festplattenspeicher
10 GB
20 GB
100 GB

Durch Klicken auf einen beliebigen Wert werden folgende Informationen angezeigt: Zeitpunkt der Änderung, Status der anderen Attribute zum Zeitpunkt der Änderung und die Change Request-Nummer, die geöffnet war, als der Speicherplatz geändert wurde.

Anzeigen von Snapshot-Details

Sie können Snapshot-Details in der Basisansicht und in der erweiterten Ansicht anzeigen. In der Basisansicht wird beispielsweise ein Snapshot einer ungeplanten Änderung an einem CI angezeigt.

So zeigen Sie Snapshot-Details an:

1. Öffnen Sie das Objekt auf der Benutzeroberfläche, und klicken Sie auf die Registerkarte "Versionskontrolle".

Im linken Seitenbereich wird eine Liste aller vorhandenen Snapshots angezeigt.

2. Klicken Sie auf einen Snapshot.

Details werden im rechten Fenster der Basisansicht bzw. der erweiterten Ansicht angezeigt. Wenn Sie nur ein Element auswählen, werden im rechten Fenster Informationen zum betreffenden Snapshot, Meilenstein (nur bei CIs) oder Standardwert angezeigt.

Die angezeigten Daten umfassen folgende Details und Indikatoren:

Leere Werte ausblenden

Ermöglicht das Filtern leerer Datenfelder. Ist diese Option nicht aktiviert, werden alle Attribute des CI angezeigt.

Hervorhebung (fett) von Werten

Zeigt an, dass ein Attribut oder eine Beziehung seit der letzten Snapshotaufnahme geändert wurde. In der Detailansicht eines Standard-CI sind alle Werte fett dargestellt.

Wert

Zeigt den vorherigen Wert des Attributs und die Uhrzeit der letzten Änderung an, wenn Sie den Cursor über den Wert führen. Die Informationen werden im Textbereich unten auf der Registerkarte "Versionskontrolle" angezeigt.

Wert "(leer)"

Zeigt an, ob ein vorheriger Wert gelöscht wurde.

Beziehungskategorie

Zeigt Informationen zur Beziehung an, einschließlich zum Typ und zum Partner-CI.

Starten von MDR im Kontext und Identifizierung von Quellen:

MDR-Anbieter kann direkt aus dem Detaileintrag des CI im Kontext starten.

Hinweis: Für in CA SDM oder früheren CA CMDB-Versionen erstellte CIs sind möglicherweise keine Informationen zu MDR und "Geändert von" vorhanden. Des Weiteren kann in CA Cohesion ACM das MDR nicht für alle Attribute und Beziehungen im Kontext gestartet werden.

Rückverfolgen von Attributänderungen zum Quell-MDR:

Erkennt, wenn ein Configuration Item-Attribut von mehr als einem MDR aktualisiert wird. Dieser Fall kann eintreten, wenn mehrere MDRs unabhängig Daten zu einer CI-Definition beitragen.

Identifizieren des maßgeblichen Quell-MDRs

Anzeigen des Status eines CI an einem bestimmten Datum (Basisansicht)

Sie können in der Basisansicht den Status eines CI an einem bestimmten Datum anzeigen.

So können Sie den Status eines CI zu einem bestimmten Datum sehen:

1. Wählen Sie ein CI aus, und rufen Sie anschließend die Seite "CI - Detail" auf.
2. Klicken Sie auf die Registerkarte "Versionskontrolle".

Die Standardansicht für das CI wird angezeigt.

3. Wählen Sie das gewünschte Datum aus.

Auf der rechten Seite der Anzeige sehen Sie nun den Status des CI zu diesem Zeitpunkt.

Anzeigen des Status eines CI zu einem bestimmten Datum (Erweiterte Ansicht)

Sie können die erweiterte Auswahl zur Anzeige des Status eines CI an einem bestimmten Datum verwenden.

So können Sie den Status eines CI zu einem bestimmten Datum sehen:

1. Wählen Sie ein CI aus, und rufen Sie anschließend die Seite "CI - Detail" auf.
2. Klicken Sie auf die Registerkarte "Versionskontrolle" und anschließend auf "Erweitert".

Die Baumstruktur "Erweiterte Ansicht" wird eingeblendet.

3. Erweitern Sie den Ordner "Datum".
4. Wählen Sie das Datum aus, für das Sie das CI anzeigen möchten.

Der Status des CI zu diesem Zeitpunkt wird angezeigt.

Starten von MDRs, die Attribute bestimmen

Verweist der Verlauf eines CI auf ein MDR, können Sie ein MDR zur Anzeige der CI-Details starten.

So starten Sie ein MDR zur Anzeige von CI-Details:

1. Wählen Sie ein CI aus, und rufen Sie anschließend die Seite "CI - Detail" auf.
2. Klicken Sie auf die Registerkarte "Versionskontrolle".
3. Klicken Sie auf "Protokoll anzeigen", oder wählen Sie den gewünschten CI-Snapshot bzw. Meilenstein aus.
4. Markieren Sie die Attributspalte, zu der Sie genauere Informationen wünschen.
5. Verweist der Verlauf eines CI auf ein MDR, klicken Sie auf die MDR-Verknüpfung.

Der MDR-Anbieter zeigt zusätzliche CI-Details an.

Drucken von Snapshots

Sie können einen Snapshot für eine ausgewähltes Datum drucken.

Gehen Sie wie folgt vor:

1. Wählen Sie das Objekt aus, und klicken Sie auf die Registerkarte "Versionskontrolle".
2. Wählen Sie die Option "Standardansicht".
3. Wählen Sie "Snapshot" aus der Dropdownliste "Snapshot-Typ" aus.
4. Wählen Sie in der Datumsliste links das gewünschte Datum aus.

5. Klicken Sie auf "Drucken".

Die Druckversion des Dokuments wird mit einem Versionskontrollbericht für das Objekt angezeigt.

6. Klicken Sie in Ihrem Webbrowser auf "Datei" > "Drucken", um das Dokument auszudrucken.

Der formatierte Text wird nun an den ausgewählten Drucker gesendet.

Drucken von CI-Meilensteinen

Sie können den Meilenstein eines CI für ein bestimmtes Datum drucken.

So drucken Sie den CI-Meilenstein eines bestimmten Datums:

1. Wählen Sie ein CI aus, und klicken Sie auf die Registerkarte "Versionskontrolle".
2. Wählen Sie entweder in der Basisansicht oder in der erweiterten Ansicht den gewünschten Meilenstein aus.
3. Klicken Sie auf "Drucken".

Die Druckversion des Dokuments wird mit einem Versionskontrollbericht für das CI angezeigt.

4. Klicken Sie in Ihrem Webbrowser auf "Datei" > "Drucken", um das Dokument auszudrucken.

Der formatierte Text wird nun an den ausgewählten Drucker gesendet.

Exportieren von Daten

Über die Seite "Versionskontrolle in CSV exportieren" können Sie die Snapshot- und Protokollinformationen in eine CSV-Datei (Comma Separated Value, durch Kommas getrennte Werte) exportieren. Die Daten werden in einer Export-Seite angezeigt. Die formatierten Daten entsprechen der Ansicht, die Sie aufgerufen haben. Zeilen werden separat angezeigt, Spaltenwerte durch Kommata getrennt und in doppelte Anführungszeichen gesetzt. Die Filter und Datenvergleiche, die Sie auf der Registerkarte "Versionskontrolle" ausgewählt haben, werden bei der Formatierung der exportierten Daten berücksichtigt.

So exportieren Sie CI-Daten:

1. Wählen Sie ein Objekt aus, und klicken Sie auf die Registerkarte "Versionskontrolle".
2. Klicken Sie auf die gewünschte Ansicht des CI.

Sie können beispielsweise auf "Protokoll anzeigen", einen Snapshot-Vergleich, einen Meilenstein (nur bei CIs) usw. klicken.

3. Klicken Sie auf "Exportieren".
Die Seite "Protokoll in CSV-Datei exportieren für CI" wird angezeigt.
4. Wählen Sie über das Kontextmenü oder die Tastatur alle Elemente aus.
5. Verwenden Sie Ausschneide- und Einfüpfungsfunktion, um die Daten aus der formatierten Seite in eine CSV-Datei oder in eine Drittanbieteranwendung zu übertragen. Sie können die Daten beispielsweise in eine Excel-Kalkulationstabelle exportieren.
Die Daten werden exportiert.

Familien-Changes und Snapshots von CIs

Änderungen der Familie können sich auf einen CI-Snapshot auswirken.

Ein Snapshot beinhaltet zwei unterschiedliche Arten von Attributen:

- gemeinsame Attribute
- familienspezifische Attribute

Wenn Sie die Familie von einem CI verändern, ändert sich der Snapshot wie folgt:

- Familienspezifische Attribute, die mit der Änderung des CI verknüpft sind.
- Snapshotdetails geben die Familie zurzeit des Snapshots wieder.

Die Familie eines CI bestimmt seine Attribute. Wenn Sie ein *familienspezifisches* Attribut und anschließend die Familie des CI ändern, dann besitzt danach das CI dieses von Ihnen geänderte *familienspezifische* Attribut nicht mehr. Das Ändern der Familie eines CI hat keine Auswirkungen auf die *gemeinsamen* Attribute.

Beispiel: Ändern Sie die mit einem CI verknüpfte Familie

Dieses Beispiel zeigt, wie Änderungen der Familie eines CI sich auf den Snapshot eines CI auswirken.

Uhrzeit	Status/Änderungen
0	Das CI befindet sich in Familie 1.
1	Der Wert eines familienspezifischen Attributs der Familie 1 wird geändert.
2	Die Werte mehrerer gemeinsamer Attribute werden geändert.
3	Die CI-Familie wird von Familie 1 zu Familie 2 geändert. Mit dieser Änderung stehen dem CI die familienspezifischen Attribute der Familie 1 nicht mehr zur Verfügung.
4	Der Wert eines familienspezifischen Attributs der Familie 2 wird geändert.
5	Mehrere gemeinsame Attribute werden geändert

- 6 Die CI-Familie wird zurück auf Familie 1 geändert. Mit dieser Änderung stehen dem CI die Werte der familienspezifischen Attribute der Familie 2 nicht mehr zur Verfügung. Die Werte der familienspezifischen Attribute der Familie 1 werden jedoch wiederhergestellt.
- 7 Mehrere gemeinsame Attribute werden geändert
- 8 Ein familienspezifisches Attribut der Familie 1 wird geändert.

Das Beispiel zeigt, dass ein Snapshot zum Zeitpunkt 7 keine Informationen über die Änderungen zu den Zeitpunkten 3 oder 4 enthält. Diese Änderungen betrafen familienspezifische Attribute der Familie 2.

Vergleichen von Snapshots (Basisansicht)

Sie können zwei oder mehrere Snapshots, Meilensteine oder Standard-CIs miteinander vergleichen.

So vergleichen Sie Snapshots, Meilensteine oder Standard-CIs:

1. Wählen Sie ein CI aus, und rufen Sie anschließend die Seite "CI - Detail" auf.
2. Klicken Sie auf die Registerkarte "Versionskontrolle".
3. Wählen Sie einen Meilenstein oder einen Snapshot in der Dropdownliste "Snapshot-Typ" aus.

Es werden Meilensteine oder Snapshots aufgelistet.

4. Wählen Sie zwei oder mehrere Snapshots, Meilensteine oder Standard-CIs aus.

In der Vergleichsansicht wird folgendes Ergebnis angezeigt:

- Eine Spalte zeigt an, inwiefern sich die Snapshots oder Meilensteine unterscheiden.
- In jeder Zeile finden Sie die Attributwerte der ausgewählten Snapshots.
- Nur Attribute, deren Werte sich unterscheiden, werden angezeigt. Das Datum wird stets angezeigt, es sei denn, die betreffenden Snapshots sind identisch.
- Da Vergleiche von Standard-CIs nicht zeitspezifisch sind, wird in den Datumfeldern immer **Standard-CI** angezeigt.
- Sie können die Ergebnisse eines Vergleichs ausdrucken, oder in eine CSV-Datei exportieren.

Vergleichen von Snapshots (Erweiterte Ansicht)

Sie können zwei oder mehrere Snapshots, Meilensteine oder Standard-CIs miteinander vergleichen.

So vergleichen Sie Snapshots, Meilensteine oder Standard-CIs in der erweiterten Ansicht:

1. Wählen Sie ein CI aus, und rufen Sie anschließend die Seite "CI - Detail" auf.
2. Klicken Sie auf die Registerkarte "Versionskontrolle" und anschließend auf "Erweitert".

Die erweiterte Auswahl zeigt das CI an.

3. Navigieren Sie in der Ordnerhierarchie zu dem Wert, den Sie für den Snapshot-Vergleich verwenden möchten.
4. Wählen Sie für jeden Snapshot-Vergleich einen Wert aus.

Der Vergleich für das CI wird angezeigt, z. B. ein Snapshot-Vergleich auf der Grundlage der ausgewählten Ordnerwerte.

In der Vergleichsansicht wird folgendes Ergebnis angezeigt:

- Eine Spalte zeigt an, inwiefern sich die Snapshots oder Meilensteine unterscheiden.
- In jeder Zeile finden Sie die Attributwerte der ausgewählten Snapshots.
- Nur Attribute, deren Werte sich unterscheiden, werden angezeigt. Das Datum wird stets angezeigt, es sei denn, die betreffenden Snapshots sind identisch.
- Da Vergleiche von Standard-CIs nicht zeitspezifisch sind, wird in den Datumfeldern immer **Standard-CI** angezeigt.
- Sie können die Ergebnisse eines Vergleichs ausdrucken, oder in eine CSV-Datei exportieren.

Hinweis: In der erweiterten Ansicht kann eine Beziehung zwischen zwei CIs ohne zugeordneten Beziehungstyp vorliegen (z. B. in CA NSM erstellte CIs). Solche Beziehungsknoten werden als (leer) identifiziert.

CA SDM Change Management

Für jedes CI, das mit einem CA Service Desk-Change-Ticket verknüpft ist, werden automatisch Daten der Versionskontrolle erzeugt. Während sich der Status des Change-Tickets von "Offen" in "Aktiv", "Gelöst" und dann in "Geschlossen" ändert, wird für jedes zugehörige CI ein Snapshot angefertigt. Mit der Versionskontrolle haben Sie folgende Möglichkeiten:

- Vergleichen des Status des CI mit dem Standard-CI an einem beliebigen Punkt des Change Management-Lebenszyklus.
- Hilft Ihnen dabei sicherzustellen, dass das CI die Bedingungen erfüllt, und beim Identifizieren von Attributen, die korrigiert werden müssen.
- Vergleichen des Status eines CIs an beliebigen Punkten im Lebenszyklus des Change sowie zu frei wählbaren Zeitpunkten dazwischen.
- Anzeigen des Fortschritts in jeder Phase des Change einschließlich bei Meilensteinen.

Die Integration von CA Service Desk und CA CMDB wird dadurch veranschaulicht, dass gezeigt wird, wie Sie Changes überprüfen können, die während des Service Management-Lebenszyklus eines CI ausgeführt wurden. In diesem Beispiel wird ein Change Request verwendet, um Komponenten eines Hardwareservers zu aktualisieren.

So erstellen Sie einen Change und verknüpfen ihn mit einem CI

1. Erstellen Sie ein Service Desk-Change-Ticket, indem Sie auf "Datei" und anschließend auf "Neuer Change" klicken.
2. Geben Sie die Change Request-Daten und die Auftragszusammenfassung ein, z. B. "Festplatten-Upgrade auf 500 GB".
3. Klicken Sie auf die Registerkarte "Configuration Items" und dann auf "CIs aktualisieren".
4. Legen Sie Suchkriterien für das CI fest (z. B. Name des Servers), und klicken Sie auf "Suchen".
5. Wählen Sie im Formular "Betroffene Configuration Items - Aktualisierung" alle CIs, die mit dem Change-Ticket verknüpft sind (z. B. der Server aus Schritt 4), und fügen Sie sie der Liste der betroffenen Configuration Items hinzu. Klicken Sie auf "OK".
6. Speichern Sie den Change Request.

So führen Sie Änderungen durch:

1. Führen Sie die Änderungen für das CI durch. Installieren Sie z. B. die Festplatte physisch im Computer, und aktualisieren Sie dann das Attribut "Festplattenkapazität" des Hardwareserver-CI.
2. Schließen Sie den Change Request.
3. Vergewissern Sie sich, dass die Änderung vollständig durchgeführt wurde. Rufen Sie hierzu das CI auf, klicken Sie auf die Registerkarte "Versionskontrolle", und vergleichen Sie die CI-Snapshots vor und nach der Änderung.

Der Vergleich des CI-Status vor dem Öffnen und nach dem Schließen des Change zeigt, dass die Festplattenkapazität des Hardwareservers vor der Änderung 100 GB betrug und nach Abschluss der Änderung 500 GB. Auch das Datum und die Uhrzeit der Änderungen werden angezeigt. Alle anderen Attribute, die sich zwischen dem Öffnen und Schließen des Change geändert haben, werden ebenfalls angezeigt.

Anzeigen von CI-Attributen in anderen CA-Produkten

Auf der Seite "Common Asset Viewer" können Sie die Attribute von Configuration Items in anderen CA-Produkten anzeigen.

So rufen Sie Configuration Item-Attribute in anderen CA-Produkten auf:

1. Finden und öffnen Sie das CI.
2. Klicken Sie auf "Anlagenansicht".
Die Seite "Common Asset Viewer" wird angezeigt.
3. Nutzen Sie die Links auf der Registerkarte "Eigene Ressourcen", um Attributinformationen in anderen CA-Produkten zu finden.
4. Sind Sie fertig, klicken Sie auf "Fenster schließen".

Sie haben Configuration Item-Attribute in anderen CA-Produkten angezeigt.

Verwenden des CMDBf-Viewers

CA SDM stellt den CMDBf-Viewer bereit, um die Ergebnisse der CI-Föderation in den MDRs anzuzeigen. Klicken Sie auf einer CI- Detailseite (oder in der CI-Liste in dem CI-Kontextmenü) auf den CMDBf-Viewer, um die CI-Attribute der föderierten CMDBs und MDRs parallel anzuzeigen. Auf der Seite der föderierten Ansicht können Sie auf "Abrufen" klicken, um die Information der föderierten MDRs zu aktualisieren. Zur besseren Lesbarkeit können CA CMDB-Metadatendateien MDR-Attributnamen und CA CMDB-Attributnamen abstimmen.

Hinweis: Diese Funktion erfordert MDRs, die Abfragen unterstützen. Konfigurieren Sie die MDR-CMDBf-Endpunkte entsprechend, um ihre Ergebnisse in der föderierten Ansicht anzuzeigen. Weitere Informationen finden Sie im *Implementierungshandbuch*.

Wenn das CI keine föderierten Daten aufweist, zeigt der Viewer nur CA CMDB-Attribute an.

CMDB Visualizer

Mit CA SDM können Sie Ihre IT-Komponenten (*Configuration Items* oder CIs, Configuration Items) an Ihre Business-Dienste anpassen. CA CMDB definiert *Beziehungen* zwischen CIs, wie wenn etwa eine Gruppe von CIs für die Bereitstellung eines Business-Service sorgt. Mit CA CMDB Visualizer können Sie die gesamte Übersicht über Ihre CI-Beziehungen anzeigen. Zudem stellt das Produkt Funktionen zur Verwaltung von Beziehungen bereit. Wenn Sie mit einem *Fokus-CI* (ein beliebiges CI) arbeiten, können Sie den Visualizer verwenden, um bis zu neun Ebenen verbundener CIs anzuzeigen.

Hinweis: (Nur für Konfiguration für erweiterte Verfügbarkeit) Wenn der Visualizer einen Server-Request während der Stilllegung des Anwendungsservers erstellt, dann wird folgende Meldung angezeigt:

„Das Herunterfahren dieses CMDB Visualizer-Servers zu Wartungszwecken ist in xx:xx geplant. Speichern Sie Ihre Arbeit, und melden Sie sich ab.“.

Sie können das Meldungsfeld ausblenden, aber die Meldung wird während der Stilllegung im oberen Bereich angezeigt. Wenn die Stilllegung des Servers abgebrochen wird, erhalten Sie eine Meldung über den Abbruch.

CA verwendet ein Modell für über- und untergeordnete Elemente, um die Beziehungen zwischen CIs zu definieren. Alle Configuration Items, die an einem Business-Dienst beteiligt sind, sind *übergeordnete Elemente* für diesen Business-Dienst (dem *untergeordneten Element*). Entsprechend können übergeordnete Elemente auch gleichzeitig *untergeordnete Elemente* sein, die auf anderen CIs aufbauen. Mit Hilfe von Visualizer können Sie die folgenden Übergeordnet/Untergeordnet-Analysen durchführen:

Durchsuchen

Zeigt eine ungefilterte Ansicht aller CIs.

Auswirkungsanalyse

Beginnt mit einem Fokus-CI (übergeordnetes Element) und sucht nach den zugehörigen untergeordneten Elementen.

Ursache

Beginnt mit einem Business-Service (als untergeordnetem Element) und zeigt alle CIs an, die als übergeordnete Elemente dieses Services dienen.

Ursachen- und Auswirkungs-CIs

Kombiniert Auswirkungsanalyse und Ursache in einer Suche.

Beziehung verfolgen

Alle möglichen Beziehungen (nach Ebenen) werden angezeigt. Wenn Sie nur ein CI auswählen, zeigt dieser Filter die Ansicht "Durchsuchen".

Kürzester Pfad

Die kürzeste Kette an Beziehungen (nach Ebenen) wird angezeigt.

Mit CMDB Visualizer können Sie die folgenden Aktionen ausführen:

- Anzeigen von mehreren CI-Ebenen in einer konfigurierbaren graphischen Ansicht.
- Überwachen oder Abbrechen des Rendering-Fortschritts.
- Suchen mit flexiblen Kriterien.
- Filtern nach CI-Familien, Beziehungstypen und anderen Attributen.
- Anzeigen von CI-Beziehungen.
- Nachverfolgen einer Beziehung zwischen zwei CIs.
- Anzeigen einer Abhängigkeitskette.
- Direktes Aufrufen von CA CMDB vom Visualizer aus.
- Anzeigen von CI-Attributen und -Eigenschaften.
- Speichern von Diagrammmetadaten
- Drucken des Diagrammlayouts
- Möglichkeit, in einem angezeigten Diagramm nach einem bestimmten CI zu suchen.

- Erstellen eines CI (je nach Rolle).
- Erstellen von neuen CI-Beziehungen (je nach Rolle).
- Verwenden des Notizblocks, um wichtige CIs zu speichern.
- Anzeigen des CI-Status.
- Ein- oder Ausblenden eines CI im Visualizer-Layout.
- Rollenbasierte Datensicherheit
- Starten eines externen MDRs.
- Aufrufen der Onlinehilfe für Visualizer-Funktionen.

Weitere Informationen:

[Durchführen der Ursachenanalyse](#) (siehe Seite 658)

[Visualizer-Administration](#) (siehe Seite 659)

Durchführen der Ursachenanalyse

Bei Verwendung des Visualizers mit dem CMDBf-Viewer, können Sie eine Ursachenanalyse ausführen.

So führen Sie eine Ursachenanalyse durch:

1. Wechseln Sie in Visualizer zu einem Service-CI, dass sich in einer Fehlerbedingung befindet (das beispielsweise langsam oder nicht verfügbar ist).
2. Klicken Sie die rechte Maustaste auf das Configuration Item, und wählen Sie aus dem Kontextmenü den Befehl "Fokus-CI erstellen".
3. Legen Sie einen Ursachenfilter mit den folgenden Kriterien fest:
 - Klassentyp: N/V
 - Abhängiger zu Anbieter-Beziehung: Alle für die Ursachenanalyse anzuzeigenden Beziehungen.

4. Klicken Sie auf "Anzeigen".

In dem anhand dieser Einstellungen erzeugten Diagramm werden alle CIs, die in einer Relation zu den Fokus-CIs stehen, wie über den Filtern angegeben angezeigt. Die Pfade zwischen CIs beinhalten die dazwischen liegenden CIs bis zur Standardebene.

5. Navigieren Sie durch die CIs und untersuchen Sie sie auf Incidents, Probleme, oder letzte Änderungen, um Hinweise auf mögliche Kandidaten für die Ursachenanalyse zu der Fokus-CI-Bedingung zu erhalten.
6. Starten Sie CA CMDB im Kontext eines bestimmten CI.
7. Klicken Sie auf "CMDBf-Viewer".

Die Seite wird in der föderierten Ansicht angezeigt. Sie enthält eine Liste der MDR-Anbieter für das CI.

8. Klicken Sie auf "Abrufen", um die neuesten MDR-Attribute abzurufen.
Die MDR-Attribute werden aktualisiert.

Visualizer-Administration

Mit der Administrationsschnittstelle von Visualizer können Sie die Einstellungen von CA CMDB Visualizer bearbeiten. Diese Funktionen stehen nur Rollen mit Administratorrechten zur Verfügung.

Folgende Registerkarten werden auf dem Visualizer deaktiviert, der auf Sekundärservern ausgeführt wird. Diese Registerkarten werden auf allen anderen CA SDM-Servern aktiviert:

Registerkarte "Visualizer-Konfiguration"

Ermöglicht die Einstellung des Servers und der Display-Informationen zu Configuration Items.

Registerkarte "Beziehung - Stil"

Definiert die grafischen Eigenschaften von Beziehungen.

Die Registerkarte "Configuration Item-Status"

Definiert die grafischen Eigenschaften von Configuration Items.

Registerkarte "Filter"

Erstellt, bearbeitet und löscht Filter zur Analyse von Configuration Items.

Registerkarte "Symbolkonfiguration"

Ordnet dem entsprechenden Symbolbild eine CI-Familie zu, wenn CMDB Visualizer von Version r11.2 auf Version 12.9 aktualisiert wurde.

Hinweis: Weitere Informationen zu Visualizer-Definitionen finden Sie in der Online-Hilfe zu CMDB Visualizer.

Hinzufügen von ermittelten Assets

Fremde Anlagen in der Management Database (MDB) können Sie in eigene CIs umwandeln.

So fügen Sie ein ermitteltes Asset hinzu

1. Klicken Sie auf die Schaltfläche "Ermittelte Assets" auf der Seite "Configuration Items - Liste".

Das Fenster "Ermittelte Assets - Suche" wird angezeigt.

2. Klicken Sie auf "Suchen". Eine Liste der ermittelten Anlagen wird nun angezeigt.
3. Wählen Sie aus der Liste das Asset aus, das Sie als Configuration Item hinzufügen möchten. Klicken Sie mit der rechten Maustaste auf das Asset, und wählen Sie im daraufhin angezeigten Kontextmenü "Neues Configuration Item erstellen" aus.

Die Seite "Neues Configuration Item erstellen" wird geöffnet. In einigen Feldern finden Sie nun Informationen zu dem Element.

4. Füllen Sie alle verbleibenden Felder aus, die für das neue CI von Bedeutung sind. Klicken Sie anschließend auf "Fortfahren".

Hinweis: Für das Erstellen eines Configuration Item werden nur die Werte "Name" und "Klasse" benötigt.

5. Geben Sie bei Bedarf Daten in die entsprechenden Felder auf der Registerkarte "Attribute" ein.

Die Familie der Klasse, die Sie für das Configuration Item ausgewählt haben, bestimmt die Attribute, die auf der Registerkarte angezeigt werden. Welche Informationen Sie hier eintragen, hängt von Ihren Geschäftsprozessen und den Informationen ab, die Sie für ein CI speichern und anzeigen möchten.

6. Klicken Sie auf "Speichern".

Das ermittelte Asset wird hinzugefügt.

Asset- und CI-Markierungen

Zwei gängige Attributmarkierungen können den CI-/Asset-Typ für Filterzwecke weiter kategorisieren und steuern, welche Entitäten in CA SDM oder anderen Produkten, z. B. CA APM, angezeigt werden.

Folgende Markierungen werden verwendet:

CI? (Ja/Nein)

Identifiziert Configuration Items.

Asset? (Ja/Nein)

Identifiziert Assets.

Standardmäßig wird ein in CA CMDB erstelltes CI als CI und nicht als Asset markiert. Sie können dies im Bedarfsfall außer Kraft setzen. Ein CI kann auch ein Asset sein. In CA CMDB kann das Asset-Flag nicht mehr geändert werden, nachdem es auf "ja" festgelegt wurde. Das Asset-Flag wird in der Regel auf "ja" festgelegt, wenn ein Asset von CA APM erstellt wurde.

Diese Markierungen sind auf allen CI-Detailformularen und in der CI-Suchfunktion verfügbar. Die Werte dieser Markierungen können im CI-Detailformular, in GRLoader und in CA CMDB-Webservices aktualisiert werden. Die Funktion "In Liste bearbeiten" unterstützt ferner das Aktualisieren neuer Markierungen in mehreren Datensätzen.

Der Objektattributname für die CI-Markierung ist **is_ci**. Der Objektattributname für die Asset-Markierung ist **is_asset**. Diese Namen sind SREL-Attribute, die auf bool verweisen. Diese Attributnamen können als XML-Tags von GRLoader verwendet werden. Fügen Sie zum Definieren des neuen CI die folgende XML hinzu, um zum Beispiel den Standardwert der Asset-Markierung beim Erstellen eines CI mit GRLoader ändern:

```
<is_asset>JA</is_asset>
```

Abstimmung von CIs

Das Ziel der Abstimmung besteht darin, sicherzustellen, dass Aktualisierungen aus mehreren Datenquellen, die sich alle auf dasselbe Geschäftsobjekt beziehen, nur ein einziges CI aktualisieren, auch wenn sie verschiedene Formen der Informationsidentifizierung verwenden. *Mehrdeutigkeit* weist auf die Möglichkeit hin, dass ein CI nicht einmalig ist. Ein CI können mögliche "Duplikate" im CMDB haben, und CI-Transaktionen können mehr als ein mögliches Ziel-CI haben. Wenn diese Ergebnisse nicht kontrolliert werden, können Fehler in der CMDB auftreten, was den Nutzen der CMDB mindert und zu ungeeigneten Geschäftsaktionen führen kann.

Die automatische CI-Abstimmung ist ein enormer Pluspunkt für CA CMDB, da sie im Vergleich zur manuellen Datenwartung wesentlich zeitsparender ist. Der Prozess der CI-Abstimmung verwendet einige spezifische identifizierende Attribute. Die automatische Abstimmung kann jedoch zu einem der folgenden Ergebnisse führen:

- Falsch positive Übereinstimmungen
Vorhandene CIs werden aktualisiert, anstatt ein CI zu erstellen.
- Falsch negative Übereinstimmungen
Neue CIs werden erstellt, anstatt ein vorhandenes CI zu aktualisieren. Die Gruppe von CIs mit ähnlichen identifizierenden Attributen ist mehrdeutig, weil sie dem gleichen tatsächlichen Geschäftsobjekt mit ähnlichen identifizierenden Attributen gleichen.

CA Service Desk Manager unterstützt die folgenden Abstimmungsansätze:

MDR-basierte Abstimmung (passiv)

Ermöglicht der CMDB, alle mehrdeutigen Daten anhand des MDR-basierten Abstimmungsvorgangs abzustimmen.

Identifizieren und Lösen von mehrdeutigen CIs (reaktiv)

Identifizieren und lösen Sie mehrdeutige CIs durch Identifizierung und Verwaltung vorhandener CIs in der CMDB.

Prüfen und Ändern eingehender Daten anhand eines Transaktionsarbeitsbereichs (Proaktiv)

Überprüfen und ändern Sie eingehende Daten anhand eines Transaktionsarbeitsbereichs (TWA), bevor Sie sie in die CMDB laden.

Weitere Informationen:

[MDR-basierte Abstimmung](#) (siehe Seite 662)

[Identifizieren und Auflösen von mehrdeutigen CIs](#) (siehe Seite 664)

[Überprüfen und Ändern von eingehenden Daten mit dem Transaktionsarbeitsbereich \(TWA\)](#) (siehe Seite 676)

MDR-basierte Abstimmung

MDR-basierte Abstimmung erfolgt im Management Data Repository, um das weitere Auftreten von mehreren CIs in der MDB zu reduzieren, die auf das gleiche Objekt in der physischen Welt verweisen.

MDR-basierte Abstimmung behandelt das MDR als vertrauenswürdige Quelle, die immer die gleiche föderierte Asset-ID benutzt, wenn sie Informationen über ein einzelnes CI übermittelt. Alle Aktualisierungen aus einem bestimmten MDR auf eine bestimmte föderierte Asset-ID aktualisieren immer die gleiche CI, sogar wenn identifizierende Attribute geändert werden.

Die in diesen Abschnitten beschriebene MDR-basierte Abstimmung, das Abstimmungs-Management und der Transaktionsarbeitsbereich (TWA) ermöglichen es Ihnen, den Abstimmungsprozess zu steuern. Um das Abstimmungs-Management und den TWA allerdings erfolgreich zu verwenden, müssen Sie zunächst verstehen, wie CA SDM Abstimmungsattribute verwendet.

Wichtig Wenn Sie einen externen Datenanbieter neu installieren oder neu starten (z. B. CA Cohesion ACM), dann deaktivieren und reaktivieren Sie dessen MDR-Definition in der CMDDB. Wenn das MDR seine föderierten Asset-IDs wiederverwendet, kann es unabsichtlich zu einer CI-Datenüberlagerung kommen.

Weitere Informationen:

[Funktionsweise des CI-Vergleichs durch MDR-Abstimmung](#) (siehe Seite 663)

[Funktionsweise der CI-Identifizierung durch MDR-Abstimmung](#) (siehe Seite 663)

Funktionsweise des CI-Vergleichs durch MDR-Abstimmung

MDR-basierte Abstimmung identifiziert das entsprechende übereinstimmende CI mithilfe des folgenden Vorgangs:

1. Wenn bei einer Transaktion eine ID angegeben wird, wurde das CI identifiziert und die Abstimmung ist abgeschlossen.
2. Wenn bei einer Transaktion keine ID angegeben wird, überprüft CA SDM, ob die föderierten Identifikationsattribute angegeben wurden und mit einem CI übereinstimmen. Wird eine Übereinstimmung gefunden, stimmt die Transaktion das übereinstimmende CI ab.
3. Wenn bei einer Transaktion weder eine ID noch föderierte identifizierende Attribute angegeben werden, verwendet die CI-Transaktion die im folgenden Abschnitt beschriebenen [Identifikationsattribute](#) (siehe Seite 663).

Funktionsweise der CI-Identifizierung durch MDR-Abstimmung

Die MDR-basierte Abstimmung verwendet die folgende Dringlichkeit zur Identifizierung eines CI:

1. ID (wenn bei einer Transaktion eine ID angegeben wird, war die Abstimmung erfolgreich)
2. Föderierte Identifikationsattribute
 - Föderierte Asset-ID
 - MDR-Name
 - MDR-Klasse
3. CI-identifizierende Attribute
 - Mandant (wenn die Mandantenfähigkeit installiert ist)
 - Name
 - Seriennummer
 - MAC-Adresse
 - Systemname
 - Alternative Asset-ID
 - DNS-Name

Identifizieren und Auflösen von mehrdeutigen CIs

Wir empfehlen, das Verfahren zur Verwaltung der Mehrdeutigkeit von Fall zu Fall zu wählen. In jedem Fall muss der Konfigurations-Administrator herausfinden, ob Mehrdeutigkeit vorliegt und den besten Ansatz bestimmen. CA SDM bietet einen breiten Lösungsansatz, um bereits im CMDB vorhandene mehrdeutige CIs zu identifizieren und zu verwalten.

Der *Mehrdeutigkeitsindex* ist eine funktionale Messung der möglichen Nicht-Einmaligkeit eines Configuration Items (CI), die auf seinen identifizierenden Attributen basiert. Der Mehrdeutigkeitsindex kann die Wahrscheinlichkeit von "gedoppelten" CIs im CMDB messen, oder die Wahrscheinlichkeit, dass eine Transaktion mehrere CI-Ziele hat.

Wichtig! Wenn Sie CIs mit Datenbankabfragen manuell löschen, können Fehler in CI-Mehrdeutigkeitsindizes auftreten. Um diese Fehler zu vermeiden, führen Sie das Hilfsprogramm `cmdb_update_ambiguity` aus, und setzen Sie den Parameter `-full` auf 1. Dieser Parameter hilft dabei, sicherzustellen, dass Sie korrekte Mehrdeutigkeitsindizes bekommen, wenn Sie `cmdb_update_ambiguity.bat` oder das Shell-Skript ausführen.

Verwenden Sie den folgenden Prozess, um mehrdeutige CIs zu identifizieren und zu lösen:

1. Identifizieren Sie mehrdeutige CIs.
 - Berechnen Sie den Mehrdeutigkeitsindex für alle CIs.
 - Überprüfen Sie die Liste der mehrdeutigen CIs auf dem Scoreboard.
2. Entscheiden Sie, ob die identifizierenden Attribute für jedes einzelne CI gültig sind.
3. Lösen Sie das mehrdeutige CI mit einer der folgenden Aktionen:
 - Ändern der identifizierenden Attribute
 - Ausschließen eines CI von der Mehrdeutigkeitsverwaltung
 - Ablehnen einer CI-Aktualisierung durch Deaktivierung des CI
 - Ersetzen von CIs

Weitere Informationen:

[Beispiel für CI-Mehrdeutigkeit](#) (siehe Seite 665)

[Identifizieren mehrdeutiger CIs und Überprüfen der Gültigkeit ihrer identifizierenden Attribute](#) (siehe Seite 666)

[Lösen von mehrdeutigen CIs](#) (siehe Seite 673)

Beispiel für CI-Mehrdeutigkeit

Daten aus vier unterschiedlichen Datenquellen werden in die CMDB geladen. Jede Datenquelle verwendet ihre eigene Teilmenge identifizierender Merkmale. Aufgrund dieser Inkonsistenz sind mehr CIs als nötig in der CMDB vorhanden.

Die folgenden Beispiele zeigen die CI-Mehrdeutigkeit:

Beispiel: Mehrdeutige CIs

Folgende vier CIs sind in der CMDB abgelegt:

- Name(Server1) DNS Name(dns1) Serial Number(serial1)
- Name(Server1) DNS Name(dns1)
- Name(Server2) DNS Name(dns1) Serial Number(serial1)
- Name(Server3) MAC Address(mac1)

Auf Grund gemeinsamer identifizierender Merkmale sind die zwei Instanzen von Server1 und Server2 mehrdeutig. Server3 ist nicht mehrdeutig.

Jedem CI ist ein Mehrdeutigkeitsindex zugewiesen. Der Mehrdeutigkeitsindex ist ungefähr die Anzahl vorhandener CIs, bei denen irgend ein identifizierendes Attribut übereinstimmt. Je größer der Index, desto mehr CIs mit übereinstimmenden Kennungen sind vorhanden, und desto größer ist die Wahrscheinlichkeit, dass CI-Daten inkonsistent eingegeben und zusätzliche CIs inkorrekt erstellt wurden. CIs mit einem Mehrdeutigkeitsindex von Null sind einmalig bezüglich aller Kennungen und daher eindeutig.

Der Mehrdeutigkeitsindex für die einzelnen obigen CIs ist:

- Erste Instanz von Server1: Zählung anderer CIs mit übereinstimmendem Namen-+ DNS-Name +-Seriennummer = $1+2+1=4$
- Zweite Instanz von Server1: Zählung anderer CIs mit übereinstimmendem Namen + DNS-Namen = $1+2=3$
- Server2: Zählung anderer CIs mit übereinstimmendem Namen-+ DNS-Name +-Seriennummer = $0+2+1=3$
- Server3; Zählung anderer CIs mit übereinstimmendem Namen + MAC-Adresse = $0+0=0$

Weitere Informationen:

[Berechnen des Mehrdeutigkeitsindex](#) (siehe Seite 667)

[Anzeigen mehrdeutiger Transaktionen über die Registerkarte "Administration"](#) (siehe Seite 671)

[Anzeigen mehrdeutiger CIs über das Scoreboard](#) (siehe Seite 672)

Identifizieren mehrdeutiger CIs und Überprüfen der Gültigkeit ihrer identifizierenden Attribute

Überprüfen Sie ein beliebiges CI mit einem Mehrdeutigkeitsindex ungleich null, ob es eindeutig ist oder aufgrund einer falschen Abstimmung versehentlich erstellt wurde. CIs sind nicht von sich aus mehrdeutig, sondern mit anderen CIs. Ein System kann viele Gruppen von mehrdeutigen CIs haben, von denen jede CIs mit gemeinsamen Werten für identifizierende Attribute enthält.

Wenn Sie die Mehrdeutigkeit eines CI untersuchen, untersuchen Sie auch die Mehrdeutigkeit von anderen CIs in derselben Gruppe. Wenn Sie die Mehrdeutigkeit eines einzelnen CIs lösen, reduzieren oder beseitigen Sie die Mehrdeutigkeit anderer CIs in der Gruppe.

CA SDM bietet Tools für das Abstimmungs-Management, mit deren Hilfe Sie mehrdeutige CIs und die zugehörige Gruppe von CIs finden können. Sie können die zu Grunde liegende Ursache für die Mehrdeutigkeit untersuchen und lösen.

Führen Sie bei der Verwaltung von Mehrdeutigkeit folgende Schritte aus:

1. Berechnen Sie den Mehrdeutigkeitsindex für alle CIs.
2. Zeigen Sie die Liste der mehrdeutigen CIs im Scoreboard an. Im Scoreboard werden alle mehrdeutigen CIs in absteigender Reihenfolge ihrer Mehrdeutigkeit aufgelistet.
3. Führen Sie beginnend mit dem CI mit der höchsten Mehrdeutigkeit im Scoreboard folgende Schritte aus:
 - a. Überprüfen Sie alle CIs in der zugehörigen Mehrdeutigkeitsgruppe. Im CI-Detailformular eines CI werden auf der Registerkarte "Abstimmung" alle weiteren CIs in der Mehrdeutigkeitsgruppe aufgelistet.
 - b. Ermitteln Sie, ob alle CIs in der Gruppe legitim sind oder bei der Abstimmung Fehler gemacht wurden. Überprüfen Sie die identifizierenden Attribute und ermitteln Sie, ob die CIs in der Gruppe richtig erstellt wurden oder ihre Erstellung aufgrund einer falschen negativen Übereinstimmung bei der Abstimmung erfolgt ist.
4. Stellen Sie ggf. fest, welche CIs in der Gruppe falsch negativ sind.

Wenn Sie festgestellt haben, dass es bei der Abstimmung zu einer falsch negativen Übereinstimmung gekommen ist und zusätzliche CIs erstellt wurden, ermitteln Sie, welche CI das gültige ist und welche CIs fälschlicherweise erstellt wurden. Berücksichtigen Sie Faktoren wie identifizierende Attribute und andere Attribute, wie das Datum der letzten Aktualisierung, verwandte Probleme, Issues und sonstige Aspekte des CI.

Berechnen des Mehrdeutigkeitsindex

Bevor Sie mit der Verwaltung von Mehrdeutigkeit beginnen können, aktualisieren Sie den Mehrdeutigkeitsindex für die vorhandenen CIs und CI-Transaktionen. Zum Aktualisieren des Mehrdeutigkeitsindex für CIs und CI-Transaktionen müssen Sie den Befehl "cmdb_update_ambiguity" ausführen.

Wichtig! Sie müssen den Befehl "cmdb_update_ambiguity" mindestens einmal ausführen, um die Mehrdeutigkeit von CIs oder CI-Transaktionen zu messen. Wenn Sie den Befehl nicht ausführen, sind alle Mehrdeutigkeitsindizes 0 (null), was keine Mehrdeutigkeit impliziert.

Sie können das Dienstprogramm vor und während der Mehrdeutigkeitsverwaltung ausführen. Planen Sie eine regelmäßige Ausführung des Dienstprogramms, damit die Mehrdeutigkeitsindizes den aktuellen Zustand Ihres Systems widerspiegeln.

So verwenden Sie den Mehrdeutigkeitsindex

1. Legen Sie die erforderlichen Parameter zum Ausführen des Dienstprogramms fest.
2. Führen Sie das Dienstprogramm aus.
3. Starten Sie den CA SDM-Webclient und navigieren Sie zu den Listen der mehrdeutigen CIs oder mehrdeutigen CI-Transaktionen, um die Mehrdeutigkeit zu verwalten.

Weitere Informationen:

[Identifizieren und Auflösen von mehrdeutigen CIs](#) (siehe Seite 664)

Befehl "cmdb_update_ambiguity"

Sie können Mehrdeutigkeitsindizes für CIs und CI-Transaktionen berechnen, indem Sie eine Befehlssyntax wie die folgende eingeben:

```
cmdb_update_ambiguity [Parameter] -m {ci | twa | all}
```

Weitere Informationen über Befehlsparameter finden Sie in ["cmdb_update_ambiguity"-Parameter](#) (siehe Seite 669).

Standardmäßig werden CIs vom letzten Datum der Durchsuchung ab durchsucht. Wenn "-full 1" angegeben ist, wird eine vollständige Durchsuchung ausgeführt.

Beispiel: Berechnen Sie die CI-Mehrdeutigkeit für eine Microsoft SQL Server-Datenbank.

Der folgende Befehl berechnet den Mehrdeutigkeitsindex für alle vorhandenen CIs und Transaktionen im TWA:

```
cmdb_update_ambiguity -m all -d MSSQL -u servicedesk -p dbpassword -s dbserver1
```

Beispiel: Berechnen Sie die CI-Mehrdeutigkeit auf einer Oracle-Datenbank

Der folgende Befehl berechnet den Mehrdeutigkeitsindex für CIs und gibt Datenbankinformationen an.

```
cmdb_update_ambiguity -m ci -d Oracle -u mdbadmin -p dbpassword -s server1 -port 1521 -SID orcl
```

Verwenden einer Konfigurationsdatei

Sie können viele Parameter des Typs "cmdb_update_ambiguity" in einer Konfigurationsdatei angeben. Sie können die Konfigurationsdatei verwenden, um Parametereinstellungen in einer verschlüsselten Form mit Hilfe von Betriebssystem-Tools zu sichern. Die gültigen Schlüsselwörter und die entsprechenden Befehlszeilenoptionen werden in der Parametertabelle aufgelistet.

Hinweis: Wenn Sie einen Parameter in der Befehlszeile und in einer Konfigurationsdatei angeben, setzt der Befehlszeilenwert den Wert in der Konfigurationsdatei außer Kraft.

Beispiel: Verwenden Sie eine Konfigurationsdatei, um die Parameter für eine Microsoft SQL Server-Datenbank anzugeben.

Der folgende Befehl führt die Konfigurationsdatei "ambiguity_mssql.cfg" aus.

```
cmdb_update_ambiguity -m all -c ambiguity_mssql.cfg
```

Format der Konfigurationsdatei

Optionen für die Konfigurationsdatei werden als *keyword=value* (Schlüsselwort=Wert) angegeben. Unter Windows kann das Verzeichnistrennzeichen ein doppelter umgekehrter Schrägstrich (\\) oder ein einzelner vorwärtsgerichteter Schrägstrich sein (/). Der Pfadname darf nicht in doppelte Anführungszeichen eingeschlossen werden ("").

Gültige Schlüsselwörter und die entsprechenden Befehlszeilenoptionen werden in der Parametertabelle aufgelistet.

Hinweis: Eine Raute (#) in Spalte 1 startet eine Kommentarzeile.

Beispiel: Microsoft SQL Server-Konfigurationseinstellungen

```
#Sample-Konfigurationsdatei für Microsoft SQL Server
DBType=MSSQL
DBUser=servicedesk
DBPassword=dbpassword
DBHost=dbserver1
LogLocation=C:\\Program-Files\\CA\\Service Desk Manager\\log
LogLevel=ERROR
SchemaName=dbo
```

Beispiel: Oracle-Konfigurationseinstellungen

```
#Sample-Konfigurationsdatei für Oracle
DBType=Oracle
DBUser=mdbadmin
DBPassword=dbpassword
DBHost=dbserver1
LogLocation=/tmp/ambiguity/log
LogLevel=INFO
DBPort=1521
DBSID=orcl
SchemaName=mdbadmin
```

Parameter für "cmdb_update_ambiguity"

Sie können Parameter über die Befehlszeile oder in einer Konfigurationsdatei festlegen (einige Parameter sind nur in der Befehlszeile verfügbar. Verwenden Sie in der Befehlszeile Anführungszeichen (""), um Pfadnamen mit Leerstellen darin einzuschließen. Verwenden Sie jedoch keine Anführungszeichen in der Konfigurationsdatei. Wenn ein Parameter sowohl in der Befehlszeile als auch in der Konfigurationsdatei festgelegt ist, so überschreibt der Wert in der Befehlszeile den Wert in der Konfigurationsdatei.

Für den Befehl "cmdb_update_ambiguity" benötigen Sie folgende Parameter:

Option	Konfigurationsdatei	Werte	Hinweise
	i-Schlüsselwort:		
-m	(keine)	tw, ci, all	(Erforderlich) Nur Befehlszeile tw = Mehrdeutigkeit nur für TWA berechnen. ci = Mehrdeutigkeit nur für CIs berechnen. all = Mehrdeutigkeit für CIs und TWA berechnen.

-d	DBType	MSSQL oder Oracle	(Erforderlich. Nur Windows.) Datenbanktyp. Unter Linux/UNIX wird nur Oracle unterstützt und diese Option wird nicht benötigt.
-u	DBuser	<db user name>	(Erforderlich) Datenbankbenutzername. Ein Benutzername mit Leerstellen muss in doppelte Anführungszeichen eingeschlossen werden (zum Beispiel: -u "sys as sysdba"). In der Konfigurationsdatei sind die Anführungszeichen nicht erforderlich.
-p	DBPassword	<db password>	(Erforderlich) Kennwort für Datenbankbenutzer Ein Kennwort mit Leerstellen muss in doppelte Anführungszeichen eingeschlossen werden (zum Beispiel: -p "secret code"). In der Konfigurationsdatei sind die Anführungszeichen nicht erforderlich.
-c	(keine)	<Konfigurationsdatei>	(Optional) Nur Befehlszeile Vollständiger Pfadname der Konfigurationsdatei. Muss in Anführungszeichen eingeschlossen werden, wenn der Pfadname eine Leerstelle enthält.
-log	LogLocation	<Verzeichnis für die Protokolldatei>	(Optional) Protokolldatei-Verzeichnis Das Standardverzeichnis lautet "NX_ROOT/log".
-level	LogLevel	INFO, FEHLER, DEBUG	(Optional) Grad der Detailtiefe, mit dem in die Protokolldatei geschrieben wird. Der Standardwert ist ERROR.
-s	DBHost	<Servername>	(Erforderlich) Hostname des Datenbankservers Um eine Instanz mit einem Microsoft SQL Server-Namen zu verwenden, geben Sie in der Befehlszeile <i>server\instance</i> oder in der Konfigurationsdatei <i>server\\instance</i> an.
-CI	CI	<CI-uuid>	(Optional) Berechnen Sie Mehrdeutigkeit für das angegebene CI und alle CIs, die mit diesem mehrdeutig sind.

-full	(keine)	0,1	(Optional) Nur Befehlszeile Optimiert die Leistung des Scans, indem nur die CIs berücksichtigt werden, die seit der letzten Ausführung des Dienstprogramms aktualisiert wurden. Ist diese Option auf "1" gesetzt, wird ein vollständiger Scan aller CIs in der Berechnung des Mehrdeutigkeitsindex erzwungen. Der Standard ist "0". Dieser Parameter bezieht sich nicht auf die Berechnung von Transaktionsmehrdeutigkeit. Das Dienstprogramm wertet immer alle Transaktionen im TWA aus.
-port	DBPort	<Port-Nummer>	(Erforderlich. nur Oracle) Oracle-Portnummer
-SID	DBSID	<SID-Name>	(Erforderlich. nur Oracle) Oracle-SID-Name
-h	(keine)		(Optional) Druckt eine Hilfeverwendungsmeldung.
-schema	SchemaName	<db-Schema-Name>	(Optional) Standard ist "mdbadmin" für Oracle bzw. "dbo" für Microsoft SQL Server.

Weitere Informationen:

[Befehl "cmdb_update_ambiguity"](#) (siehe Seite 667)

Anzeigen mehrdeutiger Transaktionen über die Registerkarte "Administration"

Nach dem Ausführen des Dienstprogramms "cmdb_update_ambiguity" können Sie über die Registerkarte "Administration" mehrdeutige CIs anzeigen und verwalten.

Zum Anzeigen mehrdeutiger CIs wählen Sie auf der Registerkarte "Administration" die Optionen "CA CMDB" > "Abstimmungs-Management" > "Mehrdeutige CIs".

Die Seite "Mehrdeutige CI – Liste" zeigt die Liste der mehrdeutigen CIs an, deren Index größer als 0 (null) ist.

Hinweis Wenn Sie auf der Seite "Mehrdeutige CI-Liste" oder auf der Listenseite für mehrdeutige CI-Transaktionen auf "Filterinhalt löschen" klicken, wird das Feld "Weitere Suchargumente" nicht gelöscht (Mehrdeutigkeit > 0).

Weitere Informationen:

[Anzeigen mehrdeutiger Transaktionen über die Registerkarte "Administration"](#) (siehe Seite 671)

Anzeigen mehrdeutiger CIs über das Scoreboard

Nach dem Ausführen des Dienstprogramms "cldb_update_ambiguity" können Sie über das Scoreboard mehrdeutige CIs anzeigen und verwalten.

So zeigen Sie mehrdeutige CIs über das Scoreboard an

1. Erweitern Sie im CA SDM-Scoreboard den Ordner "C MDB"
2. Wählen Sie "Abstimmungs-Management" > "Mehrdeutige CIs", und klicken Sie auf eine der folgenden Optionen:
 - Alle
 - Während des letzten Tages aktualisiert
 - Während der letzten Woche aktualisiert
 - Während des letzten Monats aktualisiert

Die Liste mehrdeutiger CIs mit einem Index größer als 0 (Null) wird angezeigt.

Hinweis Wenn Sie auf der Seite "Mehrdeutige CI-Liste" oder auf der Listenseite für mehrdeutige CI-Transaktionen auf "Filterinhalt löschen" klicken, wird das Feld "Weitere Suchargumente" nicht gelöscht (Mehrdeutigkeit > 0).

Weitere Informationen:

[Identifizieren und Auflösen von mehrdeutigen CIs](#) (siehe Seite 664)

Lösen von mehrdeutigen CIs

Nachdem Sie mehrdeutige CIs identifiziert haben und festgestellt haben, ob ihre identifizierenden Attribute gültig sind, führen Sie einen der folgenden Schritte aus, um die Mehrdeutigkeit der CIs in der Mehrdeutigkeitsgruppe zu lösen:

Ändern der identifizierenden Attribute

Wenn Sie feststellen, dass die identifizierenden Attribute unvollständig oder ungültig sind, können Sie die identifizierenden Attribute des CIs über die Web-Schnittstelle, GRLoader oder CMDBf so festlegen, dass das CI eindeutig ist.

Hinweis: Wenn MDR das CI aktualisiert, kann MDR die manuell ausgeführten Abstimmungsänderungen rückgängig machen.

Ausschließen eines CI von der Mehrdeutigkeitsverwaltung

Wenn Sie feststellen, dass die identifizierenden Attribute des CI korrekt sind und eine bekannte, gültige Mehrdeutigkeit darstellen, können Sie das CI von den Mehrdeutigkeitsverwaltungslisten und der Mehrdeutigkeitsberechnung anderer CIs ausschließen und das CI als nicht mehrdeutig (Mehrdeutigkeit ausschließen) kennzeichnen.

Ablehnen einer CI-Aktualisierung durch Deaktivierung des CI

Wenn Sie feststellen, dass die identifizierenden Attribute eines CI falsch sind und Aktualisierungen mit diesen Attributen zu Datenbeschädigungen führen, können Sie das CI deaktivieren und dadurch weitere Aktualisierungen verhindern. Der Anwender bzw. das MDR, von dem die Informationen generiert wurden, erhält einen Fehler, und die gesamte Transaktion wird abgelehnt.

Ersetzen von CIs

In manchen Fällen liegen die Aktualisierungen von CMDB außerhalb der Kontrolle des Administrators, und im System müssen ungültige identifizierende Daten zusammen mit gültigen, nicht identifizierenden Attributdaten vorhanden sein. Die eingehenden Transaktionsattributdaten können transparent an ein ersetzendes CI umgeleitet werden.

Hinweis: Die transparente Umleitung von Attributdaten von einem CI an ein anderes kann zu Verwirrungen führen, das Transaktionsdaten möglicherweise nicht in demselben CI gespeichert werden wie die identifizierenden Attribute der Transaktion Sie glauben machen. Verwenden Sie nach eigenem Ermessen diese Methode, wenn keine der vorherigen Methoden verwendet werden kann.

Ausschließen von CIs aus der Mehrdeutigkeitsverwaltung

Manchmal zeigt es sich, dass ein bestimmtes CI unberücksichtigt bleiben sollte, obwohl es einen Mehrdeutigkeitsindex größer als 0 erhält. Jedes CI, dessen Kontrollkästchen "Mehrdeutigkeit ausschließen" aktiviert ist, wird nicht als Teil des Mehrdeutigkeitsindex oder der Mehrdeutigkeitsverwaltungsfunktionen betrachtet.

Ausschließen von Mehrdeutigkeit für ein CI

Sie können die Mehrdeutigkeitsoption für ein CI über die Web-Schnittstelle aktualisieren.

So schließen Sie Mehrdeutigkeit für ein CI aus:

1. Wählen Sie das CI aus, das Sie von der Mehrdeutigkeitsverwaltung über die Seite "Mehrdeutige CI – Liste" ausschließen möchten.

Die Seite "Configuration Item – Detail" wird angezeigt.

2. Klicken Sie auf "Bearbeiten".

Die Seite "Configuration Item aktualisieren" wird angezeigt.

3. Aktivieren Sie auf der Registerkarte "Abstimmung" das Kontrollkästchen "Mehrdeutigkeit ausschließen", und klicken Sie auf "Speichern".

Das CI wird von der Mehrdeutigkeitsindexberechnung und anderen Mehrdeutigkeitsverwaltungsfunktionen ausgeschlossen.

So schließen Sie unter Verwendung von GRLoader Mehrdeutigkeit aus:

Sie können die Option zum Ausschließen von Mehrdeutigkeit für ein CI aktualisieren, indem Sie unter Verwendung von GRLoader die Markierung "not_ambiguous" für das CI setzen.

Die möglichen Werte für "not_ambiguous" sind:

YES (1)

Entfernt das CI aus der Mehrdeutigkeitsverwaltung. Das CI wird ungeachtet der identifizierenden Attribute anderer CIs als eindeutig identifiziert. Der Mehrdeutigkeitsindex der CI bleibt bei Null.

NO 0 (Standard)

Dieses CI ist für die Mehrdeutigkeitsverwaltung aktiviert. Die Eindeutigkeit der identifizierenden Attribute eines CI bestimmt dessen Mehrdeutigkeitsindex. Die identifizierenden Attribute für das CI werden zur Berechnung des Mehrdeutigkeitsindex anderer CIs herangezogen.

Hinweis: Weitere Informationen zu GRLoader finden Sie im *Technischen CA CMDB-Referenzhandbuch*.

So weisen Sie Aktualisierungen zurück:

Wenn ein CI als inaktiv gekennzeichnet ist, kann es nicht mehr aktualisiert werden. Setzen Sie das CI auf "Inaktiv", wenn CA CMDB Daten für ein bestimmtes CI ablehnen soll (nach Name, Seriennummer, MAC-Adresse usw.) und MDR über die Ablehnung informiert werden soll.

Auf diese Weise können Sie problematische Daten direkt zurückweisen und an ihren Ursprung zurücksenden, so dass das MDR die zurückgewiesene Eingabe korrigieren kann.

Sie können ein CI über die Web-Schnittstelle als inaktiv festlegen, indem Sie das CI bearbeiten, die Option "Inaktiv" aktivieren und auf "Speichern" klicken. Sie können ein CI unter Verwendung von GRLoader- oder CMDBf-Webservices als inaktiv festlegen. Inaktive CIs können auch wieder aktiviert werden.

Ersetzen mehrdeutiger CIs

Sie können ein mehrdeutiges CI ersetzen, um Daten an ein bestimmtes Ziel-CI umzuleiten. Sie können ersetzte CIs anzeigen, die inaktiv sind und deren Aktualisierungen über die Web-Schnittstelle ignoriert werden.

Hinweis: Aktualisierungen, die von GRLoader- oder CMDBf-Web-Services an ersetzte CIs gesendet werden, werden an das ersetzende CI umgeleitet. Aktualisierungen identifizierender Attribute werden jedoch ignoriert.

So ersetzen Sie ein mehrdeutiges CI:

1. Wählen Sie auf der Seite "Mehrdeutige CI – Liste" das CI aus, das Sie als Fokus-CI (ersetzendes CI) festlegen möchten.

Die Seite "Configuration Item – Detail" wird angezeigt.

2. Klicken Sie auf "Bearbeiten".

Die Seite "Configuration Item aktualisieren" wird angezeigt.

3. Klicken Sie auf die Registerkarte "Abstimmung".

Alle CIs, die vom Fokus-CI nicht eindeutig abgegrenzt sind, werden angezeigt.

Bestimmen Sie, welche CIs durch das Fokus-CI ersetzt werden sollen. Überprüfen Sie jedes CI in der Liste, indem Sie darauf klicken, um die zugehörige Seite "Configuration Item-Details" anzuzeigen.

4. Wählen Sie mindestens ein mehrdeutiges CI aus, das durch das Fokus-CI ersetzt werden soll, und klicken Sie auf "Ersetzen".

Die ausgewählten CIs werden durch das Fokus-CI ersetzt.

Anzeigen ersetzter CIs über die Registerkarte "Administration"

Ersetzte CIs können über die Registerkarte "Administration" angezeigt werden.

Zum Anzeigen ersetzter CIs wählen Sie auf der Registerkarte "Administration" die Optionen "CA CMDB" > "Abstimmungs-Management", "Ersetzte CIs gefunden".

Die Liste "Ersetzte CIs gefunden" wird angezeigt.

Anzeigen ersetzter CIs über das Scoreboard

Ersetzte CIs können im Scoreboard angezeigt werden.

So zeigen Sie ersetzte CIs im Scoreboard an:

1. Erweitern Sie im CA SDM-Scoreboard den Ordner "CMDB"
2. Erweitern des Ordners "Abstimmungs-Management".
3. Klicken Sie auf den Knoten "Ersetzte CIs gefunden".

Die Liste "Ersetzte CIs gefunden" wird angezeigt.

Überprüfen und Ändern von eingehenden Daten mit dem Transaktionsarbeitsbereich (TWA)

Sie können CI- und Beziehungstransaktionen vor der Ausführung bereitstellen, indem Sie Daten in den TWA-Staging-Bereich kopieren. Im Staging-Bereich können Sie CIs und Beziehungen über die Web-Schnittstelle oder anhand von systemeigener SQL bearbeiten.

Sie können die CI-Transaktionen auch validieren, um die Erstellung neuer CIs zu vermeiden, wenn vorhandene CIs aktualisiert werden. Bei dieser Vorgehensweise können Sie die einzelnen Transaktionen und die möglichen aktualisierbaren CIs anzeigen, so dass Sie die Transaktion manuell auf das Ziel-CI abstimmen können. Ebenso können Beziehungstransaktionen validiert werden, um auf die richtigen CIs zu verweisen.

Der *Mehrdeutigkeitsindex* ist eine funktionale Messung der möglichen Nicht-Einmaligkeit eines Configuration Items (CI), die auf seinen identifizierenden Attributen basiert. Der Mehrdeutigkeitsindex kann die Wahrscheinlichkeit von "gedoppelten" CIs im CMDB messen, oder die Wahrscheinlichkeit, dass eine Transaktion mehrere CI-Ziele hat.

Überprüfen Sie und ändern Sie mehrdeutige CI-Transaktionen anhand des folgenden Prozesses:

1. Identifizieren Sie mehrdeutige CI-Transaktionen.
 - Berechnen Sie den Mehrdeutigkeitsindex für alle CI-Transaktionen.
 - Überprüfen Sie die Liste der mehrdeutigen CI-Transaktionen auf dem Scoreboard.
2. Entscheiden Sie, ob die identifizierenden Attribute für jede CI-Transaktion mit dem beabsichtigten CI abgestimmt sind.
3. Lösen Sie die mehrdeutigen CI-Transaktionen mit einer der folgenden Aktionen:
 - Ändern der identifizierenden Attribute
 - Geben Sie das Ziel-CI an.

Weitere Informationen:

[Beispiel für CI-Transaktionsmehrdeutigkeit](#) (siehe Seite 678)

[Identifizieren von mehrdeutigen CI-Transaktionen](#) (siehe Seite 679)

[Lösen von mehrdeutigen CI-Transaktionen](#) (siehe Seite 681)

[Transaktionsarbeitsbereich](#) (siehe Seite 683)

[Auffüllen des Transaktionsarbeitsbereichs](#) (siehe Seite 684)

[Aktualisieren von Daten im TWA über die Web-Schnittstelle](#) (siehe Seite 696)

[Verwalten bereitgestellter Transaktionen](#) (siehe Seite 682)

[Laden von Transaktionen in die CMDB](#) (siehe Seite 701)

[Manuelle Abstimmung](#) (siehe Seite 699)

[TWA-Administration](#) (siehe Seite 703)

Beispiel für CI-Transaktionsmehrdeutigkeit

Transaktionsdaten werden aus unterschiedlichen Datenquellen in CA CMDB geladen. Jede Datenquelle verwendet ihre eigene Teilmenge von identifizierenden Merkmalen und kann möglicherweise die Ziel-CIs für die Transaktionen nicht vollständig identifizieren. Wegen dieser Inkonsistenz können mehr CI-Transaktionen in CA CMDB vorhanden sein, als gültig sind.

Es folgt ein Beispiel für CI-Transaktionsmehrdeutigkeit:

Beispiel: Verwalten von mehrdeutigen CI-Transaktionen

Die folgende CI-Transaktion residiert im TWA:

- Name(Server1) DNS Name(dns1), Serial Number(serial1)

Die folgenden CIs residieren in der CA CMDB:

- Name(Server2) DNS Name(dns1)
- Name(Server3) DNS Name(dns1), Serial Number(serial1)
- Name(Server4) MAC Address(mac1), Serial Number(serial1)

Aufgrund der gemeinsamen Merkmale sind Server1-Transaktionen mit Server2, Server3 und Server4 in CA CMDB mehrdeutig.

Allen CI-Transaktionen ist ein Mehrdeutigkeitsindex zugeordnet. Der Mehrdeutigkeitsindex entspricht ungefähr der Anzahl vorhandener CIs, die einem der identifizierenden Attribute entsprechend, abzüglich einem, angegeben in der CI-Transaktion. Je größer der Index, desto größer ist die Anzahl anderer CIs, bei denen die Transaktionskennungen übereinstimmen, und daher desto größer die Möglichkeit, dass CI-Daten inkonsistent eingegeben wurden und die Möglichkeit, dass zusätzliche CIs inkorrekt erstellt wurden. CI-Transaktionen mit einem Mehrdeutigkeitsindex von Null haben identifizierende Attribute, die über alle CIs hinweg einmalig sind oder für die ein Ziel-CI angegeben wurde, und sind deswegen eindeutig.

Beispiel: Berechnung des Mehrdeutigkeitsindex

Folgende vier CI-Transaktionen sind im TWA abgelegt:

- Name(Server1) DNS Name(dns1), Serial Number(serial1)
- Name(Server2) DNS Name(dns1), Serial Number(serial1)

Die folgenden CIs residieren in der CA CMDB:

- Name(Server1) DNS Name(dns1), Serial Number(serial1)
- Name(Server2) DNS Name(dns1), Serial Number(serial1), Mac Address(mac1)

Die Mehrdeutigkeit der ersten Transaktion (Server1) ist 0, weil eine genaue Übereinstimmung mit den identifizierenden Attributen der CIs von Server1 vorliegt. Das einzige mögliche Ziel-CI für diese Transaktion ist Server1-CI.

Die zweite Transaktion (Server2) ist mehrdeutig für Server1-CI und Server2-CI.

Der Mehrdeutigkeitsindex für die Server2-Transaktion besteht aus den folgenden Komponenten:

- Anzahl von übereinstimmenden CIs mit "Name (Server2)" = 1
- Anzahl von übereinstimmenden CIs mit "DNS Name(dns1)" = 2
- Anzahl von übereinstimmenden CIs mit "Serial Number (serial1)" = 2

Basierend auf den gemeinsamen identifizierenden Merkmalen für CIs ist der Mehrdeutigkeitsindex für Server2-Transaktionen $(1-1) + (2-1) + (2-1) = 2$

Identifizieren von mehrdeutigen CI-Transaktionen

Sie können vor dem Laden von Transaktionsdaten Transaktionen mit mehrdeutigen CI-Zielen überprüfen und ändern. Sie können auch CI-Transaktionen auflösen, die kein Ziel-CI, aber identifizierende Attribute für ein oder mehrere CIs aufweisen. Dieser Lösungsschritt gewährleistet, dass das richtige CI aktualisiert wird, und verhindert die Erstellung von falschen oder inkonsistenten Daten.

Auf der Detailseite der CI-Transaktion werden auf der Registerkarte "Abstimmung" alle CIs aufgelistet, die mit dieser Fokus-CI-Transaktion mehrdeutig sind. Überprüfen Sie die CI-Attribute, wie das Datum der letzten Aktualisierung, verwandte Probleme, Issues und andere Aspekte des CI, um das der Transaktion entsprechende Ziel-CI zu identifizieren.

Hinweis: Um Mehrdeutigkeit für CIs oder CI-Transaktionen anzuzeigen, müssen Sie den Mehrdeutigkeitsindex mit Hilfe des Dienstprogramms "[cmdb update ambiguity](#)" (siehe Seite 667) berechnen.

Weitere Informationen finden Sie unter [Überprüfen und Ändern von eingehenden Daten mithilfe des Transaktionsarbeitsbereichs \(TWA\)](#) (siehe Seite 676).

Anzeigen mehrdeutiger Transaktionen über die Registerkarte "Administration"

Mehrdeutige Transaktionen können über die Registerkarte "Administration" angezeigt und verwaltet werden.

Zum Anzeigen mehrdeutiger Transaktionen wählen Sie auf der Registerkarte "Administration" die Optionen "CA CMDB" > "Abstimmungs-Management" > "Mehrdeutige CI-Transaktionen gefunden".

Die Liste von CI-Transaktionen mit einem Index größer als 0 (Null) wird angezeigt.

Hinweis Wenn Sie auf der Seite "Mehrdeutige CI-Liste" oder auf der Listenseite für mehrdeutige CI-Transaktionen auf "Filterinhalt löschen" klicken, wird das Feld "Weitere Suchargumente" nicht gelöscht (Mehrdeutigkeit > 0).

Anzeigen mehrdeutiger Transaktionen über das Scoreboard

Sie können mehrdeutige Transaktionen über das Scoreboard anzeigen und verwalten.

So zeigen Sie mehrdeutige Transaktionen im Scoreboard an:

1. Erweitern Sie im CA SDM-Scoreboard den Ordner "CMDB"
2. Wählen Sie "Abstimmungs-Management" > "Mehrdeutige CI-Transaktionen gefunden", und klicken Sie auf eine der folgenden Optionen:
 - Alle
 - Während des letzten Tages aktualisiert
 - Während der letzten Woche aktualisiert
 - Während des letzten Monats aktualisiert

Die Liste von CI-Transaktionen mit einem Mehrdeutigkeitsindex größer als 0 (Null) wird angezeigt.

Hinweis Wenn Sie auf der Seite "Mehrdeutige CI-Liste" oder auf der Listenseite für mehrdeutige CI-Transaktionen auf "Filterinhalt löschen" klicken, wird das Feld "Weitere Suchargumente" nicht gelöscht (Mehrdeutigkeit > 0).

Lösen von mehrdeutigen CI-Transaktionen

Nachdem Sie mehrdeutige CI-Transaktionen identifiziert haben und ermittelt haben, ob deren identifizierenden Attribute bzw. das Ziel-CI gültig sind, führen Sie einen der folgenden Schritte aus, um die Mehrdeutigkeit in der CI-Transaktion zu lösen:

Ändern der identifizierenden Attribute

Wenn Sie feststellen, dass die identifizierenden Attribute unvollständig oder ungültig sind, können Sie die identifizierenden Attribute der CIs über die Web-Schnittstelle so festlegen, dass das CI eindeutig ist.

Angeben des Ziel-CIs

Wenn Sie feststellen, dass das Ziel-CI nicht festgelegt oder ungültig ist, können Sie ein CI für eine mehrdeutige Transaktion angeben, sodass die entsprechenden Daten unabhängig von den Werten der in der Transaktion angegebenen identifizierenden Attribute an ein bestimmtes Ziel-CI geleitet werden.

Angeben von Ziel-CIs für mehrdeutige CI-Transaktionen

Sie können ein CI für eine mehrdeutige Transaktion angeben, sodass die entsprechenden Daten unabhängig von den Werten der in der Transaktion angegebenen identifizierenden Attribute an ein bestimmtes Ziel-CI geleitet werden.

So geben Sie das Ziel CI für eine mehrdeutige CI Transaktion an

1. Wählen Sie auf der Seite "Mehrdeutige Transaktionen – Liste" eine CI Transaktion aus.
Die Seite "Configuration Item – Transaktionsdetail" wird angezeigt.
2. Klicken Sie auf "Bearbeiten".
Die Seite "Configuration Item – Transaktion aktualisieren" wird angezeigt.
3. Wählen Sie auf der Registerkarte "Abstimmung" ein CI aus der Liste, um es als Ziel-CI für die Transaktion festzulegen. Klicken Sie auf "Ziel-CI" festlegen und dann auf "Speichern".
Das ausgewählte CI wird zum Ziel-CI der Transaktion.

Verwalten bereitgestellter Transaktionen

CA CMDB bietet eine Funktion, mit der Sie Daten speichern können, bevor Sie sie in CA CMDB laden. Diese "bereitgestellten" Daten werden als Transaktionen im Transaktionsarbeitsbereich (TWA) gespeichert. Eine bereitgestellte Transaktion ist eine Arbeitseinheit, die ein CI oder eine Beziehung erstellt oder aktualisiert. Der TWA kann viele Transaktionen für ein bestimmtes CI bzw. eine bestimmte Beziehung enthalten.

Sie können in CMDB geladene Daten erfassen, bevor diese gebunden werden, sodass Sie folgende Änderungen ausführen können:

- Nicht dem Standard entsprechende Daten können bereinigt und standardisiert werden.
- Unvollständige Daten können ergänzt werden. So kann zum Beispiel die Lokation von CIs, deren Namen mit "NY" beginnt, auf "New York" gesetzt werden.
- Daten, die nicht den vorhandenen Suchtabellen (SRELs) entsprechen, können geändert werden.
- Transaktionen können für eine spätere Implementierung geplant werden.
- Stimmen Sie Transaktionen auf vorhandene CIs in CA CMDB ab, Bevor Sie die Daten laden.
- Validieren Sie die CI- und Beziehungstransaktionen validieren, um die Erstellung ungültiger Daten oder neuer CIs zu verhindern, wenn ein einzelnes CI oder vorhandene CIs aktualisiert werden sollen. Zeigen Sie die einzelnen Transaktionen und die potenziellen CIs, die von ihr aktualisiert werden können, an, damit Sie die Transaktion manuell auf das Ziel-CI abstimmen können.

Mithilfe des TWA können Sie den Abstimmungsvorgang proaktiv verwalten. Sie können GRLoader zum Laden der Daten in den TWA konfigurieren, wobei CA CMDB Sie die Transaktionsdaten ändern lässt, um Transaktionen zu verarbeiten, die das falsche CI erstellen, möglicherweise aktualisieren oder referenzieren können.

Weitere Informationen finden Sie unter [Überprüfen und Ändern von eingehenden Daten mithilfe des Transaktionsarbeitsbereichs \(TWA\)](#) (siehe Seite 676).

Transaktionsarbeitsbereich

Mit dem Transaktionsarbeitsbereich (TWA) in CA SDM können Sie CI- und Beziehungsdaten untersuchen und ändern, bevor Sie sie in CMDB laden.

Der TWA-Prozess funktioniert folgendermaßen:

1. [Laden Sie die Daten](#) (siehe Seite 684) in den TWA. Der Inhalt kann aus CI-Transaktionen oder CI-Beziehungstransaktionen bestehen. Beim Eingabevorgang erfolgt keine Abstimmung von Datensätzen; er dient lediglich dazu, den Arbeitsbereich in einer der folgenden Weisen mit CI- und Beziehungstransaktionsdaten zu füllen:
 - GRLoader: Liest XML-Daten und speichert diese mit den Optionen "-littwa" oder "-littwar" im TWA.
 - Native SQL: Daten gelangen über die Standard-SQL-Verarbeitung in den TWA.
 - Erstellen Sie mithilfe der Web-Schnittstelle eine CI-Transaktion oder eine Beziehungstransaktion.
2. (Optional) Stimmen Sie Transaktionen manuell auf vorhandene CIs in <CMDB ab, bevor Sie die Daten laden. Sie können das [Laden der Daten auch simulieren](#) (siehe Seite 690), um im Voraus festzustellen, ob eine Reihe von Transaktionen neue CIs (und somit neue Mehrdeutigkeiten für andere CIs) oder Beziehungen erstellen kann.

Weitere Informationen finden Sie unter [Überprüfen und Ändern von eingehenden Daten mithilfe des Transaktionsarbeitsbereichs \(TWA\)](#) (siehe Seite 676).

3. Ändern Sie die Daten. Sie können den TWA über die folgenden Quellen ändern:

CA SDM-Benutzeroberfläche

Über die webbasierte Benutzeroberfläche können Sie Transaktionen im Arbeitsbereich ansehen und ändern.

Native SQL

Wenn Sie viele Änderungen auf mehrere Transaktionen anwenden, kann Native SQL die Daten im TWA ändern.

Hinweis: Änderungen, die mit Native SQL vorgenommen werden, können alle Sicherheitsmaßnahmen von CA SDM umgehen.

4. GRLoader lädt die Daten mithilfe der Optionen "-lftwa" oder "-lftwai" aus dem TWA in CA CMDB. Jede TWA-Zeile wird als separate Transaktion angesehen.
 1. Wenn bei der Ausführung von GRLoader ein Fehler auftritt, wird der Fehlercode in der Transaktion aufgefüllt, um anzuzeigen, dass der Vorgang nicht vollständig ausgeführt wurde (so werden spätere Wiederholungen erleichtert).
 2. Die restlichen Datensätze werden als vollständige Transaktionen gekennzeichnet.
5. Überprüfen Sie die Transaktionsergebnisse, und korrigieren Sie etwaige Fehler mithilfe der Web-Schnittstelle. Wiederholen Sie ggf. die Schritte 3 und 4.

Beachten Sie Folgendes:

- Wenn Sie benutzerdefinierte Familien oder Attribute erstellt haben und nun möchten, dass die entsprechenden Spalten im Arbeitsbereich erscheinen, ändern Sie den Arbeitsbereich, um die benutzerdefinierten Spalten einzuschließen. Weitere Informationen finden Sie im Abschnitt [Erweitern von TWA-Objekten](#) (siehe Seite 704).
- Verwenden Sie die aktuelle Version von GRLoader, um die Vorteile von TWA zu nutzen. Wenn Sie ein Produkt verwenden, das eine frühere Version von GRLoader umfasst, aktualisieren Sie GRLoader auf die aktuelle Version.
- Änderungen an Transaktionen im TWA werden geprüft.

Auffüllen des Transaktionsarbeitsbereichs

Eingabedaten können aus zahlreichen Quellen stammen, z. B.:

- CA-Produkte wie CA Cohesion ACM, CA Wily CEM, CA Wily Introscope und CA Spectrum, die Daten mittels GRLoader importieren
- Jedes andere MDR, das Daten mittels GRLoader importiert
- Eine andere CMDB
- Microsoft Excel-Kalkulationstabellen
- Datenbanktabellen
- Ein von einem Anbieter ausgewähltes ETL-Tool

Weitere Informationen finden Sie unter [Datenbankeinschränkungen](#) (siehe Seite 707).

Laden von Daten in den TWA mit GRLoader

Die folgenden GRLoader-Optionen unterstützen die Verwendung des TWA:

-littwa

Lädt XML-Daten in TWA im Ausgangszustand.

-littwar

Lädt XML-Daten in TWA im fertigem Zustand.

-lftwa

Lädt Transaktionen aus dem TWA in CMDB.

-lftwai

Lädt Transaktionen aus dem TWA in CMDB und deaktiviert erfolgreiche Transaktionen.

Über GRLoader eingegebene XML-Dokumente können ohne Änderung in CMDB oder den TWA geladen werden.

Mit Hilfe von GRLoader mit der Option "-littwa" (in TWA laden) können Daten in den Transaktionsarbeitsbereich geladen werden. Die GRLoader-Konfigurationsdatei enthält:

```
grloader.loadtotwa=yes
```

Im TWA-Modus werden CIs und Beziehungen nicht direkt erstellt, sondern mittels GRLoader werden die Informationen in die Tabellen des Transaktionsarbeitsbereichs eingefügt. Daten, die in den TWA geladen wurden, können bearbeitet, geändert und überprüft werden. Nach diesen Änderungen der Daten können individuelle Transaktionen unter Verwendung von -lftwa oder -lftwai in CMDB geladen werden.

Wenn CI-Daten in CMDB geladen werden, wird automatisch eine Abstimmung der CIs durchgeführt. Ist dieser Vorgang erfolgreich, dann wird ein einzelnes CI in CMDB mit Daten eines einzelnen Business-Objekts aktualisiert. Wenn *CI-Transaktionen* in den TWA geladen werden, findet keine automatische Abstimmung statt. Im TWA können mehrere Transaktionen mit identifizierenden Attributen für ein einzelnes CI angezeigt werden. Bereits vorhandene Zeilen im TWA werden nicht aktualisiert, wenn neue Zeilen im Modus "In TWA laden" hinzugefügt werden. Dies gilt auch, wenn die Zeile genau mit einem bereits vorhandenen CI übereinstimmt. Auch identische CI-Definitionen können mehrmals im TWA angezeigt werden.

GRLoader validiert Datenwerte, wenn es im Modus "Aus TWA laden" ("-lftwa" oder "-lftwai") ausgeführt wird, um Objekte in CMDB zu erstellen, oder wenn es beim Ausführen den Simulationsmodus ("-simci" oder "-simrel") verwendet. Weitere Einzelheiten finden Sie unter [Simulieren von TWA-Operationen](#) (siehe Seite 690). Wird GRLoader im Modus "In TWA laden" ("-lftwa" oder "-lftwar") ausgeführt, werden die Datenwerte nicht validiert.

Der Parameter "-lftwai" (oder die Konfigurationsoption "grloader.loadtotwa.inactivate") deaktiviert erfolgreich geladene TWA-Transaktionen. Nachdem eine erfolgreich geladene Transaktion als inaktiv markiert worden ist, kann sie mit Hilfe von "Archivierung/Löschung" dauerhaft aus dem TWA entfernt werden.

Beispiel: In CMDB laden

Der folgende Befehl lädt Daten direkt in die CMDB:

```
grloader ... -i mydata.xml -a -n
```

Die XML-Datei "mydata.xml" enthält Folgendes:

```
<GRLoader>
  <ci>
    <name>Server1</name>
    <class>Server</name>
  </ci>
</GRLoader>
```

Beispiel: In TWA laden

Der folgende Befehl lädt Daten in den TWA, damit sie vor dem Laden in die CMDB bearbeitet werden können:

```
grloader ... -i mydata.xml -lftwa
```

Weitere Informationen:

[XML-Eingabe](#) (siehe Seite 687)

[Suche](#) (siehe Seite 687)

[Datumsformat](#) (siehe Seite 688)

[EMPTY](#) (siehe Seite 689)

XML-Eingabe

GRLoader verwendet eine XML-Eingabedatei. Wenn in den TWA geladen wird, werden die folgenden XML-Spalten zugewiesen. Somit werden Konflikte vermieden, wenn sich die Spaltennamen mit den Standardspaltennamen in der Datenbank überschneiden.

VON XML-Name	ZU Datenbankspalte
tenant	tgt_tenant
ID	tgt_id
delete_flag	tgt_delete_flag

Für Beziehungen gelten die folgenden Zuordnungen:

VON XML-Name	ZU Datenbankspalte
name	provider_name oder dependent_name
dns_name	provider_dns_name oder dependent_dns_name
delete_flag	tgt_delete_flag

Zuordnungen werden umgekehrt, wenn aus den TWA-Datenbanktabellen geladen wird.

Suche

Wenn Sie Daten für die Suche (SREL) von Attributen im TWA angeben, so müssen diese mit dem Format des systemeigenen XML in GRLoader übereinstimmen.

Anfrageattribute nehmen nur bestimmte Werte an, die in den zugehörigen Tabellen definiert sein müssen. Diese Attribute können auch über zusätzliche Einschränkungen und Ausnahmen verfügen, die erfüllt sein müssen, damit die Zuordnung ausgeführt werden kann. Die angegebenen Werte sind gleich, egal ob sie über XML, SQL oder die TWA-Web-Schnittstelle festgelegt wurden.

Um zu entscheiden, ob ein Attribut ein SREL ist, lesen Sie die folgenden Abschnitte im Handbuch *CA CMDB-Technische Referenz*:

- Familien und Klassen (SREL-Attribute werden angegeben)
- Kontakt und andere Suchfelder
- Felder, die mit Daten in bestehenden Tabellen (SREL) überprüft werden.

Beispiel: XML-Suche

Im folgenden Beispiel wird die alternative SREL-Spalte eingestellt, indem die Suchparameter festgelegt werden:

```
<ci>
<name>Server1</name>
<owner lookup="userid">mckpe99</owner>
</ci>
```

Im TWA kommen Sie zum gleichen Ergebnis, wenn Sie die alternative SREL-Spalte an den Datenwert anhängen und mit Trennzeichen umgeben (siehe unten, "grloader.workarea.delimiters"). Die entsprechende Transaktion wird im Transaktionsarbeitsbereich wie folgt dargestellt:

ID	Name	Eigentümer
100	Server1	mckpe99 {userid}

Sie können auch das oben benutzte Trennzeichen in der Grloader-Konfigurationsdatei anwenden:

```
grloader.workarea.delimiters=xy
```

wobei x und y verschiedene Zeichen sind, die in der Regel nicht im Arbeitsbereich vorhanden sind.

Datumsformat

GRLoader unterstützt die folgenden Datumsformatoptionen in XML:

- datefmt=UTC
- datefmt=localtime (Standard)

Beispiele: datefmt-XML

```
<ci>
<name>Server1</name>
<purchase_date datefmt="UTC"> 1241197235</purchase_date>
</ci>
```

```
<ci>
<name>Server3</name>
<purchase_date> 2009/05/01</purchase_date>
</ci>
```

Die entsprechende Transaktion wird im Transaktionsarbeitsbereich wie folgt dargestellt:

ID	Name	purchase_date
101	Server1	1241197235
102	Server2	2009/05/01

Hinweis: Wenn ein Datum ein Sonderzeichen, wie z. B. einen Schrägstrich enthält (/), dann wird angenommen, dass es sich bei dem Format um "localtime" handelt. Hinweis: Wenn das Datum keine Sonderzeichen enthält, wird angenommen, dass es sich um UTC handelt.

EMPTY

GRLoader unterstützt die Option "update_if_null" im XML-Code zum Löschen eines Felds in CMDB. Im folgenden Beispiel wird gezeigt, wie das Feld "Eigentümer" für Server1 gelöscht wird. Ohne dieses Attribut ist das Feld "Eigentümer" nicht betroffen. Im TWA können Sie das Schlüsselwort EMPTY verwenden.

Beispiel: update_if_null XML

```
<ci>
<name>Server1</name>
<owner update_if_null="yes"></owner>
</ci>
```

Durch Angabe des Schlüsselworts "EMPTY" als Zeichenfolgenwert wird der Datenbankwert im TWA gelöscht. Die entsprechende Transaktion im Arbeitsbereich lautet:

ID	Name	Eigentümer
102	Server1	EMPTY

Der Schlüsselwortwert kann mithilfe der Konfigurationsoption "grloader.emptyvalue" festgelegt werden:

```
grloader.emptyvalue=xxxx
```

xxxx stellt eine beliebige Zeichenfolge dar, die nicht in den Arbeitsbereichsdaten vorhanden ist.

Simulieren von TWA-Operationen

Mithilfe der folgenden Optionen können Sie im Vorfeld feststellen, ob eine Reihe von Transaktionen neue CIs oder Beziehungen (und somit neue Mehrdeutigkeiten für andere CIs) erstellen können:

-simci

Simuliert nur die Verarbeitung von CI Transaktionen. Mit dieser Option kann festgestellt werden, ob Transaktionen CIs erstellen oder aktualisieren. Wenn die Option "-simci" verwendet wird, führt GRLoader eine Datenvalidierung aus.

-simrel

Simuliert nur die Verarbeitung von Beziehungstransaktionen. Mit dieser Option kann festgestellt werden, ob Beziehungstransaktionen erstellen oder Beziehungen aktualisieren. Die Option "-simrel" prüft Beziehungen auf die Existenz des Providers und abhängiger CIs, bestätigt Beziehungstypen und so weiter.

Die Ausgabe des Simulationsmodus wird an den TWA oder die Datei "_err.xml" weitergegeben. Im normalen Lademodus enthält die Datei "_err.xml" die CI-Eingabe und eine Bemerkung, die angibt, ob das CI eingefügt oder aktualisiert wurde. Bei Verwendung einer Simulation zeigt die GRLoader-Meldung in der Liste der CI-Transaktionen an, ob das CI oder die Beziehung eingefügt oder aktualisiert wurde. Andere relevante Fehlermeldungen werden ebenfalls angezeigt. Der Transaktionsstatus bleibt unverändert.

Eine Simulation kann auch in einer Konfigurationsdatei durch die Verwendung der Optionen **grloader.simulateloadci** und **grloader.simulateloadrelation** ermöglicht werden.

Hinweis: Wenn die GRLoader-Eingabe gleichzeitig CIs und Beziehungen erstellt, kann die Option "-simrel" nur vorhandene CIs verarbeiten, nicht CIs, die in der Zukunft erstellt werden sollen. Wegen dieser Beschränkung schließen sich die Optionen "-simci" und "-simrel" gegenseitig aus.

Aktualisieren von Daten im TWA mit SQL

Der TWA wird in MDB gespeichert und kann mit SQL-Abfragen direkt aktualisiert werden.

Weitere Informationen:

[TWA-Tabellen](#) (siehe Seite 691)
[TWA-SQL-Spaltennamen](#) (siehe Seite 692)
[Einfügen neuer Datensätze in den TWA](#) (siehe Seite 694)
[Verwenden von ODBC-Treibern](#) (siehe Seite 694)
[CI-Kennungen im TWA](#) (siehe Seite 695)
[Festlegen des Transaktionsstatus](#) (siehe Seite 695)
[Freigeben von Tabellen für CA SDM](#) (siehe Seite 696)

TWA-Tabellen

Tabellen des Transaktionsarbeitsbereichs beinhalten:

ci_twa_ci

Eine einzelne Tabelle, die alle Attribute über alle CI-Familien hinweg enthält. Die Daten dieser Tabelle werden in einem nicht normalisierten Formular gespeichert, damit Benutzer und Dienste den Inhalt verstehen und ändern können.

ci_twa_relation

Ergänzt die Tabelle "ci_twa_ci". Diese Tabelle enthält Informationen zu CI-Beziehungen.

Die TWA-Spaltennamen entsprechen, mit einigen Ausnahmen, den Attributen, die mit GRLoader verwendet werden.

Hinweis: Weitere Informationen zu CI-Attributen finden Sie im *Technischen Referenzhandbuch zu CA CMDB*.

TWA-SQL-Spaltennamen

Spaltennamen in den Tabellen "ci_twa_ci" und "ci_twa_relation" entsprechen mit einigen Ausnahmen den CI- und Beziehungsattributnamen.

Gemeinsame TWA-Felder für "ci_twa_ci" und "ci_twa_relation"

apply_after_dt (Nach Datum anwenden)

GRLoader führt die Transaktion nur aus, wenn das aktuelle Datum nach dem Datum für "Nach Datum anwenden" liegt. Gemessen wird in Sekunden ab der Epoche. Wenn der Wert bei Null liegt (0), wird dieses Feld ignoriert.

tran_chg_ref_num (Change)

Gibt die mit dieser Transaktion verknüpfte Change-ID an. Von der "-chg"-Option in GRLoader wird dieses Attribut verwendet, um nur Transaktionen mit der bestimmten Change-Nummer auszuwählen.

Hinweis: Weitere Informationen zum Verwenden der "-chg"-Option finden Sie im Abschnitt über das [Filtern nach Change-Nummer](#) (siehe Seite 703).

tran_status (Transaktionsstatus)

Gibt den Status der Transaktion an. Er muss einen der folgenden Werte haben (nur Transaktionen mit tran_status=1 werden ausgeführt).

Wert	Kurze Beschreibung	Ausführliche Beschreibung
0	Beginn	Standardwert. Eingriff zur Umstellung auf "Bereit" erforderlich, damit GRLoader auf diese Transaktion reagieren kann
1	Bereit	Die Transaktion kann in die entsprechenden CI- oder Beziehungstabellen geladen werden.
2	Erfolgreich	Erfolgreich bearbeitete Transaktion
3	Warnung	Warnung beim Laden in "ca_owned_resource/bmhier"
4	Fehler	Fehler beim Laden in "ca_owned_resource/bmhier"
40000+	Benutzerdefinierte Verwendung	

tran_message (Meldung)

GRLoader-Meldung, die die Ergebnisse des Ladevorgangs oder der Simulation anzeigt.

tran_dt (Transaktionsdatum)

Verhindert die unabsichtliche Überlagerung von aktuellen Informationen durch alte Transaktionsdaten. Das Transaktionsdatum wird mit dem letzten Änderungsdatum des CIs verglichen, und GRLoader lehnt die Transaktion ab, wenn das CI neuer ist.

Wenn GRLoader eine Transaktion ablehnt, weil sie älter als das Ziel-CI ist, prüfen Sie, ob die Transaktion noch anwendbar ist. Setzen Sie dann das Transaktionsdatum manuell auf ein aktuelleres Datum und führen Sie GRLoader erneut aus.

tgt_delete_flag (Aktiv?)

Deaktiviert das Ziel-CI oder die Beziehung. Setzen Sie diesen Wert auf "1" (eins). Wenn Sie jedoch "delete_flag" auf 1 setzen, wird damit die Transaktion gelöscht.

"ci_twa_ci"-Spalten

Zusätzlich zu den folgenden Spaltennamen können Sie auch CI-Attributnamen als Spaltennamen in den SQL-Anweisungen angeben.

tgt_id (Ziel-CI)

Gibt die UUID des Ziel-CIs an. Wird bei der manuellen Abstimmung verwendet.

superseded_by (Ersetzt durch)

Gibt die UUID des ersetzten CIs an.

tgt_tenant (Mandant)

Gibt den Mandantennamen an, der dem Ziel-CI zugeordnet ist. Mandanten können nur zum Zeitpunkt der Erstellung von CIs zugewiesen werden, wenn der GRLoader-Benutzer eine entsprechende Autorisierung hat. Gilt nur, wenn die Funktion für mehrere Mandanten aktiviert ist.

"ci_twa_relation"-Spalten

Zusätzlich zu den folgenden Spaltennamen können Sie auch CI-Attributnamen als Spaltennamen in den SQL-Anweisungen angeben.

Verwenden Sie die folgenden Datenbankspaltennamen, wenn Sie SQL für die Definition der Beziehungstransaktionen verwenden:

provider_name (Übergeordneter Name)

provider_mac_address (MAC-Adresse des Providers)

provider_serial_number (Übergeordnete Seriennummer)

provider_system_name (Übergeordneter Hostname)

provider_asset_num (Nummer des übergeordneten Assets)

provider_dns_name (Übergeordneter DNS-Name)

provider_tenant (Provider-Mandant)

AND

dependent_name (Abhängiger Name)

dependent_mac_address (Abhängige MAC-Adresse)

dependent_serial_number (Abhängige Seriennummer)

dependent_system_name (Abhängiger Hostname)

dependent_asset_num (Abhängige Asset-Nummer)

dependent_dns_name (Abhängiger DNS-Name)

dependent_tenant (Untergeordneter Mandant)

Wenn übergeordnete oder untergeordnete CI UUIDs bekannt sind, können Sie die folgenden Felder verwenden:

"provider_id" gibt die UUID des übergeordneten CIs an.

"dependent_id" gibt die UUID des untergeordneten CIs an.

Hinweis: "provider_tenant" und "dependent_tenant" gelten nur, wenn die Funktion für mehrere Mandanten aktiviert ist.

Einfügen neuer Datensätze in den TWA

Sie können von außerhalb von CA SDM einen neuen Datensatz in die Tabellen "ci_twa_ci" und "ci_twa_relation" einfügen.

Zum Einfügen von Datensätzen in die Tabellen "ci_twa_ci" und "ci_twa_relation" geben Sie in der Spalte "ID" wie folgt eine "0" an:

```
insert into ci_twa_ci values(id, name) values(0, 'test-ci');  
insert into ci_twa_relation values(id, type) values(0, 'test-relation-type');
```

Vorsicht: Wenn die Option für mehrere Mandanten aktiviert ist, geben sie je nach Bedarf die Attribute "tenant", "tgt_tenant", "provider_tenant" oder "dependent_tenant" an. Wenn Sie TWA-Transaktionen erstellen, ohne einen Mandanten anzugeben, wird der öffentliche Mandant verwendet.

Verwenden von ODBC-Treibern

Sie können statt GRLoader auch SQL verwenden, um den TWA zu laden. Es wird empfohlen, den zu CA SDM gehörigen ODBC-Treiber zu verwenden, anstelle von Native SQL-Diensten. Die Verwendung des ODBC-Treibers bietet die folgenden Vorteile:

- Leistung
- Sicherheit
- Datenbank-Unabhängigkeit

- Datenintegrität in einer Umgebung, in der Datenbankaktualisierungen vom CA SDM-Server zur gleichen Zeit durchgeführt werden können, in der das Tool zur Massенbearbeitung ausgeführt wird.

Unbedingt beachten

- Nur CA SDM-ODBC-Treiber erfüllen Sicherheitsfunktionen wie Mandantenfähigkeit, Datenpartitionierung, und rollenbasierter Zugriff. Bei der Ausführung von SQL mit systemeigenen DBMS-Treibern werden keine Sicherheitsfunktionen angewendet.
- Sichern Sie Ihre Daten regelmäßig, wenn Sie Aktualisierungen mit Native SQL durchführen.

CI-Kennungen im TWA

In der Tabelle "ci_twa_ci" werden drei Kennungen einer CI-Transaktion zugeordnet: "ID", "tgt_id" und "superseded_by". Diese Attribute werden im Folgenden erläutert:

- "ID" ist die Sequenznummer der Transaktion. **Ändern Sie dieses Feld nicht.** IDs von 1-2.000.000.000 sind für die Verwendung von Systemen vorgesehen, die den TWA außerhalb des CA SDM-Servers ändern. IDs von 2.000.000.001 bis etwa 4 Milliarden sind für die Verwendung von CA SDM vorgesehen. Wenn dem System keine IDs mehr zur Verfügung stehen, müssen Sie die Tabelle neu initialisieren.
- "tgt_id", "provider_id" oder "dependent_id" ist die UUID des Ziel-CI. Aktivieren Sie dieses Feld, wenn Sie eine manuelle Abstimmung ausführen.
- "superseded_by" ist die UUID des ersetzenden CI. Setzen Sie dieses Feld, wenn Sie das ersetzende CI für die Transaktion festlegen.

Festlegen des Transaktionsstatus

Sie können den Transaktionsstatus ("tran_status") jeder Transaktion im TWA festlegen. Damit GRLoader eine Transaktion verarbeitet, muss der Status auf "Bereit" (tran_status=1) gesetzt werden.

Wert	Kurze Beschreibung	Ausführliche Beschreibung
0	Beginn	Standardwert. Eingriff zur Umstellung auf "Bereit" erforderlich, damit GRLoader auf diese Transaktion reagieren kann
1	Bereit	Die Transaktion kann in die entsprechenden CI- oder Beziehungstabellen geladen werden.
2	Erfolgreich	Erfolgreich bearbeitete Transaktion
3	Warnung	Warnung beim Laden in "ca_owned_resource/bmhier"

Wert	Kurze Beschreibung	Ausführliche Beschreibung
4	Fehler	Fehler beim Laden in "ca_owned_resource/bmhier"
40000+	Benutzerdefinierte Verwendung	

Wenn GRLoader mit `-lftwa` mindestens zweimal ausgeführt wird, aktualisiert sich der Status nach dem ersten Mal. Bei allen nachfolgenden Ausführungen werden keine Transaktionen gefunden. Setzen Sie den Status der bereiten Transaktionen vor jeder Ausführung von `-lftwain` in GRLoader zurück.

Weitere Informationen zur Darstellung von XML-Daten in den TWA-Tabellen finden Sie in den XML-Beispielen der vorherigen Abschnitte.

Freigeben von Tabellen für CA SDM

Nur SQL Server

Wenn Sie SQL verwenden, um die Tabellen "ci_twa_ci" und "ci_twa_relation" zu aktualisieren, definieren Sie manuell die Spalte "last_mod_dt" wie folgt:

```
SET last_mod_dt = DATEDIFF(s, '19700101', GETUTCDATE())
```

Beispiel: Festlegen von "last_mod_dt"

Das folgende Beispiel zeigt, wie das Feld "last_mod_dt" festgelegt wird:

```
UPDATE ci_twa_ci
    SET tran_status=1,
        last_mod_dt = DATEDIFF(s, '19700101', GETUTCDATE())
    WHERE tran_status=1,
```

Hinweis: Aktualisierte TWA-Tabellen erscheinen möglicherweise erst nach einigen Minuten in der Web-Schnittstelle, bzw. im GRLoader. Weitere Informationen zur Zeitplanung von Aktualisierungen finden Sie in der Option "NX_DBMONITOR_TIMER_MINUTES".

Aktualisieren von Daten im TWA über die Web-Schnittstelle

Sie können CI- und Beziehungstransaktionen vor der Ausführung bereitstellen, indem Sie Daten in den Staging-Bereich des TWA kopieren. Im Staging-Bereich können Sie CIs und Beziehungen unter Verwendung der Web-Schnittstellen bearbeiten.

Außerdem können Sie die CI- und Beziehungstransaktionen validieren, um die Erstellung ungültiger Daten oder neuer CIs zu verhindern, wenn ein einzelnes CI oder vorhandene CIs hätten aktualisiert werden sollen. Bei dieser Vorgehensweise können Sie die einzelnen Transaktionen und die möglichen aktualisierbaren CIs anzeigen, so dass Sie die Transaktion manuell auf das Ziel-CI abstimmen können.

Um den Transaktionsarbeitsbereich zu verwalten, wählen Sie die Registerkarte "Administration" aus, und navigieren Sie zum Knoten "CA CMDB, Transaktionsarbeitsbereich". Über diesen Knoten können Sie die Seiten des Transaktionsarbeitsbereichs verwalten.

Hinweis: Weitere Informationen finden Sie in der *Online-Hilfe*.

Weitere Informationen:

[Verwalten von CI-Transaktionen](#) (siehe Seite 698)

[Verwalten von mehrdeutigen CI-Transaktionen](#) (siehe Seite 699)

[Manuelle Abstimmung](#) (siehe Seite 699)

Verwalten von CI-Transaktionen

Die Detailseite für CI-Transaktionen zeigt alle nicht leeren Attribute der Transaktion an. Wenn Sie das Kontrollkästchen "Leere Werte ausblenden" deaktivieren, werden alle CI-Attribute angezeigt. Weitere Attributinformationen erhalten Sie über den Attributnamen.

Sie haben folgende Möglichkeiten:

- Transaktion anzeigen
- Transaktion erstellen
- Transaktion bearbeiten
- Änderungen der Transaktionen speichern oder abbrechen (nur im Bearbeitungsmodus)
- Ursprüngliche Transaktionsdaten wiederherstellen (nur im Bearbeitungsmodus)
- Daten anzeigen oder verstecken (Registerkarte "Attribute")
- Ziel-CI festlegen (Registerkarte "Abstimmung")

Nach dem Speichern einer Transaktion klicken Sie auf die Registerkarte "Abstimmung", damit die betreffende Transaktion überprüft, ob das gewünschte Ziel-CI Mehrdeutigkeiten enthält. Sind Mehrdeutigkeiten vorhanden, können Sie [ein Ziel-CI angeben](#) (siehe Seite 681). Sobald Sie mit der Eingabe aller Daten fertig sind, können Sie [das Laden der Daten simulieren](#) (siehe Seite 690), um sie zu validieren und die Abstimmung zu überprüfen.

Wichtig! In den TWA über diese Web-Schnittstelle eingegebene Daten müssen die Regeln befolgen, die im Abschnitt zum [Laden von Daten in den TWA mit GRLoader](#) (siehe Seite 685) beschrieben sind.

Die Web-UI validiert keine Daten im TWA, die zwischen Groß- und Kleinschreibung unterscheiden. Überprüfen Sie, dass die eingegebenen Werte genau den Suchwerten entsprechen. Alternativ dazu können Sie beim Ausführen von GRLoader die Option "-I" angeben, um Suchen ohne Berücksichtigung der Groß- und Kleinschreibung auszuführen.

Hinweis: Auch wenn "tgt_id" oder "superseded_by" als UUIDs in der Transaktion gespeichert sind, werden sie auf der Web-Schnittstelle als CI-Namen angezeigt.

Verwalten von mehrdeutigen CI-Transaktionen

Sie können vor dem Laden von Transaktionsdaten Transaktionen mit mehrdeutigen CI-Zielen überprüfen und ändern. Sie können auch CI-Transaktionen auflösen, die kein Ziel-CI, aber identifizierende Attribute für ein oder mehrere CIs aufweisen. Diese Lösung gewährleistet, dass das richtige CI aktualisiert wird, und verhindert die Erstellung von falschen oder inkonsistenten Daten.

Nach dem Speichern einer Transaktion klicken Sie auf die Registerkarte "Abstimmung", damit die betreffende Transaktion überprüft, ob das gewünschte Ziel-CI Mehrdeutigkeiten enthält. Sind Mehrdeutigkeiten vorhanden, können Sie [ein Ziel-CI angeben](#) (siehe Seite 681). Sobald Sie mit der Eingabe aller Daten fertig sind, können Sie [das Laden der Daten simulieren](#) (siehe Seite 690), um sie zu validieren und die Abstimmung zu überprüfen.

Weitere Informationen zum Abstimmen der Daten im TWA finden Sie unter [Überprüfen und Ändern von eingehenden Daten mithilfe des Transaktionsarbeitsbereichs \(TWA\)](#) (siehe Seite 676).

Manuelle Abstimmung

Um ein CI manuell abzustimmen, legen Sie das Ziel- CI fest, das mit den identifizierenden Attributen der Transaktion übereinstimmt, und legen Sie die "tgt_id" dieser Transaktion auf die UUID des Ziel-CIs fest.

Wenn GRLoader eine Transaktion verarbeitet, die eine "tgt_id" angibt, wird das Ziel-CI mit den Transaktionsinformationen aktualisiert und dieses CI erneut registriert, wenn sich seine identifizierenden Attribute geändert haben.

Sie können das Ziel-CI ausdrücklich in der Transaktion angeben. Sie können auch die Registerkarte "Abstimmung" verwenden, um ein Ziel-CI auszuwählen.

Weitere Informationen finden Sie unter [Überprüfen und Ändern von eingehenden Daten mithilfe des Transaktionsarbeitsbereichs \(TWA\)](#) (siehe Seite 676).

Angeben von Ziel-CIs für mehrdeutige CI-Transaktionen

Sie können ein CI für eine mehrdeutige Transaktion angeben, sodass die entsprechenden Daten unabhängig von den Werten der in der Transaktion angegebenen identifizierenden Attribute an ein bestimmtes Ziel-CI geleitet werden.

So geben Sie das Ziel CI für eine mehrdeutige CI Transaktion an

1. Wählen Sie auf der Seite "Mehrdeutige Transaktionen – Liste" eine CI Transaktion aus.

Die Seite "Configuration Item – Transaktionsdetail" wird angezeigt.

2. Klicken Sie auf "Bearbeiten".

Die Seite "Configuration Item – Transaktion aktualisieren" wird angezeigt.

3. Wählen Sie auf der Registerkarte "Abstimmung" ein CI aus der Liste, um es als Ziel-CI für die Transaktion festzulegen. Klicken Sie auf "Ziel-CI" festlegen und dann auf "Speichern".

Das ausgewählte CI wird zum Ziel-CI der Transaktion.

Verwalten von Beziehungstransaktionen

In "Beziehungstransaktionen - Liste" werden Dateneingaben für Beziehungstransaktionen angezeigt.

Über diese Seite können Sie folgende Aufgaben ausführen:

- Nach Beziehungstransaktionen suchen

Auf der Liste haben Sie folgende Möglichkeiten:

- Erstellen von Beziehungstransaktionen
- In Liste bearbeiten (außer dem Identifizieren von Attributen)

Aktualisieren von Beziehungstransaktionen

Sie können Daten für einzelne Beziehungstransaktionen anzeigen und ändern. Die Seite "Beziehungstransaktion – Detail" bietet folgende Möglichkeiten:

- Erstellen von Beziehungstransaktionen
- Anzeigen der Transaktionen
- Transaktion bearbeiten
- Änderungen der Transaktionen speichern oder abbrechen (nur im Bearbeitungsmodus)
- Ursprüngliche Transaktionsdaten wiederherstellen (nur im Bearbeitungsmodus)

So aktualisieren Sie eine Beziehungstransaktion:

1. Klicken Sie auf "Bearbeiten".
Die Seite "Beziehungstransaktion aktualisieren" wird angezeigt.
2. Bearbeiten Sie die Daten in den Feldern und ergänzen Sie sie.
3. Wählen Sie die Option "Aktiv".
4. Klicken Sie auf "Speichern".
Die Beziehungstransaktion wird gespeichert.

Sobald Sie mit der Eingabe aller Daten fertig sind, können Sie das Laden der Daten simulieren, um sie zu validieren und die Abstimmung zu überprüfen.

Wichtig! In den TWA über diese Web-Schnittstelle eingegebene Daten müssen die Regeln befolgen, die im Abschnitt zum [Laden von Daten in den TWA mit GRLoader](#) (siehe Seite 685) beschrieben sind.

Die Web-UI validiert keine Daten im TWA, die zwischen Groß- und Kleinschreibung unterscheiden. Überprüfen Sie, dass die eingegebenen Werte genau den Suchwerten entsprechen. Alternativ dazu können Sie beim Ausführen von GRLoader die Option "-i" angeben, um Suchen ohne Berücksichtigung der Groß- und Kleinschreibung auszuführen.

Hinweis: Auch wenn "provider_id" oder "dependent_id" als UUIDs in der Transaktion gespeichert sind, werden sie in der Web-Schnittstelle als CI-Namen angezeigt.

Laden von Transaktionen in die CMDB

Anstatt die XML-Eingabe zur Erstellung von CIs und Beziehungen zu verwenden, können Sie die folgenden Optionen zur Auswahl des TWA als Eingabequelle festlegen:

–lftwa (aus TWA laden)

–lftwai (aus TWA laden und inaktiv)

Hinweis: Im Gegensatz zu anderen GRLoader-Modi, die die Datei "err.xml" verwenden, werden beim Laden aus dem TWA Fehlermeldungen an das Meldungsfeld der Transaktion zur Ansicht zurückgegeben.

Nach der Verarbeitung der Transaktionen legt GRLoader den Transaktionsstatus fest, um anzugeben, ob die TWA-Transaktionen erfolgreich abgeschlossen wurden oder fehlgeschlagen sind. Wenn GRLoader die Option "-lftwa" mehrmals nacheinander ausführt, setzen Sie den Status der Transaktion zwischen den Ausführungen auf "Bereit", da bereits geladene Daten nicht erneut geladen werden.

Die Transaktion wird vom TWA ausgeführt, als ob GRLoader unter der Verwendung von XML-Eingabe ausgeführt werden würde. Die Transaktionssicherheit basiert auf dem Benutzer, der den Ladevorgang aus dem TWA durchführt, und nicht auf dem Benutzer, der die TWA-Transaktion ursprünglich geladen hat.

Eine Überprüfung findet statt, wenn die Transaktionen erfolgreich verarbeitet werden.

Anmerkung: Bevor Sie das Laden ausführen, können Sie anhand der Simulationsoptionen ("-simci") und "-simrel") feststellen, ob eine Reihe von Transaktionen neue CIs oder Beziehungen erstellt. Weitere Informationen finden Sie unter [Simulieren von TWA-Operationen](#) (siehe Seite 690).

Weitere Informationen:

[So vermeiden Sie Datenregression](#) (siehe Seite 702)

[Filtern nach Change-Nummer](#) (siehe Seite 703)

So vermeiden Sie Datenregression

Während sich Transaktionsdaten eines CI im TWA befinden, können einige andere Aktionen diese CIs aktualisieren, was dazu führen kann, dass die TWA-Transaktionsdaten ungültig werden. Um unerwünschte Datenregression zu verhindern, vergleicht GRLoader das TWA-Feld "tran_dt" (Transaktionsdatum) mit dem Datum der letzten Änderung ("last_update_dt") des CI bzw. dem Datum der letzten Änderung ("last_mod_dt") der Beziehung. Wenn das Feld "last_update_dt" neuer ist, lehnt GRLoader die TWA-Transaktion ab und schreibt eine Fehlermeldung in die Spalte "tran_message".

Sie können dies über eine der folgenden Maßnahmen lösen:

- Verwenden Sie die Web-Schnittstelle, um das CI- oder Beziehungsfeld "tran_dt" (Transaktionsdatum) auf einen besser geeigneten Wert zu setzen.
- Definieren Sie die GRLoader-Option `grloader.workarea.ignore_transaction_dates="yes"`, um die Transaktionsdaten zu ignorieren, und fügen Sie die Daten ein.

Hinweis: Wenn GRLoader eine Transaktion ablehnt, weil sie älter als das Ziel-CI ist und Sie geprüft haben, dass die Transaktion ausgeführt werden soll, dann setzen Sie das Transaktionsdatum manuell auf ein aktuelleres Datum und führen Sie GRLoader erneut aus.

Achtung! Die Option zum Ignorieren der Transaktionsdaten kann Daten-Backleveling oder Datenregression verursachen. Wenn ein CI oder eine Beziehung mehrmals mit derselben Ausführung von "-lftwa" in GRLoader aktualisiert wird, wird das Datum "last_update" des CI bzw. der Beziehung auf den aktuellen Zeitpunkt der ersten Aktualisierung festgelegt. Um mehrere Aktualisierungen für dasselbe CI oder dieselbe Beziehung zuzulassen, wird eine zusätzliche Überprüfung durchgeführt, um festzustellen, ob das CI bzw. die Beziehung nach dem Start von GRLoader aktualisiert wurde. Wenn ja, wird die Aktualisierung zugelassen.

Filtern nach Change-Nummer

Die GRLoader-Option "-chg" kann dazu verwendet werden, nur Transaktionen auszuwählen, die mit einem Change-Ticket verknüpft sind. Wenn Sie nach Change-Nummer filtern möchten, müssen Sie das Change-Attribut (tran_chg_ref_num) auf die entsprechende Change-Anfragenummer setzen.

Hinweis: Die Change-Zeichenfolge wird beim Laden in CMDB nicht validiert.

Beispiel: Nach Change-Ticket filtern

Mit der folgenden Option werden nur Transaktionen geladen, die in Zusammenhang mit Change 23434 stehen.

```
grloader -lftwa -chg 23434
```

TWA-Administration

Der TWA kann die folgende Verwaltung benötigen:

- TWA erweitern - erforderlich, wenn Sie OOB-Familien erweitern oder wenn Sie Ihre eigenen benutzerdefinierten Familien definieren.
- TWA archivieren und löschen
- Verwenden des TWA mit CA Cohesion ACM
- Datenbankeinschränkungen

Weitere Informationen:

[So erweitern Sie das TWA-Objekt:](#) (siehe Seite 704)

[Archivieren und Löschen des TWA](#) (siehe Seite 705)

[TWA-Befehlsoptionen für GRLoader](#) (siehe Seite 705)

[TWA-Optionen für die GRLoader-Konfigurationsdatei](#) (siehe Seite 706)

[Verwenden des TWA mit CA Cohesion ACM](#) (siehe Seite 707)

[Datenbankeinschränkungen](#) (siehe Seite 707)

So erweitern Sie das TWA-Objekt:

Jegliche Änderungen am CA CMDB-Familienschema erfordern parallele Änderungen am TWA-Schema. Wenn keine benutzerdefinierten Familien oder Attribute definiert wurden, sind keine Änderungen im TWA erforderlich.

So erweitern Sie das TWA-Objekt

1. Passen Sie die benutzerdefinierten Familien und Attribute mit Hilfe der Verfahren unter "Erweitern von CA CMDB" im *Administrationshandbuch* an.
2. Fügen Sie mit dem Schemadesigner-Tool von Web Screen Painter die neuen Familienattribute zum Schema "ci_twa_ci" hinzu.

So fügen Sie dem Schema "ci_twa_ci" ein neues Attribut hinzu:

1. Verwenden Sie das Schemadesigner-Tool von Web Screen Painter und öffnen Sie das Schema für die Tabelle "ci_twa_ci".
2. Fügen Sie der Erweiterungstabelle das gewünschte Familienattribut hinzu.
3. Veröffentlichen Sie das geänderte Schema "ci_twa_ci".

Hinweis: Das neue Attribut muss als STRING vorliegen und den längstmöglichen Textwert beinhalten.

3. Fügen Sie wie folgt die Metadaten für die benutzerdefinierte Familie zu TWA hinzu:
 1. Verwenden Sie das Schemadesigner-Tool von Web Screen Painter und öffnen Sie die Datei "cmdb_metadata_site_families.html".
 2. Fügen Sie "PDM_INCLUDE" für die entsprechende Datei "cmdb_metadata_extension.html" hinzu, die für die benutzerdefinierte Familie erstellt wurde.

Archivieren und Löschen des TWA

Um den TWA zu verwalten, stellt CA SDM die folgenden Archivierungs- und Lösungsregeln bereit:

CI-Inaktive Transaktionen

archiviert und löscht CI-Transaktionen, die für die Löschung markiert werden.

CI-Erfolgreiche Transaktionen

archiviert und löscht CI-Transaktionen, die erfolgreich abgeschlossen wurden.

Beziehung – Inaktive Transaktionen

archiviert und löscht Beziehungstransaktionen, die für die Löschung markiert sind.

Beziehung – Erfolgreiche Transaktionen

archiviert und löscht Beziehungstransaktionen, die erfolgreich abgeschlossen wurden.

Sie können auswählen, wie oft die Regeln ausgeführt werden sollen oder ob sie aktiviert sein sollen.

Sie können die Regeln zum Archivieren und Löschen des TWA anpassen und aktivieren. Wenn Sie den TWA häufig verwenden, achten Sie darauf, dass die Anzahl der Einträge im TWA von DBMS beschränkt wird.

Wenn Sie den TWA neu initialisieren müssen, um alle darin enthaltenen Daten zu löschen, gehen Sie wie folgt vor:

- Setzen Sie alle Transaktionen auf "Inaktiv"
- Führen Sie eine Archivierungslöschung aus

Wichtig! Verwenden Sie nicht SQL zum Löschen aller Einträge im TWA, da es die erforderlichen Kopfzeilendatensätze löscht.

TWA-Befehlsoptionen für GRLoader

CA SDM stellt die folgenden Befehlsoptionen für die Verwendung in der GRLoader-basierten TWA-Verarbeitung zur Verfügung:

-littwa

Lädt XML in den Ausgangszustand.

-littwar

Lädt XML in den Zustand "Bereit".

-lftwa

Lädt Transaktionen aus dem TWA.

-lftwai

Lädt Transaktionen aus dem TWA und deaktiviert erfolgreiche Transaktionen.

-chg *nnnn*

Wird mit -lftwa und -lftwar benutzt. Wählt nur solche Transaktionen aus, die Change *nnnn* zugeordnet sind.

Hinweis: Die Change-Zeichenfolge wird beim Laden in CMDB nicht validiert.

-l

Die Groß-/Kleinschreibung von Suchattributen wird ignoriert. Sofern Sie diese Option nicht verwenden, ist bei Freitext für Suchattribute standardmäßig auf Groß-/Kleinschreibung zu achten.

-simci

Ermittelt, ob CI-Transaktionen CIs erstellen oder aktualisieren können. Wenn diese Option verwendet wird, führt GRLoader eine Fehlerprüfung nur in Bezug auf CIs aus.

-simrel

Ermittelt, ob Beziehungstransaktionen Beziehungen erstellen oder aktualisieren können. Diese Option prüft Beziehungen auf das Vorhandensein von Provider und abhängigen CIs, validiert Beziehungstypen usw.

TWA-Optionen für die GRLoader-Konfigurationsdatei

CA CMDB bietet die folgenden TWA-Optionen für die GRLoader-Konfigurationsdatei:

`grloader.emptyvalue=EMPTY`

`grloader.loadfromtwa=yes`

`grloader.loadfromtwa.inactivatesuccessful=yes/no`

`grloader.loadtotwa=yes`

`grloader.loadtotwa.ready=yes/no`

`grloader.workarea.delimiters={ }`

`grloader.workarea.ignore_transaction_dates=yes`

`grloader.simulateloadci=yes/no`

`grloader.simulateloadrelation=yes/no`

Verwenden des TWA mit CA Cohesion ACM

Um den TWA mit CA Cohesion ACM zu verwenden, wenden Sie den Patch RO08739 auf CA Cohesion ACM r5 an. Dieser Patch ermöglicht es Ihnen, auf der Registerkarte "Exportoptionen" der Definition des CA CMDB-Exportberichts im Feld "Weitere Optionen" die Option "-littwa" festzulegen. Aktualisieren Sie die GRLoader-Komponente. Bei Fragen wenden Sie sich an den CA-Support.

Datenbankeinschränkungen

Der TWA unterliegt folgenden Dateneinschränkungen der zugrunde liegenden Datenbank:

- Wenn TWA und Microsoft SQL Server verwendet werden, darf die Gesamtlänge einer Datentransaktion 8060 Byte nicht überschreiten.
- Wenn die Hilfsprogramme "dbload" und "pdm_load" verwendet werden, ist der Ladevorgang auf 512 Spalten begrenzt.
- Oracle hat eine Beschränkung von 1000 Spalten. Wenn Sie CA CMDB anpassen, stellen Sie sicher, dass die Gesamtanzahl an Attributen der verschiedenen Familien 1000 nicht überschreitet (gilt sowohl für von CA zur Verfügung gestellte als auch für anwenderdefinierte Attribute).
- Die Einschränkungen von SQL Server 2005 werden in der folgenden Tabelle beschrieben:

Art der Einschränkung	Limit (32-Bit und 64-Bit)
Spalten pro breite Tabelle	30000
Spalten pro Basistabelle	1024
Spalten pro SELECT-Anweisung	4096
Byte pro Zeile	8060
Zeilen pro Tabelle	Durch vorhandenen Speicherplatz begrenzt

CA CMDB-Datenwartung

Die Aufgaben, die Sie durchführen, um CMDB-Daten zu verwalten, erfordern Administratorrechte. Diese Aufgaben umfassen das Einrichten von Familien, Klassen, und Beziehungstypen, die verwendet werden, um Configuration Items und Beziehungsinformationen zu verwalten.

Weitere Informationen:

[CA CMDB-Strukturen für Familie und Klasse](#) (siehe Seite 708)

[Ändern der Familie/Klasse eines einzigen CI](#) (siehe Seite 709)

[Ändern der Familie/Klasse einer Liste von CIs](#) (siehe Seite 709)

[Ändern von CI-Familien oder CI-Klassen mit GRLoader](#) (siehe Seite 710)

[Erweitern von CA CMDB](#) (siehe Seite 710)

CA CMDB-Strukturen für Familie und Klasse

In CA CMDB stehen Ihnen standardmäßig bestimmte CI-Familien sowie deren CI-Klassen zur Verfügung.

Hinweis: Weitere Informationen zur Standard-Struktur für Familien/Klassen in CA CMDB finden Sie im *technischen CA CMDB-Referenzhandbuch*.

Hinweis: Für die folgenden Service Desk- und CA APM-Basisfamilien gibt es keine eigenen CA CMDB-Erweiterungstabellen:

- Computer
- Kontakt (als Basisobjekt)
- Hardware
- Standort (als Basisobjekt)
- Organisation (als Basisobjekt)
- Sonstige
- Projekt
- Software

In der CA CMDB erhalten CIs in diesen Datenbankfamilien Seiten mit CI-Details mit einigen externen Feldern. Sie enthalten nicht die Registerkarte "Attribute". Um die erweiterten CA CMDB-Funktionen, wie etwa die Nachverfolgung von familienspezifischen Attributen, Versionskontrolle, Snapshots und Baselines, nutzen zu können, wird empfohlen, diese CIs mit Hilfe der Funktion zum Ändern von Familien und Klassen in CA CMDB-Familien zu konvertieren.

Ändern der Familie/Klasse eines einzigen CI

Sie können die Familie und Klasse eines einzelnen Configuration Items ändern.

So ändern Sie die Familie und Klasse eines einzelnen Configuration Items:

1. Wählen Sie das CI aus, das Sie ändern möchten.
2. Klicken Sie auf "Bearbeiten".
Die Seite "CI aktualisieren" öffnet sich.
3. Ändern Sie den Wert "Klasse" des CI. Legen Sie eine Klasse für das CI fest, legen Sie gleichzeitig eine Familie fest. Sie können den Wert manuell eingeben, oder auf die Lupe klicken. Nun können Sie aus einer Liste von Klassen auswählen.
4. Klicken Sie auf "Speichern".
Die Familie und Klasse des einzelnen CI wird geändert.

Ändern der Familie/Klasse einer Liste von CIs

Sie können die Familie und Klasse einer Liste von CIs ändern.

So ändern Sie die Familie/Klasse einer Liste von CIs:

1. Klicken Sie unter "CI-Liste" auf "Filter anzeigen".
2. Füllen Sie ein oder mehrere der Suchfelder aus, und suchen Sie die Configuration Items, die Sie bearbeiten möchten.
3. Klicken Sie auf "Suche".
Unter "CI-Liste" werden nun alle Configuration Items angezeigt, die Ihren Suchkriterien entsprechen.
4. Klicken Sie auf "In Liste bearbeiten".
Unter "CI-Liste" werden nun alle Felder angezeigt, in denen Sie für sämtliche ausgewählte Configuration Items Änderungen vornehmen können.
5. Bearbeiten Sie die Felder "Familie" und "Klasse" nach Ihren Wünschen.
6. Klicken Sie auf "Alle ändern".
7. Klicken Sie auf "Speichern".
Aktualisieren Sie nun die CI-Liste, werden die aktualisierten Configuration Items angezeigt

Ändern von CI-Familien oder CI-Klassen mit GRLoader

Sie können die Familie und Klasse für ein CI mit GRLoader ändern.

So ändern Sie CI-Familien oder CI-Klassen mit GRLoader:

1. Generieren Sie einen XML-Code, um das CI-Attribut zu ändern.
2. Öffnen Sie in GRLoader das CI, das Sie ändern möchten.
3. Führen Sie nun den XML-Code in GRLoader aus, um das CI-Attribut zu ändern.

Die Familie und Klasse für ein CI werden geändert.

Beispiel: Festlegen der Klasse eines geöffneten CI auf "Dokument"

Im folgenden Beispiel sehen Sie ein XML-Fragment, das für ein geöffnetes CI die Klasse *Dokument* festlegt.

```
<ci>
  <name>Dokument Nr. 1
  <class>Dokument
</ci>
```

Wichtig! Versuchen Sie nicht, gleichzeitig Familie und Klasse eines CI zu ändern. Möchten Sie beides ändern, müssen Sie zwei separate CI-Aktualisierungen durchführen, und hierfür GRLoader zweimal starten.

Erweitern von CA CMDB

CA CMDB ist ein sehr flexibles System, das entsprechend Ihren Geschäftsanforderungen auf zusätzliche Familien, Klassen und Attribute erweitert werden kann. Neue Attribute können familienspezifisch oder *allgemein* (für alle Familien geltend) sein. Während CA CMDB vordefinierte Familien mit vielen auf Industriestandards basierenden Klassen und Attribute bietet, müssen für einige Geschäftsfälle eine oder mehrere der folgenden Aktivitäten ausgeführt werden:

- Erweitern einer oder mehrerer der CI-Familien durch Hinzufügen neuer Attribute. Um zum Beispiel eine GPS-Koordinate für jedes Gerät auf Ihrem Niederlassungscampus hinzuzufügen, können Sie ein `gps_coordinate`-Attribut definieren und eine beliebige Familie hinzufügen. Wenn Sie nur eine Familie erweitern müssen, definieren Sie die neuen Attribute mit dem Web Screen Painter-Schemadesigner in der vorhandenen Erweiterungstabelle. Außerdem müssen Sie beim Hinzufügen eines Attributs auch immer die Seite "Detail" der Registerkarte "Attribut" sowie die Metadatenformulare ändern, die das Attribut verwenden. Weitere Informationen finden Sie unter [Hinzufügen von Familienattributen](#) (siehe Seite 712).

- Erweitern aller CI-Familien durch Hinzufügen eines allgemeinen Attributs. Weitere Informationen finden Sie unter [Hinzufügen allgemeiner Attribute](#) (siehe Seite 713).
- Hinzufügen neuer Klassen zu einer vorhandenen Familie, um mehr Klassifizierungsdetails in Ihrem System zu unterstützen. Statt der generischen Serverklasse können Sie zum Beispiel eine getrennte Klasse für jedes Servermodell erstellen. Weitere Informationen finden Sie unter [Definieren einer neuen CI-Klasse](#) (siehe Seite 714).
- Hinzufügen einer neuen Familie mit Hilfe einer vorhandenen Erweiterungstabelle und ihrer Attribute. Eine neue Familie bietet eine alternative Möglichkeit zur Organisierung oder Klassifizierung von CIs. Weitere Informationen finden Sie unter [Definieren einer neuen CI-Familie](#) (siehe Seite 714).
- Wenn die vorhandene Klassen- oder die Familienstruktur nicht Ihren Anforderungen entspricht, können Sie mit einem Minimalsatz von Attributen noch einmal neu anfangen. Wenn Sie eine neue Familie mit Hilfe einer neuen Erweiterungstabelle hinzufügen möchten, definieren Sie die neue Erweiterungstabelle und ihre Attribute mit Hilfe des Web Screen Painter-Schemadesigners und erstellen Sie außerdem die neuen Formulare, die zum Anzeigen und Aktualisieren erforderlich sind. Weitere Informationen finden Sie unter [Erstellen eines neuen Attribut-Frameworks](#) (siehe Seite 715).

Wichtig: Das Erweitern von CA CMDB setzt besondere Kenntnisse von CA SDM-Datenstrukturen und -tabellen sowie Kenntnis von Web Screen Painter (WSP) voraus. Es wird empfohlen, dass Sie sich hierzu mit CA Services in Verbindung zu setzen und ferner die folgenden Abschnitte gründlich zu lesen und zu verstehen, bevor Sie versuchen, CA CMDB-Familien und -Attribute zu erweitern.

Hinzufügen neuer CA CMDB-Attribute

Das Hinzufügen eines neuen CA CMDB-Attributs erfordert sorgfältige Planung. CA CMDB bietet bereits zahlreiche Attribute in den vordefinierten Familien und Klassen. Ermitteln Sie daher zunächst, ob diese für Ihre Anforderungen ausreichen, bevor Sie eine Anpassung in Erwägung ziehen.

Wenn Sie feststellen, dass ein neues Attribut notwendig ist, wird empfohlen, möglichst konservativ zu verfahren und sich zu fragen, ob Folgendes erforderlich ist:

- Hinzufügen eines oder mehrerer neuer Attribute zu einer vorhandenen Familie
- Hinzufügen des neuen Attributs zu mehreren Familien

- Hinzufügen eines neuen allgemeinen Attributs, das für alle Familien gilt

Sie können eine vorhandene Familie durch Hinzufügen von neuen Attributen erweitern. Wenn zum Beispiel einigen Geräten auf Ihrem Niederlassungscampus eine GPS-Koordinate zugewiesen wird, können Sie einer beliebigen relevanten CI-Familie ein `gps_coordinate`-Attribut hinzufügen. Weitere Informationen finden Sie unter [Hinzufügen von Familienattributen](#) (siehe Seite 712).

Wenn Sie feststellen, dass die identifizierten Attributbedingungen die Verwendung neuer Familien und Klassen erfordern, schlagen Sie unter [Hinzufügen einer neuen CA CMDB-Familie oder -Klasse](#) (siehe Seite 713) nach.

Hinzufügen von Familienattributen

Sie können neue Attribute mit Hilfe des Web Screen Painter-Schemadesigners einer oder mehreren bestehenden Familien hinzufügen, wobei die Datenbank mit den zugehörigen CA SDM-Tabellen und -Dateien so aktualisiert wird, dass das neue Attribut eingefügt wird. Diese Methode ist der manuellen Aktualisierung der geänderten Tabellen und Dateien vorzuziehen.

So fügen Sie einer Familie ein neues Attribut hinzu:

1. Öffnen Sie das Schema, das der Erweiterungstabelle der Familie entspricht, mit Web Screen Painter-Schemadesigner.
2. Fügen Sie der Erweiterungstabelle das gewünschte Attribut hinzu.
3. Veröffentlichen Sie die geänderte Erweiterungstabelle.

Hinweis: GRLoader und Versionskontrolle holen neue Attribute automatisch ohne weitere Eingriffe ab. Es wird jedoch empfohlen, zusätzlich die Protokollierung zu aktivieren. Diese ist für Auditierungszwecke und die Aktivierung der Versionskontrolle zum Aufzeichnen aller Snapshots erforderlich.

Überprüfen Sie, dass `UI_INFO` für das Attribut auf **AUDITLOG** gesetzt ist, um die Protokollierung zu aktivieren.

Nachdem ein neues Familienattribut erstellt wurde, muss es jedem Bildschirmformular hinzugefügt zu werden, damit Benutzer dieses Attribut sehen und aktualisieren können. Es muss ferner zu dem für diese Erweiterungstabelle spezifischen Metadatenformular hinzugefügt zu werden. Weitere Informationen finden Sie unter [Hinzufügen von Attributen zu Formularen](#) (siehe Seite 718).

Außerdem erfordert die Versionskontrolle Metadaten, einschließlich Informationen zu Spaltenüberschriften und der verwandten CI-Standardattribute. Sie müssen neue Metadaten für alle neu erstellten Attribute definieren. Anweisungen hierzu finden Sie unter [Erstellen von Metadaten](#) (siehe Seite 719).

Hinzufügen allgemeiner Attribute

Allgemeine Attribute sind in der Tabelle **ca_owned_resource** im **nr**-Objekt gespeichert. Diese Tabelle bietet die folgenden anpassbaren Felder:

- smag_1
- smag_2
- smag_3
- smag_4
- smag_5
- smag_6

Wenn Sie weniger als sieben angepasste Attribute unter allen CI-Familien benötigen, sind diese Felder eine gute Lösung.

Diese benutzerdefinierten Felder werden in der bereitgestellten Form nicht in Formularen angezeigt. Um CA CMDB-Benutzern das Anzeigen oder Aktualisieren eines smag_*n*-Feldes zu ermöglichen, fügen Sie dieses mit dem Web Screen Painter (WSP) nach Wunsch einem beliebigen Anzeigeformular hinzu. Alle Protokollierungs- und GRLoader-Funktionen sind bereits aktiviert.

Hinweis: Informationen zu Verfahren mit Web Screen Painter-Schemadesigner finden Sie im Kapitel "Anpassung" im *CA Service Desk-Implementierungshandbuch* und im Abschnitt "Datenbankschema anpassen" in der Online-Hilfe zu Web Screen Painter.

Hinzufügen einer neuen CA CMDB-Familie oder-Klasse

Das Hinzufügen einer neuen CA CMDB-Familie erfordert sorgfältige Planung. CA CMDB bietet zahlreiche vordefiniert Familien und Klassen. Ermitteln Sie daher zunächst, ob diese für Ihre Anforderungen ausreichen, bevor Sie eine Anpassung in Erwägung ziehen. Ist dies nicht der Fall, können einige neuen Anforderungen durch einen der folgenden Schritte erfüllt werden:

- Definieren eine neue Klasse in einer vorhandenen Familie
- Definieren einer neuen Familie, die eine vorhandene Erweiterungstabelle verwendet

Wenn Sie feststellen, dass bestehende Erweiterungstabellen für Ihre Anforderungen unzureichend sind, überspringen Sie diesen Abschnitt, und fahren Sie mit dem Abschnitt [Erstellen eines neuen Attribut-Frameworks](#) (siehe Seite 715) fort, um eine Erweiterungstabelle und die erforderlichen Formulare zu erstellen.

Definieren einer neuen CI-Klasse

Sie können neue Klassen hinzufügen, um höhere Ebenen der Klassifizierungsgenauigkeit zu unterstützen. Statt zum Beispiel eine der von CA CMDB bereitgestellten Klassen in der Familie Hardware.Server zu verwenden, können Sie zusätzliche Klassen für verschiedene Servergeräte definieren.

Überprüfen Sie in der Liste der CI-Klassen, ob bereits eine geeignete Klasse existiert, bevor Sie eine neue CI-Klasse erstellen.

Hinweis: Wenn Sie auch eine neue Familie benötigen, um einen neuen Satz von Klassen zu verwalten, überspringen Sie dieses Thema, und fahren Sie mit [Definieren einer neuen CI-Familie](#) (siehe Seite 714) fort. Dann können Sie zurückgehen und die neue Familie mit Klassen füllen.

So definieren Sie eine CI-Klasse mit der Verwaltungsoberfläche:

1. Navigieren Sie zur Configuration Item-Klassenliste.
2. Klicken Sie auf "Neu erstellen".
Die Seite "Neue Configuration Item-Klasse erstellen" wird angezeigt.
3. Geben Sie einen eindeutigen Namen für die neue Klasse ein.
4. Geben Sie den geeigneten Familiennamen im Feld "Familie" ein, oder klicken Sie auf das Symbol oberhalb des Feldes, um nach einer Familie zu suchen.
5. Achten Sie darauf, dass der Datensatzstatus auf "Aktiv" eingestellt ist.
6. Klicken Sie auf "Speichern".
Die neue CI-Klasse ist nun definiert und einsatzbereit. Sie können jetzt neue CIs zu erstellen.

Definieren einer neuen CI-Familie

Vor der Erstellung einer Configuration Item-Familie sollten Sie überprüfen, ob nicht bereits eine geeignete Familie in der Liste der Configuration Item-Familien existiert. Ist dies nicht der Fall, können Sie neue Familien als alternative Methode zur Organisation oder Klassifizierung von CIs mit Hilfe vorhandener Attribute erstellen.

Wenn die neue Familie, die Sie benötigen, weder eine vorhandene Erweiterungstabelle noch die Standardtabelle verwenden kann, schließen Sie alle zusätzlichen Vorbereitungen ab, die unter [Erstellen eines neuen Attribut-Frameworks](#) (siehe Seite 715) beschrieben sind. Die neue Erweiterungstabelle kann zum Definieren neuer Familien verwendet werden.

So definieren Sie eine CI-Familie mit der Verwaltungsoberfläche:

1. Navigieren Sie zur Liste "Configuration Item-Familie".

2. Klicken Sie auf "Neu erstellen".

Die Seite "Neue Configuration Item-Familie erstellen" wird angezeigt.

3. Geben Sie einen eindeutigen Namen für die neue Familie ein.
4. Achten Sie darauf, dass der Datensatzstatus auf "Aktiv" eingestellt ist.
5. Wählen Sie im Feld "Erweiterungsname" die Erweiterungstabelle aus, die den Familietyp identifiziert, den Sie erstellen möchten. Hierbei kann es sich um eine neue Erweiterungstabelle handeln, die Sie kürzlich erstellt haben.

Fügen Sie beispielsweise eine Familie für nicht näher bestimmte Hardware hinzu, wählen Sie "ci_hardware_other". So stellen Sie sicher, dass die korrekten Attribute auf der Registerkarte "Attribute" angezeigt werden, wenn Sie neue Configuration Items erstellen, deren Klassen die neue Familie verwenden. Wenn Sie im Feld "Erweiterungsname" keinen Tabellennamen auswählen, wird beim Erstellen eines Configuration Item innerhalb der neuen Familie die Standardtabelle verwendet, und die Standardattribute werden angezeigt.

6. Geben Sie in das Feld "Beschreibung" eine Beschreibung ein.

Die eingegebene Beschreibung wird zu Informationszwecken in der Liste "Configuration Item-Familie" angezeigt.

7. Klicken Sie auf "Speichern".

Die Configuration Item-Familie wurde definiert.

Nun, da die neue Familie definiert ist, können Sie ihr Klassen hinzufügen wie unter [Definieren einer neuen CI-Klasse](#) (siehe Seite 714) beschrieben.

Erstellen eines neuen Attribut-Frameworks

Wenn keine der vorhandenen Klassen- oder Familienstrukturen Ihren Anforderungen entspricht, können Sie mit einem Mindestsatz von Attributen noch einmal neu anfangen. Hierzu ist die Erstellung einer neuen Erweiterungstabelle und anderer Unterstützungsstrukturen erforderlich.

Bevor Sie die CA CMDB-Verwaltungsoberfläche zum Definieren einer neuen CI-Familie anhand einer neuen Erweiterungstabelle verwenden, erstellen Sie die neue Erweiterungstabelle mit dem Web Screen Painter-Schemadesigner.

Um die neue Erweiterungstabelle zu verwenden, müssen Sie außerdem neue HTML-Formulare für folgende Komponenten erstellen:

- eine neue CI-Detailseite
- eine neue Registerkarte "Attribute" mit verknüpften Attributen
- ein neues Metadatenformular und Metadaten

CA CMDB stellt Vorlagen bereit, die Sie zum Erstellen dieser HTML-Formulare verwenden können. Die folgenden Abschnitte bieten ausführlichere Informationen zu den Voraussetzungen.

Hinweis: Informationen zu Verfahren mit Web Screen Painter-Schemadesigner finden Sie im Kapitel "Anpassung" im *CA Service Desk-Implementierungshandbuch* und im Abschnitt "Datenbankschema anpassen" in der Online-Hilfe zu Web Screen Painter.

Definieren Sie Folgendes, um das neue Framework in der CA CMDB-Benutzerschnittstelle zu verwenden :

- eine oder mehrere CI-Familien, die die neue Erweiterungstabelle verwenden
- CI-Klassen zum Klassifizieren Ihrer CIs nach Typ

Weitere Informationen:

[Hinzufügen einer neuen CA CMDB-Familie oder-Klasse](#) (siehe Seite 713)

Erstellen einer neuen Erweiterungstabelle

Bevor Sie eine Familie anhand einer neuen Erweiterungstabelle definieren können, müssen Sie die Datenbank mit der neuen Tabelle und darüber hinaus auch das CA CMDB-Schema mit Informationen zu dieser Tabelle aktualisieren.

So erstellen Sie eine Erweiterungstabelle:

1. Definieren Sie die neue Erweiterungstabelle und den Erweiterungsnamen mit Web Screen Painter-Schemadesigner.
2. Speichern und veröffentlichen Sie die neue Erweiterungstabelle.

Hinweis: WSP-Schemadesigner erstellt automatisch den Protokollierungsauslöser in CA CMDB.

Fahren Sie mit dem nächsten Abschnitt fort, um die CI-Detailseite zu erstellen.

Erstellen von CI-Detailseiten

Eine CI-Detailseite ist erforderlich, um die Anzeige von Attributen für CIs zu unterstützen, die mit einer neuen Erweiterungstabelle verknüpft sind.

Navigieren Sie zur Seite "CI-Detail".

1. Klicken Sie auf "Datei" > "Neu", und erstellen Sie ein Formular anhand von `detail_extension.template`, während der Web Screen Painter-Schemadesigner aktiv ist.
2. Speichern Sie dieses neue Formular als **`detail_extension.htmlpl`**. *extension* ist hier der Name der Erweiterungstabelle.
3. Befolgen Sie die in der Datei aufgeführten Anweisungen, und ersetzen Sie dabei die Zeichenfolge `***EXTENSION***` durch den Namen der neuen (zuvor definierten) Erweiterungstabelle.
4. Speichern Sie die Datei mit allen Änderungen.

Die Seite "CI-Detail" umfasst zwei Attributabschnitte:

- einen Abschnitt für allgemeine Attribute namens `cmdb_detail.htmlpl`
- einen familienspezifischen Abschnitt (die Registerkarte "Attribute") namens `nr_cmdb_extension_tab.htmlpl`. *extension* ist hier der Name der neuen Erweiterungstabelle.

Fahren Sie mit dem nächsten Abschnitt, [Erstellen der Registerkarte "CA Attribute"](#) (siehe Seite 717) fort.

Erstellen der Registerkarte "CA Attribute"

Die Registerkarte "Attribute" zeigt die familienspezifischen Attribute für ein CI.

So erstellen Sie die Registerkarte "Attribute":

1. Klicken Sie auf "Datei" > "Neu", und erstellen Sie ein Formular anhand von `nr_cmdb_extension_tab.template`, während der Web Screen Painter-Schemadesigner aktiv ist.
2. Speichern Sie diese Datei als **`nr_cmdb_extension_tab.htmlpl`**. *extension* ist hier der Name der neuen Erweiterungstabelle.
3. Befolgen Sie die in der Datei aufgeführten Anweisungen, und ersetzen Sie dabei die Zeichenfolge `***EXTENSION***` durch den Namen der neuen (zuvor definierten) Erweiterungstabelle.
4. Speichern und veröffentlichen Sie die Datei mit allen Changes.

Fahren Sie mit dem nächsten Abschnitt fort, um die Registerkarte "Attribute" zu füllen.

Hinzufügen von Attributen zu Formularen

Nachdem Sie ein neues Attribut mit dem Web Screen Painter-Schemadesigner in einer Erweiterungstabelle erstellt haben, muss dieses einem beliebigen Formular hinzugefügt werden, das zur Anzeige oder Aktualisierung verwendet wird. Für neue familienspezifische Attribute muss lediglich das Formular der Registerkarte "Attribute" namens **nr_cmdb_extension_tab.html** geändert werden. *extension* ist hier der Name der Erweiterungstabelle. Dieses Formular muss so bearbeitet werden, dass es alle neuen Attribute enthält.

So bearbeiten Sie ein Attributformular:

1. Verwenden Sie Web Screen Painter Visual Editor, und klicken Sie auf "Datei" > "Öffnen", um auf das geeignete Formular zuzugreifen.
2. Verschieben Sie die neuen Attribute per Drag-and-Drop auf das Formular.

Hinweis: Von CA CMDB bereitgestellte Formulare können nicht einfach mit dem Visual Editor von Web Screen Painter bearbeitet werden. Verwenden Sie stattdessen den Web Screen Painter-Texteditor auf der Registerkarte "Quelle".

3. Speichern und veröffentlichen Sie das Formular.

Wenn Sie noch kein Metadatenformular erstellt haben, fahren Sie mit dem Abschnitt [Erstellen von Metadatenformularen](#) (siehe Seite 718) fort. Um Metadaten für ein neues Attribut auf dem Formular zu definieren, fahren Sie mit dem Abschnitt [Erstellen von Metadaten](#) (siehe Seite 719) fort.

Erstellen von Metadatenformularen

Eine neue Erweiterungstabelle erfordert ein eigenes Metadatenformular, um Spaltenüberschriften und CI-Standardinformationen für die Versionskontrolle zu definieren.

So erstellen Sie das Metadatenformular:

1. Klicken Sie auf "Datei" > "Öffnen", während der Visual Editor von Web Screen Painter aktiv ist, um auf "cmdb_metadata_extension.template" zuzugreifen.
2. Speichern Sie diese Datei als **cmdb_metadata_extension.html**. *extension* ist hier der Name der neuen Erweiterungstabelle.
3. Befolgen Sie die in der Datei aufgeführten Anweisungen, und ersetzen Sie dabei die Zeichenfolge *****EXTENSION***** durch den Namen der neuen (zuvor definierten) Erweiterungstabelle.
4. Speichern und veröffentlichen Sie das Formular mit allen Änderungen.

Fahren Sie mit dem nächsten Abschnitt fort, um das Metadatenformular zu füllen.

Erstellen von Metadaten

Metadaten umfassen Informationen zu Attributspaltenüberschriften und CI-Standardinformationen, die für die Funktion Versionskontrolle erforderlich sind.

Wichtig: Metadaten erfordern eine sorgfältige Planung, um sicherzustellen, dass Snapshots die richtigen Daten und die Versionskontrolle die richtigen Titel enthalten sowie erfolgreiche Standard-CI-Vergleiche vorliegen.

So erstellen Sie Metadaten:

1. Klicken Sie auf "Datei" > "Öffnen", während der Visual Editor von Web Screen Painter aktiv ist, um auf **cmdb_metadata_extension.html** zuzugreifen. *extension* ist hier der Name der Erweiterungstabelle.
2. Kopieren und ändern Sie die angegebene Zeile für jedes Attribut in der neuen Erweiterungstabelle anhand der im Formular aufgeführten Anweisungen.

Hinweis: Die folgenden erforderlichen Attribute, benötigen keine Metadaten:

- ID
- Last_modified_by
- Etc (muss bereitgestellt werden)

3. Speichern und veröffentlichen Sie alle Änderungen.

Wenn Sie Metadaten einer existierenden CA CMDB-Familie hinzufügen, werden Audit-Änderungen auf der Registerkarte "Versionskontrolle" richtig angezeigt. Wenn Sie Metadaten jedoch für eine neue Erweiterungstabelle definieren, muss es für Ihre Attribute eine neue Familie und Klasse geben. Weitere Informationen finden Sie unter [Hinzufügen einer neuen CA CMDB-Familie oder -Klasse](#) (siehe Seite 713).

Die Strukturen für Ihre neue Erweiterungstabelle sind jetzt eingerichtet. Fahren Sie mit [Definieren einer neuen CI-Familie](#) (siehe Seite 714) fort, um eine neue Familie für Ihre Attribute zu definieren.

Beispiel

In diesem Beispielszenario erstellen Sie die Familie **Automobil** und in dieser die Klasse **Limousine**, um den Bestand für die Fertigung, Lieferung, den Miettransport oder andere Zwecke zu verfolgen. Selbstverständlich könnten Sie auch viele andere Automobilklassen erstellen. Dieses Beispiel dient nur zur Veranschaulichung.

Schritt 1: Erstellen der neuen Erweiterungstabelle

1. Klicken Sie im Web Screen Painter-Schemadesigner auf "Erweiterungstabelle hinzufügen".
2. Geben Sie einen Namen für die neue Erweiterungstabelle ein. In diesem Beispiel ist dies **Fahrzeug**.

Die Erweiterungstabelle **zFahrzeug** wird erstellt, und ihre Eigenschaften werden angezeigt

Hinweis: "z" wird am Anfang aller neuen Tabellennamen hinzugefügt, um sie von den in der Anwendung vordefinierten Tabellen zu unterscheiden.

3. Legen Sie auf der Registerkarte "Tabelleninfo" für das Feld "Funktionsgruppe" **Bestand** fest. Andere Felder werden mit Standardwerten gefüllt.
4. Fügen Sie nach Belieben neue Spalten und Attributinformationen hinzu.
5. Speichern und veröffentlichen Sie die neue Erweiterungstabelle.

Schritt 2: Erstellen einer neuen Familie

So erstellen Sie eine Familie:

1. Navigieren Sie zur CI-Familienliste.
2. Klicken Sie auf "Neu erstellen".
Die Seite "Neue Configuration Item-Familie erstellen" wird angezeigt.
3. Geben Sie einen eindeutigen Namen für die neue Familie ein. In diesem Beispiel ist dies **Automobil**.
4. Überprüfen Sie, ob der Datensatzstatus auf "Aktiv" gesetzt ist.
5. Wählen Sie den Namen der Erweiterungstabelle aus. In diesem Beispiel ist dies **zFahrzeug**.
6. Klicken Sie auf "Speichern".

Die neue CI-Familie wird erstellt.

Schritt 3: Erstellen einer neuen Klasse

1. Navigieren Sie zur CI-Klassenliste.
2. Klicken Sie auf "Neu erstellen".
Die Seite "Neue Configuration Item-Klasse erstellen" wird angezeigt.
3. Geben Sie einen eindeutigen Namen für die neue Klasse ein. In diesem Beispiel ist dies **Limousine**.

4. Überprüfen Sie, ob der Datensatzstatus auf "Aktiv" gesetzt ist.
5. Wählen Sie die Familie aus. In diesem Beispiel ist dies **Automobil**.
6. Klicken Sie auf "Speichern".

Das neue CI-Klasse wird erstellt.

Schritt 4: Erstellen des neuen CI-Detailformulars

So erstellen Sie das CI-Detailformular:

1. Öffnen Sie im Visual Editor von Web Screen Painter das Formular "detail_extension.template".
2. Speichern Sie die Vorlage mit dem Namen **detail_zFahrzeug.htmlpl**.
Das neue Formular wird unter "NX_ROOT\site\mods\wsp\project\web\analyst" gespeichert
3. Ersetzen Sie im neuen Formular alle Instanzen von *****EXTENSION***** durch **zFahrzeug**
4. Speichern und veröffentlichen Sie das neue CI-Detailformular.

Schritt 5: Erstellen der Registerkarte "CA Attribute"

So erstellen Sie das Registerkartenformular "Attribute":

1. Öffnen Sie im Visual Editor von Web Screen Painter das Formular "nr_cmdb_extension_tab.template".
2. Speichern Sie die Vorlage mit dem Namen **nr_cmdb_zFahrzeug_tab.htmlpl**.
Das neue Formular wird unter "NX_ROOT\site\mods\wsp\project\web\analyst" gespeichert
3. Ersetzen Sie im neuen Formular alle Instanzen von *****EXTENSION***** durch **zFahrzeug**
4. Fügen Sie dem Formular nach Belieben Attribute hinzu.
5. Speichern und veröffentlichen Sie das neue Registerkartenformular "Attribute".

Schritt 6: Erstellen des Metadatenformulars

So erstellen Sie das Metadatenformular:

1. Öffnen Sie im Visual Editor von Web Screen Painter das Formular "cmdb_metadata_extension.template".
2. Speichern Sie die Vorlage mit dem Namen **cmdb_metadata_zFahrzeug.htmlpl**.
Das neue Formular wird unter "NX_ROOT\site\mods\wsp\project\web\analyst" gespeichert

3. Ersetzen Sie alle Instanzen von *****EXTENSION***** durch **zFahrzeug**.
4. Fügen Sie unter Verwendung der Überschriften- und Attributplatzhalter Metadaten für alle familienspezifischen Attribute hinzu.
5. Speichern und veröffentlichen Sie das neue Metadatenformular.

Configuration Audit and Control Facility (CACF)

Configuration Audit and Control Facility (CACF) vereinigt die drei Disziplinen Change Management, Configuration Management (CMDB) und Discovery Management, um sicherzustellen, dass Changes korrekt ausgeführt werden und keine nicht autorisierten Changes stattfinden.

Die Change-Verifizierung hilft dabei, sicherzustellen, dass die CMDB Änderungen akkurat widerspiegelt, und die Discovery-Management-Tools verifizieren die Änderungen.

Die Change-Verifizierung birgt folgende Vorteile:

Change Management

- Stellt sicher, dass autorisierte Changes richtig ausgeführt werden
- Erkennt falsch ausgeführte Changes
- Erkennt nicht autorisierte Änderungen
- Management-Berichte
- Komplettes Auditing aller Changes auf Attributebene
- Erkennt sich überschneidende oder im Konflikt stehende Changes

Configuration Management

- Die CMDB enthält eine genaue und aktuelle Darstellung aller verwalteten CIs
- Der zukünftige Zustand von CIs unter Berücksichtigung vorgeschlagener Change-Spezifikationen kann angezeigt werden
- Komplettes Auditing von CIs

CACF besteht aus zwei Hauptabschnitten, der CMDB-Verwaltungsoberfläche und der Change Management-Oberfläche. Im folgenden Abschnitt werden sie genauer beschrieben.

Weitere Informationen:

[CACF-Verwaltung und Richtliniendefinition](#) (siehe Seite 724)

[Verwaltete Attribute](#) (siehe Seite 740)

[Verwaltete Change-Zustände](#) (siehe Seite 740)

[Change-Spezifikationen](#) (siehe Seite 743)

[Ablauf der Change-Verifizierung](#) (siehe Seite 748)

[Archivieren und Bereinigen von Audit-Daten](#) (siehe Seite 754)

[Implementieren einer Change-Verifizierungsstrategie](#) (siehe Seite 755)

[Planen und Implementieren von Change-Verifizierung](#) (siehe Seite 759)

[Best Practices für Change-Verifizierung](#) (siehe Seite 766)

[Manuelles Verifizieren von aktualisierten Attributwerten](#) (siehe Seite 770)

[Beispiel: Rogue-Aktualisierungen nur von einer bestimmten Lokation erlauben](#) (siehe Seite 775)

[Beispiel: Durchführen eines Upgrade für Laptops in Ihrer Organisation](#) (siehe Seite 777)

[Beispiel: Sperren nicht verifizierter Changes](#) (siehe Seite 778)

[Beispiel: Erlauben einer CI-Aktualisierung, wenn kein übereinstimmender Change vorhanden ist](#) (siehe Seite 779)

[Beispiel: Verschieben aller Aktualisierungen aus CA Configuration Automation in den TWA](#) (siehe Seite 779)

[Beispiel: Richtlinienergebnisse zu Testzwecken nur ins Protokoll schreiben](#) (siehe Seite 780)

[Beispiel: Ablehnen einer CI-Aktualisierung](#) (siehe Seite 780)

[Beispiel: Erlauben von Changes ohne Spezifikationen](#) (siehe Seite 781)

[Beispiel: Verbieten von Changes ohne Spezifikationen](#) (siehe Seite 781)

[Beispiel: Erlauben von Rogue-Einfügungen aus ausgewählten Quellen](#) (siehe Seite 782)

[Beispiel: Erlauben einer Rogue-Aktualisierung für ein CI, dass nicht zur Produktion gehört](#) (siehe Seite 782)

CACF-Verwaltung und Richtliniendefinition

Der CMDB-Administrator definiert CIs und Attribute, die verwaltet werden, sowie die Richtlinie für das Aktualisieren dieser CIs und Attribute. CACF-Komponenten werden im Konfigurationssteuerungs-Knoten im CA CMDB-Abschnitt der Registerkarte "Verwaltung" verwaltet. Definition und Anzeige von CACF-Change-Spezifikationen können in "Change", "CI", über Incident-Formulare sowie im Knoten "Configuration Audit" auf der Registerkarte "Administration" durchgeführt werden.

Der Administrator ist dafür zuständig, die Erlaubnis von Standard-Changes zu evaluieren, obligatorische und vertrauenswürdige Datenquellen festzulegen und zu definieren, welche CIs und CI-Attribute über CACF verwaltet werden sollen. Wenn falsch ausgeführte Changes oder Rogue-Änderungen auftreten (auch als Abweichung bezeichnet), kann CA SDM den neuen Wert akzeptieren, einen Incident erstellen oder die Daten für eine spätere Verarbeitung in den Transaktionsarbeitsbereich (Transaction Work Area, TWA) kopieren. CA SDM kann diese Aktionen beliebig kombinieren.

Wichtig! Der Konfigurationsadministrator *muss* eine [Strategie für die Change-Verifizierung](#) (siehe Seite 755) für Ihre Umgebung festlegen. Die Standardrichtlinie für CACF erlaubt alle Änderungen an allen CIs, auch, wenn es sich um Rogue-Änderungen handelt oder für einen Change kein übereinstimmendes Ticket vorliegt.

Sie können Change-Verifizierungsrichtlinien dynamisch oder im Voraus geplant implementieren. Sie können diese Richtlinien sowohl generisch als auch hoch spezifisch gestalten. Die Change-Verifizierungsrichtlinie beschreibt, wie CA SDM auf die folgenden Events reagiert:

Aktualisierungen aus nicht autorisierten MDRs

Zeigt an, dass bestimmte MDRs für bestimmte Attribute autorisiert sind. Aktualisierungen von CI-Attributen aus nicht autorisierten MDRs können selektiv akzeptiert oder abgelehnt werden.

Sie können zum Beispiel Richtlinien definieren, um zu verhindern, dass [assign the value for acm in your book] die IP-Adresse eines CI aktualisiert, auch wenn ein übereinstimmender Change vorhanden ist. Erlauben Sie Aktualisierungen der IP-Adresse nur dann, wenn es sich beim Quell-MDR um Spectrum handelt.

Rogue-Änderungen

Entdeckt und verwaltet Aktualisierungen von CIs, wenn kein entsprechender Change vorhanden ist. Legen Sie eine Richtlinie zur Verwaltung von Rogue-Änderungen fest, die Hinzufügungen oder Aktualisierungen von CI-Daten erforderlich macht.

Sie können beispielsweise eine Richtlinie dafür definieren, dass bei Änderungen an CIs mit dem Namen "server*" in New York ohne übereinstimmenden Change das CI nicht geändert wird, sondern die Daten in den TWA geladen werden.

Falsch ausgeführte Changes

Erkennt, wenn Changes nicht richtig [implementiert](#) (siehe Seite 726) werden.

Audit-Funktionen ermöglichen es dem Configuration Manager, Änderungen an Richtlinien und CACF-Objektdefinitionen anzuzeigen. CACF protokolliert alle versuchten CI-Aktualisierungen unabhängig davon, sie erlaubt sind oder nicht. Dieses Protokoll hilft Ihnen dabei, zu entscheiden, welche Richtlinie eine Änderung an einem CI erlaubt oder nicht zugelassen hat.

Der Configuration Administrator definiert, in welchen Status Changes bearbeitbar sind und bei welchen es sich um Verifizierungsstatus handelt. Standardmäßig können Sie Change-Spezifikationen bearbeiten, wenn sich der Change im Status *RFC* befindet, und die Change-Verifizierung geschieht im Status *Verifizierung in Bearbeitung*. Optional können Änderungstickets automatisch höher gestuft oder geschlossen werden, sobald alle zugeordneten Change-Spezifikationen erfolgreich ausgeführt sind.

Wichtig! Möglicherweise tritt eine Herabsetzung der Leistung ein, wenn der Configuration Administrator die Option "Incident erstellen" mit mehr als einer aktiven Verifizierungsrichtlinie aktiviert.

Hinweis: Standardmäßig berücksichtigt CACF Aktualisierungen von Attributwerten für Changes mit aktiver Change-Verifizierung als Nicht-Rogue-Änderungen. Dies entspricht dem Status "Verifizierung in Bearbeitung". Der Configuration Administrator kann [dieses Verhalten ändern](#) (siehe Seite 740).

Weitere Informationen:

[Definieren von Change-Spezifikationen durch Change-Analysten](#) (siehe Seite 726)

[Change-Verifizierung](#) (siehe Seite 726)

[Verwendung von Change-Spezifikationen durch Change Manager](#) (siehe Seite 727)

[Funktionsweise der Configuration Audit and Control Facility](#) (siehe Seite 729)

Definieren von Change-Spezifikationen durch Change-Analysten

Der Change Management-Bereich der Benutzeroberfläche für Change-Verifizierungen ist mit dem Change-Ticketformular integriert. Change-Analysten erstellen normalerweise Change-Spezifikationen, wenn sie einen Change erstellen. Der Change-Analyst definiert die Änderung in Bezug auf das spezifische CI und CI-Attribut, die sie ändern möchten.

Der Change-Analyst kann die Change-Spezifikation mithilfe einer der folgenden Vorlagen beschreiben:

- Nehmen Sie exakte Eingaben für CI, CI-Attribut und Wert vor.

Beispiel: Die IP-Adresse für server1 ändert sich durch die Implementierung des Change in 10.10.10.10.

- Geben Sie CI-Attribut und Wert an, lassen Sie den CI-Namen aus.

Beispiels: Alle an den Change angefügten CIs ändern sich durch den Change in einen Speicherplatz von 8 GB.

- Geben Sie einen Attributwert an, der verwendet werden soll, wenn das Attribut nicht erkannt werden kann.

Beispiel: Nach dem Change befinden sich laut CMDB alle CIs in New York.

- Verwenden Sie den erkannten Wert.

Beispiel: Sie kennen die neue IP-Adresse vor dem Change nicht, wissen aber mit Sicherheit, dass die IP-Adresse geändert wird. Legen Sie die IP-Adresse des CI auf denselben Wert fest, den das maßgebliche MDR entdeckt.

Wenn der Change genehmigt ist, werden die Change-Spezifikationen als Teil desselben Genehmigungsprozesses genehmigt. Spätere Änderungen an der Spezifikation können verboten sein und werden vollständig überwacht.

Change-Verifizierung

Die Change-Verifizierung hilft dabei, sicherzustellen, dass Changes entsprechend Change-Spezifikationen ausgeführt werden. Die Verifizierung wird durchgeführt, wenn ein Change in einen Change Management-Zustand wie "Verifizierung in Bearbeitung" gelangt, sowie wenn CIs aktualisiert werden. Wenn Daten aus einem MDR oder über einen Import durch einen Web-Cient-Anwender in die CMDB gelangen, vergleicht CACF die eingehenden Attributdaten mit aktiven Change-Spezifikationen. Wenn die CI-Attributdaten übereinstimmen, verifiziert CACF den Change. Wenn die eingehenden Daten nicht mit den Change-Spezifikationen übereinstimmen, kann je nach Richtlinie durch Aktionen auf die Abweichung reagiert werden.

Ausgeführte Richtlinien können folgende Aktionen auslösen:

- Lehnt eine einzelne Attributaktualisierung der Transaktion ab.
- Lehnt die gesamte Transaktion einschließlich aller Attribut-Wertpaare ab.

- Lädt die ganze Transaktion in den TWA, um die Bearbeitung bis zum Abschluss der Genehmigung und Verifizierung der Transaktion aufzuschieben.
- Erstellt einen Incident, der die einzelnen Abweichungen beschreibt.

Hinweis: Diese Aktion kann vorhandene Benachrichtigungs- und Automatisierungsvorgänge auslösen. Um zu verhindern, dass mehrere Incidents erstellt werden, wird bei einer erkannten Rogue-Änderung ein einziger Incident für alle Rogue-Änderungen an einem CI erstellt.

- Akzeptiert die Transaktion bedingungslos, wenn Daten aus autorisierten Quell-MDRs akzeptiert werden.

Zum Beispiel kann der CMDB-Administrator eine Richtlinie definieren, die einen Incident erstellt, wenn ein Change an einem Produktionsserver falsch ausgeführt wird. Wenn importierte Daten aus einem nicht autorisierten MDR mit keiner ausstehenden Change-Spezifikation übereinstimmen, erstellt CACF einen Incident. Die Richtlinie kann eine CI-Aktualisierung mit den nicht übereinstimmenden Importdaten erlauben oder ablehnen. Außerdem haben Change Manager die Möglichkeit, den neu erkannten Wert zu akzeptieren, auch wenn der Wert nicht genau mit der geplanten Change-Spezifikation übereinstimmt.

Hinweis: Wenn während der Verifizierung der Change-Spezifikation mehrere Discoverys auftreten, können früher verifizierte Changes durch Discovery-Daten ungültig gemacht werden. Am Ende von Verifizierung ist das CI in dem Zustand, der allen Change-Spezifikationen entspricht.

Verwendung von Change-Spezifikationen durch Change Manager

Der Change Manager kann die folgenden Aktionen durchführen:

- Anzeigen und Ändern des Verifizierungsstatus der einzelnen Change-Spezifikationen.

Beispiel: Der Change Manager will wissen, welche Change-Spezifikationen für Change 12345, der sich im Status *Verifizierung ausstehend* befindet, noch ausstehend sind.

- Verwalten von Incidents für Rogue-Änderungen oder nicht ordnungsgemäß durchgeführte Changes.

Beispiel: Der Change Manager möchte verstehen, welche Changes nicht verifiziert werden konnten und welche Changes zusätzliche Untersuchungen benötigen.

- Verwalten von Changes, die manuelles Eingreifen benötigen.

Beispiel: Ein Change erfordert die manuelle Verifizierung eines nicht auffindbaren Change, und der Change-Analyst muss die Aufgabe ausführen.

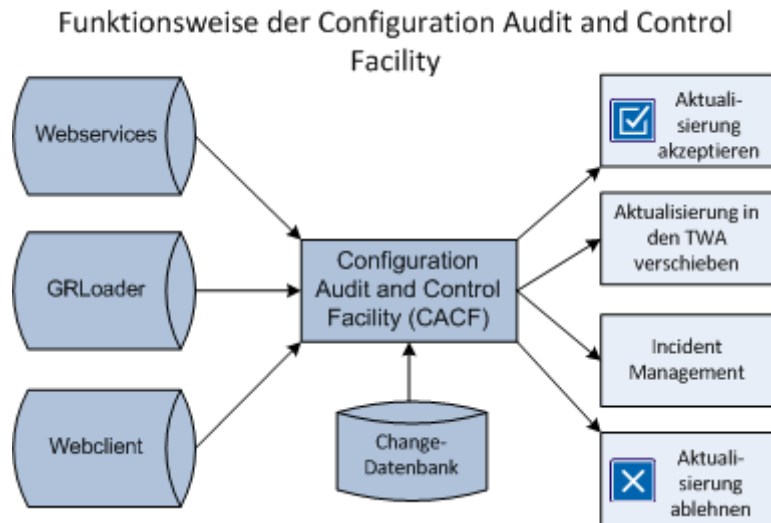
Beispiel: Der Change Manager untersucht Change 12345 und entscheidet, dass zehn verschiedene Change-Spezifikationen für ihn vorliegen. Aufgrund eines Tippfehlers war Change-Spezifikation Nummer 9 falsch und kann abgebrochen werden.

Durch Audit-Funktionen können Änderungen am Change-Status durch aktualisierte und überschriebene Change-Spezifikationen angezeigt werden. Das Scoreboard zeigt den Status des ausgeführten Systems sowie außerordentliche Bedingungen, die Eingriffe oder Untersuchungen erforderlich machen, an. CA Business Intelligence-Berichte ermöglichen eine längerfristige Ansicht der Effizienz von Configuration Manager-Richtlinien, um den Zustand Ihrer Umgebung zu überwachen.

Funktionsweise der Configuration Audit and Control Facility

Die CACF-Funktion steuert eingehende CI-Daten, bevor sie in die CMDB geladen werden. Diese Verifizierung hilft dabei, sicherzustellen, dass alle angeforderten Changes richtig ausgeführt werden, und entdeckt und verwaltet Rogue-Änderungen automatisch. Der Configuration Administrator (CMDB-Administrator) definiert Verifizierungsrichtlinien, um zu bestimmen, wie CA SDM antwortet, wenn eine Abweichung vom angeforderten Change auftritt.

Das folgende Diagramm veranschaulicht, wie CACF arbeitet:



1. Eingehende CI-Daten werden von Webservices, GRLoader, MDR, oder der Webanwenderoberfläche geladen, um eine Attributaktualisierung für ein CI in der CMDB anzufordern.
2. Basierend auf den von Ihrem Configuration Administrator eingerichteten Verifizierungsrichtlinien führt CACF eine oder mehrere der folgenden Aktionen durch:
 - CACF akzeptiert die Aktualisierung und ändert die CI-Daten in der CMDB.
 - CACF verschiebt die Aktualisierung zur späteren Weiterverarbeitung in den TWA.
Beispiel: Ihr Change Manager verarbeitet Transaktionen im TWA.
 - CACF erstellt einen Incident und lässt Sie das Ticket verwalten.
Beispiel: Ihr Incident-Management-Prozess erfordert, dass der Incident für Berichterstellungszwecke verwaltet wird.
 - CACF lehnt die Aktualisierung ab, und die CI-Daten werden in der Datenbank nicht geändert.

Verifizierungsrichtlinie

Nachdem Configuration Manager und Change Manager sich auf eine Change-Verifizierungsrichtlinie geeinigt haben, werden diese Entscheidungen in Form einer CA SDM-Change-Verifizierungsrichtlinie festgehalten. Ein System kann mehrere Verifizierungsrichtlinien haben. Wenn eine CI-Aktualisierung eintritt, wählt CACF eine einzelne Verifizierungsrichtlinie für jedes aktualisierte Attribut aus, und diese Richtlinie kann zur Folge haben, dass das CI aktualisiert wird. Wenn eine entsprechende Change-Spezifikation vorliegt, kann auch ein TWA-Eintrag oder ein Incident erstellt werden.

Hinweis: Wenn Sie Aktualisierungen durch den Web-Client überwachen wollen, geben Sie das MDR-Klassenmuster als **Web-Client** (Groß-/Kleinschreibung beachten) in der Verifizierungsrichtlinie an. Die Verwendung dieses Musters gilt für englische und lokalisierte CA SDM-Versionen, wenn Sie Aktualisierungen über den Web-Client überwachen wollen.

Wichtig! Das Festlegen der notwendigen Richtlinien für Ihre Umgebung erfordert eine umfassende Auseinandersetzung mit den Zielen der Organisation und der Art und Weise, wie die Richtlinien umgesetzt werden sollen.

Auswahl der Verifizierungsrichtlinien

Wenn ein CI aktualisiert wird, wählt CACF für jedes aktualisierte Attribut eine Richtlinie aus. Die getroffene Auswahl hängt von der Quelle der Aktualisierung, dem Ziel-CI sowie davon, ob eine übereinstimmende Change-Spezifikation vorhanden ist, ab. Wenn mehrere Richtlinien übereinstimmen, wählt CACF die Richtlinie mit der niedrigsten Sequenznummer aus, um die Attributaktualisierung zu verwalten.

Hinweis: CACF kann mehrere Richtlinien auswählen, um eine einzelne Transaktion zu verwalten, durch die mehrere Attribute aktualisiert werden. Zum Beispiel kann die Aktualisierung eines CI mit einer neuen Beschreibung und einer neuen IP-Adresse zwei unterschiedliche Richtlinien auslösen.

Jede Richtlinie hat vier Abschnitte, die CACF für die Richtlinienauswahl verwendet:

Identifizierung und Priorität

Identifiziert eine Richtlinie und gibt die Reihenfolge für die Auswertung der Richtlinie an.

Change-Ausrichtung

Wählt Transaktionen basierend auf der engsten Übereinstimmung der Attributaktualisierung mit einer vorhandenen Change-Spezifikation aus.

Transaktionsfilter

Gibt die Datenquellen an, für die diese Richtlinie gilt.

CI-Filter

Gibt die CIs an, für die diese Richtlinie gilt.

Eine Richtlinie stimmt mit einer Attributaktualisierung überein, wenn alle Filter zutreffen. Wenn eine Richtlinie mit keiner Transaktion übereinstimmt, überspringt CACF die Richtlinie und wertet andere Richtlinien im System aus. Wenn CACF alle Richtlinien überspringt, wird die CI-Attributaktualisierung standardmäßig erlaubt.

Verifizierungsrichtlinien-Filtersyntax

Um das Festlegen generischer Richtlinien zu erleichtern, werden in Change-Ausrichtungs-, Transaktions- und CI-Filtern Sternchen als Platzhalter für das letzte Zeichen im Muster akzeptiert. Verwenden Sie ein Ausrufezeichen am Anfang dieser Filter, um sie zu negieren.

Wichtig! Richtlinienmusterregeln unterscheiden sich von Regeln für geplante Change-Spezifikationswerte. Für Richtlinienfilter können Sie keine eingebetteten Sternchen (*) oder Sonderzeichen "Größer gleich" (>) und "Kleiner gleich" (<) verwenden.

Bei der Auswahl von Richtlinienfiltern muss Groß- und Kleinschreibung auch dann beachtet werden, wenn für die gesuchten Attribute festgelegt ist, dass Groß- und Kleinschreibung nicht beachtet werden muss.

Hinweis: Ein leerer Richtlinienfilter (ohne Wertangabe im Feld) findet nur leere Werte, während ein Richtlinienfilter mit einem Sternchen mit allen Werten übereinstimmt.

Beachten Sie die folgenden Informationen mit den folgenden Beispielverifizierungsrichtlinien:

- Richtlinie1 entspricht den CIs name(prod*) attribute(IP-Adresse), wenn eine übereinstimmende Change-Spezifikation vorhanden ist.
- Richtlinie2 entspricht den CIs name(prod*) attribute(IP-Adresse), wenn eine Rogue-Aktualisierung vorhanden ist.
- Richtlinie3 entspricht den CIs name(test*) attribute(Installierter Speicher) aus mdr(Cohesion).
- Richtlinie4 entspricht den CIs name("") attribute(Installierter Speicher).

Die folgende Liste beschreibt die möglichen Ergebnisse dieser Richtlinien:

- Wenn eine Aktualisierung an CI(test2) attribute(Installierter Speicher) auftritt, verwaltet Richtlinie3 die Aktualisierung. CACF ignoriert Richtlinie1 und Richtlinie2.
- Wenn eine Aktualisierung an CI(prod3) attribute(Installierter Speicher) auftritt und eine übereinstimmende Change-Spezifikation vorhanden ist, verwaltet Richtlinie1 die Aktualisierung.
- Wenn eine Aktualisierung an CI(development4) attribute(IP-Adresse) auftritt, aktualisiert CACF das CI mit der neuen IP-Adresse, da keine übereinstimmende Richtlinie vorhanden ist.
- Wenn eine Aktualisierung an CI(prod1) attribute(Festplattenkapazität) auftritt, aktualisiert CACF das CI mit dem neuen Wert, da keine Richtlinie für attribute(Festplattenkapazität) vorhanden ist. In diesem Beispiel verwaltet CACF das Festplattenkapazitätsattribut *nicht*.
- Richtlinie4 stimmt nur mit CIs mit leeren Namen überein. Weil leere CI-Namen ungültig sind, wird der Change nie ausgeführt.

Verifizierungsrichtlinien-Priorität nach Sequenznummer

Wenn mehrere Richtlinien mit einer Attributaktualisierung übereinstimmen, wählt CACF die Richtlinie mit der niedrigsten Sequenznummer aus. Berücksichtigen Sie die folgenden Richtlinien und ihre Sequenznummern.

- Richtlinie name(Richtlinie1) sequence(1000) CI(prod*)
- Richtlinie name(Richtlinie2) sequence(2000) CI(prod-NY*)

Wenn eine Aktualisierung an CI(prod1) auftritt, verwaltet Richtlinie1 die Transaktion.
Wenn eine Aktualisierung an CI(prod-NY-1) auftritt, verwaltet ebenfalls Richtlinie1 die Transaktion, da sie eine niedrigere Sequenznummer hat. In diesem Beispiel tritt Richtlinie2 niemals in Kraft.

Wir empfehlen, dass Sie die Sequenznummern so ändern, dass die spezifischste Richtlinie die niedrigste Sequenznummer hat. Beachten Sie dazu die folgenden Beispielrichtlinien:

- Richtlinie name(Richtlinie1) sequence(2000) CI(prod*)
- Richtlinie name(Richtlinie2) sequence(1000) CI(prod-NY*)

Wenn eine Aktualisierung an CI(prod1) auftritt, verwaltet Richtlinie1 die Transaktion.
Wenn eine Aktualisierung an CI(prod-NY-1) auftritt, verwaltet Richtlinie2 die Transaktion, da sie eine niedrigere Sequenznummer hat.

Change-Ausrichtung

Richtlinien filtern, wie eng eine CI-Attributaktualisierung mit einer Change-Spezifikation übereinstimmt. Nach einer CI-Aktualisierung sucht CACF nach einer Change-Spezifikation, die sowohl mit dem CI als auch mit dem Attributnamen übereinstimmt. Durch diese Suche kann die Change-Spezifikation überprüft werden. Diese Change-Ausrichtung kann folgendermaßen auftreten:

- Für Attribut und CI sind Change-Spezifikationen vorhanden.
- Für das CI sind Change-Spezifikationen vorhanden, die *keine* Change-Spezifikationen enthalten.
- Eine Rogue-Einfügungstransaktion tritt auf, die auf ein neues CI verweist. Es ist *kein* Change mit dem daran angefügten CI vorhanden.
- Eine Rogue-Aktualisierungstransaktion tritt auf, die auf ein vorhandenes CI verweist. Es ist kein Change mit dem daran angefügten CI vorhanden.

Nur Changes in einem Change-Zustand mit *aktivierter Change-Verifizierung* werden berücksichtigt, wenn nach einem übereinstimmenden Change gesucht wird. Geschlossen, nicht genehmigte, ungeplante oder andere nicht ausgeführte Changes werden nicht berücksichtigt, wenn nach einem übereinstimmenden Change gesucht wird.

Nachdem die CACF-Funktion die Change-Ausrichtung einer Transaktion bestimmt hat, führt sie eine Suche nach einer entsprechenden Richtlinie aus. Eine Richtlinie kann einen mehr Change-Ausrichtungstypen verwalten:

Change mit Spezifikationen

Zeigt an, dass ein Change mit einer Change-Spezifikation, die das Aktualisierungs-CI und den Attributnamen angibt, vorhanden ist.

Changes ohne Spezifikationen

Zeigt Changes mit dem angegebenen aktualisierten CI ohne vorhandene Change-Spezifikationen an.

Rogue-Einfügung

Zeigt ein eingefügtes CI an, für das kein übereinstimmender Change in einem Verifizierungszustand vorhanden ist.

Wichtig! Richtlinien zum Verhindern von Rogue-Einfügungen müssen ein verwaltetes Attribut der Art *Name* oder *Alle Verwalteten Attribute* haben (wobei *Name* für ein aktives verwaltetes Attribut steht).

Die CACF-Funktion erlaubt Rogue-Einfügungen und -Aktualisierungen, wenn eine Transaktion nur nicht verwaltete Attribute hat.

Rogue-Aktualisierung

Zeigt ein aktualisiertes CI an, das keine übereinstimmenden Changes in einem Verifizierungszustand hat.

Weitere Informationen:

[Beispiel: Erlauben von Changes ohne Spezifikationen](#) (siehe Seite 781)

[Verhindern von Rogue-Änderungen am Attribut](#) (siehe Seite 764)

Beispiel: Richtlinien für Change-Ausrichtung

Die folgenden Beispielrichtlinien spezifizieren Change-Ausrichtungen:

- Richtlinie name(legacy) filtert nach CI(*) attribute(Jedes beliebige verwaltete Attribut) alignment(Changes ohne Spezifikationen) action(Attributaktualisierung zulassen)
- Richtlinie name(new) filtert nach CI(*) attribute(Jedes beliebige verwaltete Attribut) alignment(Changes mit Spezifikationen) action(Aktualisierung nur zulassen, falls sie mit der Change-Spezifikation übereinstimmt)
- Richtlinie name(no-rogue) filtert nach CI(*) attribute(Jedes beliebige verwaltete Attribut) alignment(Rogue-Einfügung oder Rogue-Aktualisierung) action(Immer gesamte Transaktion abbrechen, Incident erstellen)

Diese Beispiele ermöglichen die folgende Funktionalität:

- Richtlinie (legacy) erlaubt es CA SDM r12.6-Changes ohne Change-Spezifikationen, das CI wie vor der CACF-Implementierung zu aktualisieren.
- Richtlinie (new) erzwingt die Change-Verifizierung für alle neuen Changes mit übereinstimmenden Change-Spezifikationen.
- Richtlinie (no-rogue) verhindert Aktualisierungen an CIs, wenn keine Changes in einem Zustand mit aktiver Verifizierung vorhanden sind.

Transaktionsfilter

Richtlinien filtern Transaktionen basierend auf der Quelle der Transaktion einschließlich [Attributname, MDR-Name, MDR-Klasse und Rolle](#) (siehe Seite 731) des Anwenders, der die Aktualisierung ausführt.

Hinweis: Wenn Sie ausschließlich nach Anwendern filtern möchten, die sich über die Webanwenderoberfläche angemeldet haben, geben Sie das Schlüsselwort **Web-Client** für die MDR-Klasse an. Die Anwender-ID des Kontakts gibt den MDR-Namen an. Diese Methode zum Identifizieren von Anwendern gilt nur für Verifizierungsrichtlinien und wird in keinem anderen Teil des Produkts angezeigt.

Beispiel: Transaktionsfilter

Die folgenden Beispielrichtlinien geben Transaktionsfilter an:

- Richtlinie name(root_access) filtert nach ci(*) attribute(Alle verwalteten Attribute) role(Administrator) action(Attributaktualisierung zulassen)
- Richtlinie name(cohesion_not_authorized) filtert nach ci(*) attribute(IP-Adresse) MDRclass(Cohesion) action(Alten Attributwert beibehalten)
- Richtlinie name(john) filtert nach ci(user1*) attribute(Alle verwalteten Attribute) MDRName(user1) MDRClass(Web-Client) action(Attributaktualisierung zulassen)

Diese Beispiele ermöglichen die folgende Funktionalität:

- Richtlinie (root_access) erlaubt es Anwendern mit Administratorzugriff, alle Werte zu aktualisieren. Wir empfehlen für diesen Richtlinientyp eine niedrige Sequenznummer.
- Richtlinie (cohesion_not_authorized) verhindert, dass die IP-Adresse des gefilterten CI aus einem MDR oder MDR class(Cohesion) aktualisiert wird. Dieses Beispiel veranschaulicht, wie Aktualisierungen aus einem nicht autorisierten MDR verhindert werden können.
- Richtlinie (user1) lässt user1 die CIs aktualisieren, die er besitzt, allerdings nur unter Verwendung des Webclient. Dieses Beispiel zeigt, wie bestimmte Anwender volle Kontrolle über ihre Daten erhalten können.

CI-Filter

Die Richtlinie filtert Transaktionen nach den Eigenschaften des aktualisierten CI. Dieser Auswahlkriterien umfassen CI-Name, Klasse, Priorität, Servicetyp und Lokation.

Wichtig! Der CI-Filter basiert auf dem Attributwert des CI vor der Aktualisierung und nicht auf dem Wert der eingehenden Transaktionsdaten.

Beispiel: CI-Filterrichtlinien

Die folgenden Beispielrichtlinien geben CI-Filter an:

- Richtlinie name(priority1) filtert nach Servicetyp (priority1-Lösung) action(Aktualisierung nur zulassen, falls sie mit der Change-Spezifikation übereinstimmt, Incident erstellen)
- Richtlinie name(prod-NY) filtert nach ci(prod*) location(NY) attribute(Alle verwalteten Attribute) action(Aktualisierung nur zulassen, falls sie mit der Change-Spezifikation übereinstimmt)
- Richtlinie name(prod-not-NY) filtert nach ci(prod*) location(!NY) attribute(Alle verwalteten Attribute) action(Attributaktualisierung zulassen)

Diese Beispiele ermöglichen die folgende Funktionalität:

- Richtlinie (priority1) erfordert, dass für CIs mit einem Servicetyp von *priority1-Lösung* ein übereinstimmender Change vorhanden ist. Diese Richtlinie ist eine Best Practice, da sie dabei hilft, die wichtigsten CIs in der CMDB genau zu steuern. Diese Richtlinie erfordert, dass alle durch Change Management verwaltete Changes Spezifikationen haben und verifiziert werden müssen, um fertiggestellt zu werden.
- Richtlinie (prod-NY) erfordert, dass für CIs in NY übereinstimmende Changes vorhanden sind. Durch das Filtern von Richtlinien nach Lokationen können Changes nacheinander auf Standortbasis verifiziert werden.
- Richtlinie (prod-not-NY) gibt durch das Ausrufezeichen im Lokationsmuster an, dass sich das CI nicht in NY befindet.

Richtlinienaktionen

Nachdem CACF eine Richtlinie ausgewählt hat, bestimmt der Aktionsabschnitt der Richtlinie das Ergebnis der Attributaktualisierung. Dieser Abschnitt identifiziert den wichtigsten Teil der Verifizierungsrichtlinie, da er Auswirkungen auf die Integrität der CMDB hat. Dieser Abschnitt wirkt sich auch auf den Change Management-Workflow, dazugehörige Benachrichtigungen und erstellte Incidents aus.

Eine Richtlinie kann eines der folgenden Aktualisierungs-Verhalten haben:

Aktualisierung nur zulassen, falls sie mit der Change-Spezifikation übereinstimmt

Diese Einstellung wendet die Aktualisierung des eingehenden Attributs bedingt auf das CI an, wenn sie mit einer Change-Spezifikation übereinstimmt. Diese Aktualisierung tritt auf, wenn sich der Change in einem Zustand mit aktivierter Verifizierung befindet. Die Auswahl dieser Option löst die Change-Verifizierung aus.

Attributaktualisierung zulassen

Wendet die eingehende Attributaktualisierung bedingungslos auf das CI an. Diese Option deaktiviert sämtliche Change-Verifizierungen. Verwenden Sie dieses Verhalten für Standard-Changes mit vertrauenswürdigen, autorisierten Datenquellen ohne Notwendigkeit eines Change Order.

Immer gesamte Transaktion abbrechen

Bricht die Aktualisierung und sämtliche Attributaktualisierungen in dieser Transaktion ab, auch wenn eine übereinstimmende Change-Spezifikation vorhanden ist. Verwenden Sie dieses Verhalten, um unbefugte Aktualisierungen von CIs aus nicht autorisierten MDRs zu verhindern. Wenn eine Richtlinie eine Transaktion abbricht, wird die gesamte Transaktion auch dann abgebrochen, wenn andere Richtlinien den Change erlaubt hätten.

Wählen Sie dieses Verhalten beispielsweise, um eine nicht autorisierte MDR davon anzuhalten, ein CI einzufügen. Geben Sie zusätzlich einen gebräuchlichen Attributnamen wie z. B. *Name* an.

Alten Attributwert beibehalten

Bricht die einzelne Attributaktualisierung ab, erlaubt jedoch die Aktualisierung anderer Attribute in der Transaktion, wenn dies durch die entsprechenden Richtlinien erlaubt ist. Verwenden Sie dieses Verhalten, wenn ein MDR auf Attributebene nicht autorisiert ist.

Eine Verifizierungsrichtlinie kann angeben, dass Incidents automatisch geschlossen werden, wenn fehlgeschlagene Verifizierungen behoben werden. Die Richtlinie kann festlegen, dass die eingehenden Transaktionsdaten in den TWA kopiert werden. Dieser Richtlinientyp ist nützlich, wenn Daten aus einem nicht autorisierten MDR überprüft werden müssen, bevor die CMDB aktualisiert wird.

Damit der Configuration Manager die CACF-Richtlinien identifizieren kann, die die Erstellung des TWA-Datensatzes ausgelöst haben, erhält das Feld "Change" im TWA den Namen der Richtlinie, durch die es erstellt wurde. Das Kopieren von Daten in den TWA ist unabhängig von Aktualisierungen des CI in der CMDB. Richtlinien können zur Folge haben, dass CI aktualisiert werden, in den TWA gelangen, oder beides.

Richtlinienplanung

Sie können Aktivierungs- und Deaktivierungsdaten für Verifizierungsrichtlinien angeben, sodass der Configuration Administrator unbeaufsichtigte Richtlinienänderungen planen kann.

Mehrere Richtlinien

Je mehr Verifizierungsrichtlinien in Ihre Umgebung aufgenommen und je mehr Attribute verwaltet werden, desto komplexer wird es, die Richtlinien zu organisieren, da sie sich in zunehmendem Maße überschneiden. Zum Beispiel könne Sie eine Richtlinie für Server-CIs und eine weitere Richtlinie für CIs in New York haben. Sie müssen entscheiden, welche Richtlinie für Server-CIs in New York gelten soll. Verwenden Sie die Sequenznummern der Richtlinien, um den Vorrang einer bestimmten Richtlinie zu erzwingen, wenn potenziell mehrere Richtlinien auf ein Attribut zutreffen könnten. Je mehr Attribute Sie verwalten, desto größer wird die Möglichkeit, dass mehrere Richtlinien eine einzelne Transaktion verwalten.

Berücksichtigen Sie die folgenden Informationen, wenn mehrere aktive Richtlinien für eine einzelne Transaktion vorliegen:

- Wenn eine der ausgewählten Richtlinien das Kopieren von Daten in den TWA erfordert, so wird dies durchgeführt.
- Wenn eine der ausgewählten Richtlinien erfordert, dass die Transaktion abgebrochen wird, bricht CACF die Transaktion komplett ab.

Wichtig! Einrichtungen, die den createAsset-Webservice verwenden (einschließlich GRLoader und CMDDBf) gliedern die Transaktion in drei getrennte Transaktionen, zwei Einfügungen und eine Aktualisierung. Aktualisierungen von `ca_owned_resource` können erlaubt sein, während Aktualisierungen an der CI-Erweiterungstabelle abgebrochen werden. Aktualisierungen von CI-familien-spezifischen Attributen in der Erweiterungstabelle werden möglicherweise nicht als nicht als Einfügungen sondern als Aktualisierungen erkannt.

Beispiel: Mehrere Richtlinien

In den folgenden Beispiele werden mehrere Richtlinien angegeben:

- Richtlinie name(IP-Adresse) attribute(IP-Adresse) action(Attributaktualisierung zulassen)
- Richtlinie name(Installierter Speicher) attribute(Installierter Speicher) action(Transaktion abbrechen)
- Richtlinie name(Festplattenkapazität) attribute(Festplattenkapazität) action(Alten Attributwert beibehalten)

Diese Beispiele ermöglichen die folgende Funktionalität:

- Wenn durch eine Transaktion nur die IP-Adresse aktualisiert wird, wird diese Aktualisierung ausgeführt.
- Wenn durch eine Transaktion nur der installierte Speicher aktualisiert wird, wird diese Aktualisierung nicht ausgeführt.
- Wenn durch eine Transaktion sowohl IP-Adresse als auch installierter Speicher aktualisiert werden, wird die Transaktion auf der Webanwenderoberfläche abgebrochen.
- Wenn durch eine Transaktion sowohl IP-Adresse als auch Festplattenkapazität auf der Webanwenderoberfläche aktualisiert werden, wird die IP-Adresse aktualisiert, die Festplattenkapazität jedoch nicht.
- Wenn durch eine Transaktion sowohl IP-Adresse als auch installierter Speicher auf der Webanwenderoberfläche aktualisiert werden, wird kein Attribut aktualisiert.

Incident-Konsolidierung

Wenn eine Verifizierungsrichtlinie die Erstellung eines Incident erfordert, kann CACF die Anzahl von offenen Incidents folgendermaßen reduzieren:

- CACF erstellt bei Rogue-Änderungen jeweils nur einen offenen Incident für ein CI. Wenn weitere Rogue-Änderungen eintreten, wird derselbe offene Incident aktualisiert.
- CACF erstellt bei fehlgeschlagenen Change-Verifizierungen jeweils nur einen offenen Incident. Wenn weitere Fehler bei der Change-Verifizierungen auftreten, wird derselbe offene Incident aktualisiert.

Verwaltete Attribute

Verwaltete Attribute zeigen die geeigneten CI-Attribute für die Change-Verifizierung durch CACF an. Standardmäßig enthält diese Liste *CI-Name* und *Alle verwalteten Attribute*. Sie fügen CI-Attribute hinzu, die als Bestandteil Ihrer Change-Verifizierungsstrategie verwaltet werden sollen. Definieren Sie verwaltete Attribute als Teil Ihrer Change-Verifizierungsstrategie im Knoten "Konfigurationssteuerung", "Verwaltete Attribute" im CA CMDB-Abschnitt der Registerkarte "Administration".

CACF berücksichtigt nicht verwaltete Attribute (d. h. nicht aufgelistete Attribute) nicht bei der Change-Verifizierung. Diese nicht verwalteten Attribute werden wie üblich aktualisiert.

Wichtig! Die Change-Verifizierung ignoriert nicht verwaltete Attribute und erlaubt, dass CIs mit ihnen aktualisiert werden, außer, wenn in einer Verifizierungsrichtlinie das Verhalten "Immer gesamte Transaktion abbrechen" angegeben ist.

Hinweis: Groß- und Kleinschreibung muss in der Definition von verwalteten Attributen nur beachtet werden, wenn CACF den geplanten Wert der Change-Spezifikation mit den eingehenden CI-Transaktionsdaten vergleicht. Bei Auswahlmustern in der Richtlinie muss Groß- und Kleinschreibung immer beachtet werden.

Im *technischen CA CMDB-Referenzhandbuch* finden Sie eine Liste der CI-Attributnamen.

Verwaltete Change-Zustände

CACF verwendet verwaltete Change-Zustände, um anzuzeigen, welche Change-Status durch CACF verwaltet werden. CACF verwendet verwaltete Change-Zustände, um zu steuern, wie oder wann Change-Verifizierung für im System vorgenommene CI-Aktualisierungen angewendet werden soll. Sie können diese Change-Zustände an die Bedürfnisse Ihrer Organisation anpassen.

Sie konfigurieren verwaltete Change-Zustände auf der Registerkarte "Administration" im Knoten "CA CMDB", "Konfigurationssteuerung", "Verwaltete Change-Zustände" ändern.

Hinweis: CACF ignoriert Changes in Change-Zuständen, die in der Liste der verwalteten Change-Zustände enthalten sind.

In der folgenden Liste werden die Optionen für verwaltete Change-Zustände beschrieben:

Change-Spezifikationen bearbeitbar

Gibt an, ob Sie die Change-Spezifikationen für einen Change bearbeiten können. Nachdem ein Change Request genehmigt wurde, können Sie ihn normalerweise nicht mehr ändern, und die möglichen Aktualisierungen werden auf wenige Überschreibungsoptionen im Zustand *Verifizierung in Bearbeitung* reduziert.

Change-Verifizierung aktiv

Gibt an, ob Änderungen, die für ein CI entdeckt, während sich der Change in diesem Status befindet, bei der Change-Verifizierung berücksichtigt werden. Changes und die dazugehörigen Change-Spezifikationen werden mit eingehenden Transaktionen verglichen, um zu überprüfen, ob sie erfolgreich ausgeführt wurden.

CACF überwacht alle CIs nach Änderungen an den verwalteten Attributwerten. Im Zuge der Verifizierung der einzelnen Änderungen am CI auf Attributebene am CI führt CACF einen Vergleich mit einer Liste von Change-Spezifikationen durch, die sich in einem Zustand mit *aktiver Change-Verifizierung* befinden.

Wenn eine Change-Spezifikation in einen solchen Zustand gelangt, werden sämtliche Change-Spezifikationen ohne spezifische CIs erweitert. Diese Erweiterung tritt ein, wenn neue Change-Spezifikationen mithilfe der Liste von an den Change angefügten CIs erstellt werden.

Wenn eine Change-Spezifikation aus diesem Zustand entfernt wird, wird die Liste von Change-Spezifikationen mit Status der Art *Festlegen, nachdem Change ausgeführt wurde* abgeschlossen. Diese Aktion aktualisiert das CI mit den geplanten Werten, die in den Change-Spezifikation angegeben sind.

Implementierungsstatus

Gibt an, ob der Zustand als Zustand behandelt wird, wenn die Änderungen für das CI ausgeführt oder implementiert werden. Wenn ein Change in diesen Übergangszustand gelangt, sind die Attributwerte im CI veränderbar und können gemäß der Anforderungen der ausstehenden Change-Spezifikationen aktualisiert werden. CACF kann diese Änderungen nicht als Rogue-Änderungen behandeln, sie aber auch nicht für die endgültige Verifizierung verwenden. Normalerweise sollte der Prozess der Change-Verifizierung die eingehenden Attributdaten erst dann vergleichen, wenn der Change vollständig ausgeführt wurde.

Schaltflächen zum Überschreiben von Change-Spezifikationen anzeigen

Gibt an, ob und auf welcher Ebene der Change-Analyst Change-Spezifikationen steuern kann. In manchen Implementierungen kann der Change-Analyst Change-Spezifikationen nach Bedarf bearbeiten, in anderen kann er sie [überschreiben](#) (siehe Seite 752) oder [abbrechen](#) (siehe Seite 753).

Change nach Verifizierung hochstufen

Gibt an, ob ein Change automatisch in den nächsten Standardzustand höhergestuft wird, wenn CACF alle Change-Spezifikationen verifiziert hat.

Standardmäßig verwaltete Change-Zustände

Sie können Change-Zustände definieren, in denen Change-Spezifikationen erstellt, überschrieben, verifiziert oder ignoriert werden.

In der folgenden Listen werden als Beispiel die standardmäßig verwalteten Change-Zustände von CA SDM beschrieben:

RFC

Definiert Change-Spezifikationen für diesen Zustand, wird bei der Change-Verifizierung allerdings nicht betrachtet. Änderungen am CI, die erkannt werden, während sich der Change in diesem Zustand befindet, werden normalerweise als Rogue-Änderungen betrachtet.

Genehmigung in Bearbeitung

Change-Spezifikationen in diesem Zustand haben die gleichen Merkmale wie RFC. Sie sind bearbeitbar und werden in der Verifizierung nicht berücksichtigt.

Nach der Change-Genehmigung werden die Change-Spezifikationen als Teil des Genehmigungsprozesses genehmigt. CACF verbietet zusätzliche Änderungen an der Spezifikation und führt eine vollständige Überwachung durch.

Implementierung in Bearbeitung

Änderungen an CIs können eintreten, werden aber weder als Rogue-Änderungen behandelt noch zur Verifizierung verwendet. Sie können die Definition dieses Change-Zustands ändern, damit Changes in diesem Zustand verifiziert werden.

Verifizierung in Bearbeitung

Change-Spezifikationen können nicht bearbeitet werden, doch Analysten können sie überschreiben. In diesem Zustand ist die [Change-Verifizierung aktiv](#) (siehe Seite 748).

Change-Spezifikationen

Ein Change enthält Change-Spezifikationen, die die spezifischen CI-Änderungen definieren, die für ein CI angefordert werden. CACF verwendet diese Change-Spezifikationen, wenn der Change in einen Verifizierungszustand gelangt, um zu prüfen und zu bestätigen, dass die Änderungen am CI richtig durchgeführt wurden. Sie können Change-Spezifikationen direkt in Changes und CIs oder im Knoten "Konfigurationssteuerung", "Change-Spezifikation" im CA CMDB-Abschnitt der Registerkarte "Administration" erstellen.

Die Change-Spezifikation besteht aus folgenden Hauptabschnitten:

Change-Nummer

Gibt den Change an, der die Änderung erforderlich macht.

CI Name

Enthält den Namen des CI, das Sie aktualisieren möchten.

Sie können das Feld "CI-Name" leer lassen, um zu implizieren, dass sich die Change-Spezifikation auf alle für den Change definierten CIs bezieht. Verwenden Sie diese Option, wenn alle CIs eines Change dasselbe verwaltete Attribut und denselben geplanten Wert verwenden. Die Change-Spezifikation bezieht sich auf alle CIs, die an den Change angehängt sind, wenn der Change-Status in einen verwalteten Change-Zustand mit aktiver Change-Verifizierung gelangt. Dies wird als "Erweiterung" bezeichnet.

Attributname

Gibt den Namen des verwalteten Attributs an, den Sie aktualisieren möchten.

Wenn "Alle verwalteten Attribute" ausgewählt ist, können sich alle verwalteten Attribute während der Verifizierung des Change ändern. Da Sie in diesem Fall mehrere Attribute aktualisieren können, können Sie keinen Planwert angeben.

Planwert

Zeigt den erwarteten Attributwert nach der Änderung an. Wenn der Change in einen Verifizierungszustand gelangt und das CI über die Webanwenderoberfläche, GRLoader oder Webservices aktualisiert wird, vergleicht CACF den geplanten Wert mit den eingehenden Daten, um eine Übereinstimmung finden.

[Sonderzeichen](#) (siehe Seite 744) können in den geplanten Wert eingebettet werden, wenn der genaue Wert unbekannt ist.

Status

Gibt den [Status der Change-Spezifikation](#) (siehe Seite 750), beispielsweise "Verifizierung ausstehend" an.

Wenn Sie den geplanten Wert nicht im Voraus kennen, jedoch wissen, dass er sich ändern kann, können Sie den Status der Change-Spezifikation auf "Erkannten Wert verwenden" festlegen. Dieses Verhalten erfordert, dass Discovery das CI aktualisiert, bevor CACF die Change-Spezifikation als validiert erachtet. Sie benötigen dieses Verhalten für Nummernfelder und SREs, die keine Sternchen als geplanten Wert akzeptieren.

Um Ihnen dabei zu helfen, den geplanten Wert festzulegen, werden auf der Registerkarte "Verlauf erkannter Attribute" alle Werte, die vor Kurzem durch ein MDR entdeckt wurden, einschließlich der Information, ob sie autorisiert oder in die CMDB geladen wurden, aufgelistet. Diese Registerkarte enthält Informationen zu Format, zu berücksichtigender Groß- und Kleinschreibung usw., damit Sie ein passendes Muster für den geplanten Wert festlegen können.

Weitere Informationen:

[Sonderzeichen](#) (siehe Seite 744)

[Definieren von Richtlinien für Massenladungsvorgänge](#) (siehe Seite 746)

[Definieren von Massenänderungen](#) (siehe Seite 746)

[CI-Versionskontrolle und zukünftiger Zustand](#) (siehe Seite 747)

Sonderzeichen

Sie können Sonderzeichen einbetten, wenn Sie den genauen Wert nicht kennen. Verwenden Sie das Sternchen für die Übereinstimmung mit einer beliebigen Anzahl von Zeichen. Das Muster *muss* mit den erkannten Daten in derselben Sequenz übereinstimmen. Leerzeichen haben eine Bedeutung als solche.

Geben Sie zum Beispiel *10.*.** als Planwert ein, um IP-Adressen zu finden, die mit *10* beginnen und zwei Punkte enthalten, die auf einen beliebigen Wert zwischen den Punkten folgen.

Beispiel: Der eingehende Wert für *server_type* enthält Windows 2003 (WIN32) 5.2.Service Pack 2 (Build 3790) Intel x86. Um diesen Wert zu überprüfen, geben Sie in der Change-Spezifikation als geplanten Wert **Service Pack 2** an.

Ein Wort am Anfang des Planwerts bedeutet, dass der erkannte Wert mit diesem Wert beginnen muss. Ein Sternchen am Anfang Planwerts bedeutet, dass der erkannte Wert mit einem beliebigen Wert anfangen kann und mit dem Wert enden muss, der auf das Sternchen folgt.

Die folgende Tabelle enthält Beispiele für die Verwendung des Asterisk:

Planwert	Erkannter Wert	Übereinstimmung oder keine Übereinstimmung
a	b	Keine Übereinstimmung

Planwert	Erkannter Wert	Übereinstimmung oder keine Übereinstimmung
a	a	Übereinstimmung
a	aba	Übereinstimmung
a	bab	Übereinstimmung
a*	a	Übereinstimmung
a*	ab	Übereinstimmung
a*	ba	Keine Übereinstimmung
*a	a	Übereinstimmung
*a	ab	Keine Übereinstimmung
*a	ba	Übereinstimmung

Ein Muster, das mit einem Ausrufezeichen anfängt, resultiert in der Negation des Werts. Sie können das Ausrufezeichen nur als das erste Zeichen im Muster verwenden. Zum Beispiel können Sie 10.!*. *.* nicht als Muster verwenden

Um numerische Werte in Zeichenfolgen zu vergleichen, verwenden Sie "Größer als" (>) oder "Kleiner als" (<) als erstes Zeichen im Planwert. Bei einem vorangestelltes Ausrufezeichen muss es das zweite Zeichen sein.

Wichtig! CACF ignoriert voran- oder nachgestellte nichtnumerische Werte in den Mustern für erkannte und geplante Werte.

Die folgende Tabelle enthält Beispiele zur Verwendung von Ausrufezeichen und den "Größer als"- und "Kleiner als"-Zeichen.

Planwert	Erkannter Wert	Übereinstimmung oder keine Übereinstimmung
>200	aaa 201 bbb	Übereinstimmung
>200GB	aaa 200 bbb	Keine Übereinstimmung
>200GB	300 GB	Übereinstimmung
!<200GB	200 Byte	Übereinstimmung
!<200	200 Bit	Übereinstimmung

Wenn Sie den geplanten Wert nicht im Voraus kennen, jedoch wissen, dass er sich ändern kann, können Sie den Status der Change-Spezifikation auf "Erkannten Wert verwenden" festlegen. Dieses Verhalten erfordert, dass Discovery das CI aktualisiert, bevor CACF die Change-Spezifikation als validiert erachtet. Sie benötigen dieses Verhalten für Nummernfelder und SREs, die keine Sternchen als geplanten Wert akzeptieren.

Um Ihnen dabei zu helfen, den geplanten Wert festzulegen, werden auf der Registerkarte "Verlauf erkannter Attribute" alle Werte, die vor Kurzem durch ein MDR entdeckt wurden, einschließlich der Information, ob sie autorisiert oder in die CMDB geladen wurden, aufgelistet. Diese Registerkarte enthält Informationen zu Format, zu berücksichtigender Groß- und Kleinschreibung usw., damit Sie ein passendes Muster für den geplanten Wert festlegen können.

Definieren von Richtlinien für Massenladungsvorgänge

Das Verwalten neuer CIs ohne vorhergehender Erstellung eines Change, der die Definition dieser CIs erfordert, stellt in CMDB-Umgebungen ein Problem dar. Berücksichtigen Sie die folgenden Informationen, wenn Sie eine große Anzahl von CIs definieren.

- Definieren Sie eine spezielle, nach Anwender-ID, MDR oder Rolle eingeschränkte Richtlinie für Massenladungsvorgänge, damit Rogue-Einfügungen erfolgreich abgeschlossen werden können.
- Definieren Sie eine spezielle Richtlinie für Massenladungsvorgänge, die alle neuen CIs zur Verifizierung und späteren Verarbeitung in den TWA umleitet. Für diese Aktion muss die an erster Stelle beschriebene spezielle Richtlinie für Massenladungsvorgänge ebenfalls vorhanden sein.

Definieren von Massenänderungen

Das Erstellen von identischen Änderungen an mehreren CIs, beispielsweise, um den Standort für eine Gruppe von CIs zu ändern, erfordert die folgenden Schritte:

1. Erstellen Sie einen Change.
2. Definieren Sie eine einzelne Change-Spezifikation, die die Änderung beschreibt, und lassen Sie den CI-Namen leer.
3. Fügen Sie alle CIs an den Change an.

Wenn Sie die genauen Details eines Change vor der Implementierung nicht kennen (z. B. wenn Sie einen neuen Server kaufen und nur den CI-Namen kennen), führen Sie die folgenden Schritte durch:

1. Erstellen Sie einen Change.
2. Erstellen Sie eine Change-Spezifikation mit "Alle verwalteten Attribute" als Attributname.
3. Lassen Sie den Planwert leer, da er unbekannt ist.

4. Bringen Sie das Ticket durch den Change Management-Prozess.
5. Wenn sich der Change in einem Zustand mit aktivierter Verifizierung befindet und Discovery ausgeführt wird, werden die eingehenden CI-Daten ins CI geladen (sofern dies von der Richtlinie erlaubt wird).
6. Wenn sämtliche Discoverys für das CI abgeschlossen sind, muss der Change Manager die Change-Spezifikation als manuell überprüft markieren.

Folgen Sie diesen Schritten, wenn es viele verschiedene Änderungen an vielen CIs gibt. Zum Beispiel wenn eine Sammlung von Servern von einem Speicherort zu einem anderen verschoben wird, und jedem eine eindeutige IP-Adresse zugewiesen wird.

1. Erstellen von Changes
2. Erstellen Sie eine Kalkulationstabelle und listen Change-Nummer, CI und neuen Attributwert jeweils in einer Zeile auf. Jede Zeile resultiert in einer eigenen Change-Spezifikation.
3. Laden Sie die Kalkulationstabelle mit GRLoader, um die erforderlichen Change-Spezifikationen zu erstellen.
4. Stufen Sie den Change und seine Change-Spezifikationen wie üblich höher.

Hinweis: Weitere Informationen zur Verwendung von GRLoader finden Sie im *technischen CA CMDB-Referenzhandbuch*.

CI-Versionskontrolle und zukünftiger Zustand

Zeigen Sie Change-Spezifikationen in der Registerkarte "Versionskontrolle" des 'CI-Detailformulars an, um weitere Informationen anzugeben und den Change samt dazugehöriger Change-Spezifikationen zu identifizieren. Auf dieser Registerkarte wird auch der Zustand des CI nach Anwendung der Änderungen angezeigt. Zeigen Sie Snapshots des CI wie zum geplanten Datum des Change an. Wenn der Change noch nicht geplant worden ist, wird er als ungeplanter Change angezeigt.

Versionskontrolle ermöglicht folgende Funktionen:

- Identifizieren Sie schnell und einfach sich überschneidende oder miteinander im Konflikt stehende Change-Spezifikationen.
- Gelangen Sie beim Programmstart direkt zur Change-Spezifikation und zeigen Sie die entsprechenden Change-Details an, indem Sie in der Detailansicht auf die Verknüpfung "Change" in der Spalte "MDR" klicken.
- Snapshots mit *Ungeplanten Changes* veranschaulichen Changes, die für einen nicht spezifizierte Zeitpunkt in der Zukunft geplant sind.
- Die Change-Nummer der Change-Spezifikationen wird jeweils rechts in der Snapshot-Beschriftung angezeigt.

- Ein Informationstext im unteren Bereich zeigt folgende Informationen zur Change-Spezifikation als Hover-Text an:
 - Change-Nummer
 - Datum der geplanten Änderung, wenn der Change ein Plandatum enthält
 - Datum für "Benötigt am" (sofern für den Change eines angegeben wurde).

Ablauf der Change-Verifizierung

Wenn ein Anwender die Speicherung eines CI anfordert, sucht CA SDM nach anwendbaren Change-Spezifikationen. Die folgenden Informationen beschreiben eine anwendbare Change-Spezifikation:

- Das CI in der Change-Spezifikation ist identisch mit jenem, das gespeichert wird.
- Der Change befindet sich in einem verwalteten Change-Zustand mit aktiver Change-Verifizierung.
- Das Attribut in der Change-Spezifikation ist identisch mit dem Attribut, das aktualisiert wird.
- Die Change-Spezifikation ist aktiv.
- Wenn keine verwalteten Attribute aktualisiert werden und keine anwendbare Richtlinie vorliegt, findet die Speicherung uneingeschränkt statt.

Wenn die eingehenden Datenwerte mit einer Change-Spezifikation genau übereinstimmen, betrachtet CACF die Change-Spezifikation als validiert. Je nach Richtlinie können durch die Verifizierung Incidents geschlossen werden, die durch die Change-Verifizierung erstellt wurden.

Die Verifizierung findet statt, wenn das CI mit Informationen aus Web-Clients, Webservices oder GRLoader aktualisiert wird, während der Change und alle zugrunde liegenden Change-Spezifikationen verifiziert werden. Wenn alle Verifizierungen für einen Change abgeschlossen sind, kann der Change optional automatisch in den nächsten Change-Zustand hochgestuft werden.

Wenn die eingehenden Datenwerte nicht mit den Werten in der Change-Spezifikation übereinstimmen, wird es als ein falsch implementierter oder fehlgeschlagener Change betrachtet. Je nach Richtlinie werden Incidents neu erstellt oder an bestehende angehängt.

Zum Beispiel findet CA SDM keine anwendbaren Change-Spezifikationen, doch es sind Changes in einem *Zustand mit aktiver Change-Verifizierung* vorhanden. Diese Changes geben das Ziel-CI an und haben keine Change-Spezifikationen. CACF verwaltet diese Changes durch Richtlinien für die Verarbeitung von *Changes ohne Spezifikationen*.

- Wenn keine anwendbaren Change-Spezifikationen oder Changes ohne Spezifikationen vorhanden sind, wird die Speicherung als Rogue-Vorgang betrachtet.
- Wenn alle Attribute bearbeitet sind, werden Richtlinien ausgelöst, die festlegen, dass die eingehenden Daten in den TWA kopiert werden müssen.

Weitere Informationen:

[Verwalten von Change-Spezifikationen](#) (siehe Seite 749)

[Change-Spezifikations-Status](#) (siehe Seite 750)

[Verwalten von fehlgeschlagenen Verifizierungen](#) (siehe Seite 752)

[Verwalten von nicht erkennbaren Attributen](#) (siehe Seite 753)

Verwalten von Change-Spezifikationen

Wenn ein Change ausgeführt oder implementiert wurde, gelangt er in einen Change-Zustand, der von CACF verwaltet wird und für den *Aktive Change-Verifizierung* festgelegt ist. Wenn sich der Change in diesem Zustand befindet, überprüft CACF alle verwandten CI-Aktivitäten und aktualisiert das Scoreboard mit dem Status des einzelnen Change-Spezifikationen.

Das Scoreboard wird vom Change Manager verwendet, um zu überprüfen, ob die erforderlichen Changes richtig ausgeführt wurden, sowie um manuelle Verifizierungen auszuführen, die durch Changes erforderlich sind.

Sobald alle Verifizierungen für einen Change abgeschlossen sind, kann der Change optional automatisch in den nächsten weiter Change-Zustand gestuft werden (normalerweise "Geschlossen"). Dadurch werden alle Change-Spezifikationen automatisch als inaktiv markiert.

Change-Spezifikations-Status

Change-Spezifikationen verwenden Status, um den Typ der durchzuführenden Verifizierung und den aktuellen Verifizierungszustand anzuzeigen. Die Statuswerte werden auch im Verifizierungsprotokoll verwendet, wenn Change-Verifizierungsvorgänge festgehalten werden, die während des Verifizierungsprozesses aufgetreten sind.

Anfangsstatus

Sie werden bei der Erstellung von Change-Spezifikationen verwendet, um den Typ der Verifizierung anzugeben, die CACF durchführen muss. Diese Status sind nicht endgültig, und der Change wird nicht als verifiziert betrachtet, wenn Change-Spezifikationen in einem dieser Status vorhanden sind.

Verifizierung ausstehend: Die Change-Spezifikation wurde nicht verifiziert, oder die CI-Aktualisierung ist ausstehend.

Macht manuelle Verifizierung erforderlich: Nachdem die Änderungen für einen Change verifiziert sind, wird eine manuelle Verifizierung erforderlich.

Erkannten Wert verwenden: Der erkannte Wert wird zum Zeitpunkt der Verifizierung ins CI kopiert und vor der Verifizierung verwendet, wenn der geplante Wert nicht bekannt wird.

Festlegen, nachdem Change ausgeführt wurde: Setzt ein CI-Attribut auf den geplanten Wert, wenn die Verifizierung abgeschlossen ist. Verwenden Sie diesen Status, um CI-Attribute festzulegen, wenn das Attribut nicht gefunden werden kann. Setzen Sie zum Beispiel den Hauptkontakt des CI auf "User1", wenn eine Änderung abgeschlossen ist.

Endstatus

Zeigt eine abgeschlossene Change-Spezifikation an und wird als endgültiger Status betrachtet. Wenn alle Change-Spezifikationen in einen dieser Endzustände gelangen, können die Changes in den nächsten Standardzustand hochgestuft werden.

Verifiziert: Die Change-Spezifikation wurde erfolgreich überprüft.

Wurde manuell verifiziert: Die Change-Spezifikation wurde manuell verifiziert.

Erkannten Wert verwendet: Das CI wurde mit dem erkannten Wert aktualisiert.

Wurde auf geplanten Wert festgelegt: Das CI wurde nach der Change-Verifizierung mit dem erkannten Wert aktualisiert.

Geplanter Wert akzeptiert: Das CI wurde mit dem geplanten Wert aktualisiert und während der Verifizierung überschrieben.

Erkannter Wert akzeptiert: Das CI wurde mit dem zuletzt erkannten Wert aktualisiert und während der Verifizierung überschrieben.

Kein Change: Der Geplante Wert hat zum Zeitpunkt der Verifizierung mit dem CI übereingestimmt, und es war keine Verifizierung erforderlich.

Abbrechen: Die Change-Spezifikation wurde vom Change Manager [abgebrochen](#) (siehe Seite 752).

Eingriffsstatus

Zeigt an, dass eine Change-Spezifikation für die Verifizierung manuelles Eingreifen benötigt. CA SDM hebt diese Status auf Listenformularen rot hervor. Diese Status sind nicht endgültig, und der Change wird nicht als verifiziert betrachtet, wenn Change-Spezifikationen in einem dieser Status vorhanden sind.

Verifizierung fehlgeschlagen: Discovery hat erkannt, dass der Wert nicht mit jenem übereinstimmt, der im Change angegeben wurde. Der Change-Analyst muss entscheiden, ob die Änderung richtig ausgeführt wurde und der Change falsch festgelegt wurde, oder ob die Angaben zum Change richtig sind und die Änderung erneut verifiziert werden muss. Je nach der Definition des verwalteten Change-Zustands und dem aktuellen Change-Status kann der Change-Analyst die fehlgeschlagene Change-Spezifikation überschreiben, ändern oder abbrechen.

Manuelle Verifizierung aktiv: Manuelle Verifizierung ist erforderlich, damit die Change-Spezifikation als endgültig markiert werden kann.

Aktionsüberschreibungsstatus

Zeigt eine Aktion an, die während der Change-Verifizierung initiiert werden muss. Diese Status sind nicht endgültig, und der Change wird nicht als verifiziert betrachtet, wenn Change-Spezifikationen in einem dieser Status vorhanden sind.

Geplanten Wert akzeptieren: Macht erforderlich, dass das CI-Attribut mit dem geplanten Wert überschrieben wird.

Erkannten Wert akzeptieren: Macht erforderlich, dass das CI-Attribut mit dem erkannten Wert überschrieben wird.

Berichterstellungsstatus

Zeigt das Ergebnis von Richtlinienvorgängen an, die im Verifizierungsprotokoll zu Protokollierungszwecken enthalten sind und nicht von Change-Spezifikationen verwendet werden.

Aktualisierung wurde zugelassen: Eine Richtlinie hat einem Request erlaubt, ein CI zu aktualisieren, und hat mit keinen Change-Spezifikationen übereingestimmt.

Verwalten von fehlgeschlagenen Verifizierungen

Wenn eine Verifizierung fehlgeschlagen hat, wird auf dem Scoreboard-Knoten "CMDB", "Configuration Audit", "Verifizierung fehlgeschlagen" die Anzahl von fehlgeschlagenen Verifizierungen und Change-Spezifikationen, die manuelle Eingriffe benötigen, rot angezeigt. Die Change-Spezifikationen können auch auf den Registerkarten "Change", "CI" oder "Administration" unter "Change-Spezifikationen" mit dem Status "Verifizierung fehlgeschlagen" angezeigt werden. Wenn eine Verifizierung fehlschlägt, kann der Change-Analyst eingreifen oder die nächste Discovery abwarten.

Wenn der verwaltete Change-Zustand die Aktion "Schaltflächen zum Überschreiben von Change-Spezifikationen anzeigen" zulässt, kann der Change-Analyst die Change-Spezifikation öffnen, die Daten überprüfen und auf eine der folgenden Optionen klicken, um die Verifizierung durch das Verschieben in einen Endzustand zu schließen:

Erkannten Wert akzeptieren

Der Analyst entscheidet, dass die Change-Spezifikation falsch ist und das Discovery-Tool den richtigen Wert entdeckt hat.

Geplanten Wert akzeptieren

Der Analyst entscheidet, dass das Discovery-Tool eine falsche oder keine Discovery durchgeführt hat und dass der geplante Wert so akzeptiert werden soll, als ob er ordnungsgemäß entdeckt worden sei.

Abbrechen

Dieser Teil des Change wurde nicht ausgeführt, und die Spezifikation wurde abgebrochen.

Verwalten von nicht erkennbaren Attributen

Wenn eine Change-Spezifikation manuelle Verifizierung benötigt, muss der Konfigurationsanalyst den Change manuell verifizieren. Auf dem Scoreboard-Knoten "CMDB", "Configuration Audit", "Manueller Eingriff" wird die Anzahl von Change-Spezifikationen, die manuelles Eingreifen benötigen, rot angezeigt. Die Change-Spezifikationen können auch auf den Registerkarten "Change", "CI" oder "Administration" unter "Change-Spezifikationen" mit dem Status "Manuelle Verifizierung aktiv" angezeigt werden.

Wenn der verwaltete Change-Zustand die Aktion "Schaltflächen zum Überschreiben von Change-Spezifikationen anzeigen" zulässt, kann der Change-Analyst die Change-Spezifikation öffnen, die Daten überprüfen und auf eine der folgenden Optionen klicken, um die Verifizierung durch das Verschieben in einen Endzustand zu schließen:

Als verifiziert markieren

Wird verwendet, wenn das Attribut nicht gefunden wird und manuell verifiziert wird.

Abbrechen

Dieser Teil des Change wurde nicht ausgeführt, und die Spezifikation wurde abgebrochen.

Archivieren und Bereinigen von Audit-Daten

Wir empfehlen, dass Sie veraltete Einträge im Verifizierungsprotokoll, dem CACF-Audit-Verlauf dem und CI-Audit-Verlauf als Teil Ihrer periodischen Datenbankwartung archivieren und bereinigen.

Wichtig! Die CA Business Intelligence-Berichte für CACF enthalten normalerweise monatliche Berichte sowie eine Jahreszusammenfassung. Die Standardzeit für Bereinigungsregeln für Protokoll, CACF-Audit-Verlauf und CI-Audit-Verlaufstabellen beträgt 30 Tage. Verwenden in Archivierungs- und Bereinigungsregeln denselben Wert, um dabei zu helfen, die Konsistenz der Daten in Verifizierungsprotokolleinträgen, Incidents und Changes zu gewähren. Sie können den Standardwert von 30 Tagen in einen Wert umändern, der besser zu Ihren Berichterstellungsanforderungen passt.

Führen Sie die folgenden Aktionen durch, um Audit-Daten zu archivieren und zu bereinigen:

1. Verwenden Sie die aktuelle Incident-Regel, um inaktive Incidents, die älter als *nn*Tage sind, zu bereinigen.

CA SDM archiviert und bereinigt Verifizierungsprotokolleinträge erst, wenn die dazugehörigen Incidents archiviert und bereinigt wurden. Wenn Sie einen Change zu einem Incident zuordnen, überprüft CA SDM nicht, ob der Change aktiv ist.

2. Verwenden Sie die aktuelle Change-Regel, um inaktive Changes, die älter als *nn*Tage sind, zu bereinigen.

CA SDM archiviert und bereinigt Verifizierungsprotokolleinträge und Change-Spezifikationen erst, wenn die dazugehörigen Changes archiviert und bereinigt wurden. Wenn Sie einen Incident zu einem Change zugeordnet haben, archiviert und bereinigt CA SDM den Change nicht.

3. Verwenden Sie die Regel "Protokoll der Verifizierungen von Rogue-Änderungen" für Rogue-Änderungen, die nicht zu einer Incident-Erstellung geführt haben.

Verwenden Sie diese Regel, um Verifizierungsprotokolleinträge, die älter als *nn*Tage sind, zu archivieren und zu bereinigen. Definitionsgemäß sind Rogue-Änderungen nicht zu Changes zugeordnet.

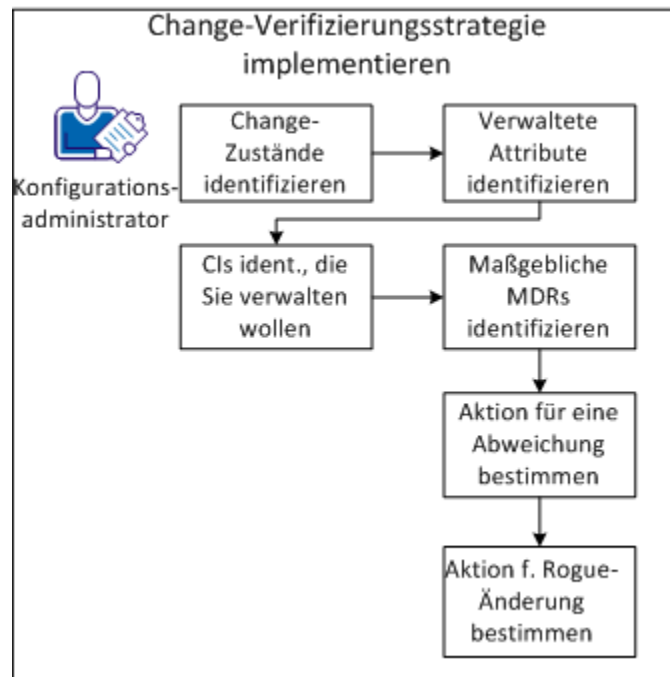
4. Verwenden Sie die Regel "CMDB-Audit", um Informationen, die auf den Registerkarten "Verlauf der Change-Spezifikationen", "Verifizierungsrichtlinien-Verlauf", "Verlauf des verwalteten Change-Zustands" und "Verlauf des verwalteten Attributs" in den entsprechenden Detailformularen angezeigt werden. CA SDM speichert diese Informationen in der ci_audit-Tabelle.

Implementieren einer Change-Verifizierungsstrategie

Der Configuration Administrator entscheidet, wie aggressiv die Change-Verifizierungsstrategie für Ihre CMDB-Umgebung implementiert werden soll. Sie identifizieren Bereiche Ihres Change-Management-Prozesses, die eine Change-Verifizierungsstrategie benötigen. Diese Bereiche umfassen Attribute mit Versionskontrolle, Change-Status mit aktiver Change-Verifizierung, veränderbare Change-Spezifikationen und autorisierte MDRs.

Beispiel: Sie wollen, dass das IP-Adressattribut nur aus MDR1 aktualisiert werden kann. Sie können auch die Aktionen bestimmen, die durchgeführt werden, wenn CACF eine Abweichung oder Rogue-Änderung entdeckt.

Das folgende Diagramm erklärt, wie eine Change-Verifizierungsstrategie durch Konfigurationsverwaltung implementiert wird:



1. [Identifizieren der Change-Zustände](#) (siehe Seite 756).
2. [Identifizieren der verwalteten Attribute](#) (siehe Seite 756).
3. [Identifizieren der zu verwaltenden CLs](#) (siehe Seite 757).
4. [Identifizieren der autorisierten MDRs](#) (siehe Seite 758).
5. [Festlegen der Aktion bei Abweichungen](#) (siehe Seite 758).
6. [Festlegen der Aktion bei Rogue-Änderungen](#) (siehe Seite 759).

Identifizieren der Change-Zustände.

Der Configuration Administrator identifiziert die Change-Zustände, für die nach einer durchgeführten Änderung Change-Verifizierung für das CI zum Einsatz kommt. Change-Zustände helfen Ihnen dabei, spezifische Bedingungen festzulegen, beispielsweise, ob Sie Change-Spezifikationen in einem bestimmten Zustand bearbeiten können. Beispiel: Sie möchten den RFC-Zustand für Changes überprüfen, die Aktualisierungen an CIs erforderlich machen.

Gehen Sie wie folgt vor:

1. Klicken Sie auf der Registerkarte "Administration" auf "CA CMDB", "Konfigurationssteuerung", "Verwaltete Change-Zustände".
2. Klicken Sie auf "RFC", um die Details des Change-Zustands anzuzeigen oder einen Change-Zustand zu erstellen, der noch nicht definiert wurde.

Hinweis: Standardmäßig können Sie im RFC-Change-Zustand nur Change-Spezifikationen bearbeiten. Im Zustand "Implementierung in Bearbeitung" können Sie Change-Spezifikationen nicht bearbeiten. Der Zustand "Verifizierung in Bearbeitung" aktiviert die Change-Verifizierung und zeigt die Überschreibungsschaltflächen, für den Change Manager sowie andere autorisierte Anwender an.

3. Geben Sie die CACF-Optionen und das Verhalten dafür an, wenn ein Change in diesen Zustand gelangt.
4. Klicken Sie auf "Speichern".

Identifizieren der verwalteten Attribute

Bestimmen Sie, welche CI-Attribute Sie für die Change-Verifizierungsstrategie verwalten wollen. Beispiel: Sie wollen Sie das Attribut der IP-Adresse (alarm_id) Attribut mit Change-Verifizierung verwalten.

Gehen Sie wie folgt vor:

1. Klicken Sie auf der Registerkarte "Administration" auf "CA CMDB", "Konfigurationssteuerung", "Verwaltete Attribute".
2. Klicken Sie auf "Neu erstellen".
3. Führen Sie die folgenden Schritte aus:
 - a. Geben Sie **alarm_id** als Attributname ein
 - b. Geben Sie **IP-Adresse** als Attributbeschriftung ein.

- c. Wählen aus der Drop-down-Liste einen anfänglichen Verifizierungsstatus aus.
Standard: Verifizierung ausstehend
- d. (Optional) Aktivieren Sie die Option "Groß- /Kleinschreibung beachten", wenn Sie erzwingen möchten, dass beim Vergleich der Planwerte der Change-Spezifikation Groß- und Kleinschreibung berücksichtigt werden muss.
Standard: Deaktiviert
- e. Klicken Sie auf "Speichern".

Identifizieren der zu verwaltenden CIs

Identifizieren Sie die CIs, die Sie mit einer Verifizierungsrichtlinie verwalten wollen.
Beispiel: Sie möchten die IP-Adresse (alarm_id) für alle CIs mit hoher Priorität, deren Name NY_Server beginnt, verwalten.

Gehen Sie wie folgt vor:

1. Klicken Sie auf der Registerkarte "Administration" auf "CA CMDB", "Konfigurationssteuerung", "Verifizierungsrichtlinien".
2. Klicken Sie auf "Neu erstellen".
3. Führen Sie die folgenden Schritte aus:
 - a. Geben Sie eine Sequenz ein, beispielsweise **100**.
 - b. Geben **NY Server IP Addresses** als Richtliniennamen ein.
 - c. Aktivieren Sie die entsprechenden Change-Ausrichtungsoptionen.
Beispiel: Sie wollen, dass die Verifizierungsrichtlinie für alle Optionen außer "Changes ohne Spezifikationen" gilt.
4. Führen Sie die folgenden Schritte durch, um die Transaktions- und CI-Filter festzulegen:
 - a. Wählen Sie aus der Drop-down-Liste "Verwaltetes Attribut" "IP-Adresse" aus.
 - b. Geben Sie ein Rollenmuster ein, oder behalten Sie das Sternchen bei, um alle Rollen auszuwählen.
 - c. Geben Sie **NY** als Lokationsmuster ein.
 - d. Geben Sie **NY_Server*** als CI-Namensmuster ein.
Dieser Filter verifiziert CIs namens NY_Server1, NY_Server2 usw.
5. Wählen Sie in der Drop-down-Liste "Aktualisierungsverhalten" *Aktualisierung nur zulassen, falls sie mit der Change-Spezifikation übereinstimmt*.
6. (Optional) Verwenden Sie den Modus "Nur Protokoll", wenn Sie mit der Richtlinie experimentieren möchten und die Ergebnisse nur im standardmäßigen Protokoll angezeigt werden sollen, ohne sich auf die aktive CMDB-Umgebung auszuwirken.
7. Klicken Sie auf "Speichern".

Identifizieren der autorisierten MDRs

Identifizieren Sie die autorisierten MDRs in Ihrer CMDB-Umgebung. Beispiel: Sie möchten Aktualisierungen an CIs aus CA Configuration Automation, als MDR1 identifiziert, zulassen. Sie erachten Aktualisierungen von Webservices, die Sie als MDR2 identifiziert haben, als nicht autorisiert, und möchten solche Requests in den TWA senden.

Gehen Sie wie folgt vor:

1. Öffnen Sie die Richtlinie "NY Server IP Addresses", und klicken Sie auf "Bearbeiten".
2. Geben Sie **MDR1** als MDR-Namensmuster ein.
Hinweis: Wenn Sie ein MDR namens "MDR2" ausschließen "MDR1", "MDR3" usw. jedoch zulassen möchten, geben Sie **!MDR2** als Muster ein.
3. Erstellen Sie eine separate Verifizierungsrichtlinie, beispielsweise "MDR2 NY Server".
4. Geben Sie dieselben Informationen wie in der vorherigen Richtlinie ein, unter Ausnahmen der folgenden Felder:
 - a. Geben Sie **MDR2** als MDR-Namensmuster ein.
 - b. Wählen Sie *Immer gesamte Transaktion abbrechen* als Aktualisierungsverhalten.
 - c. Wählen Sie in der Drop-down-Liste "Daten in TWA schreiben" "Immer" aus.
5. Klicken Sie auf "Speichern".

Festlegen der Aktion bei Abweichungen

Legen Sie die Aktion bei Abweichungen fest. Beispiel: Eine Änderung an einem CI stimmt nicht mit den im Change angegebenen Werten überein. Sie wollen, dass die Verifizierungsrichtlinie einen Incident für die Abweichung erstellt.

Gehen Sie wie folgt vor:

1. Öffnen Sie die von Ihnen erstellte Richtlinie "MDR2 NY Server", und klicken Sie auf "Bearbeiten".
2. Wählen Sie in der Drop-down-Liste "Incident erstellen" "Ja" aus, und weisen Sie eine Vorlage zu.
3. Klicken Sie auf "Speichern".
4. Ein Endanwender erstellt einen Change mit einer Change-Spezifikation zum Aktualisieren eines CI aus MDR2.
5. CACF erstellt einen Incident, wenn MDR2 eine CI-Aktualisierung mit einem Wert anfordert, der nicht mit dem geplanten Wert in der im Change definierten Change-Spezifikation übereinstimmt.

Festlegen der Aktion bei Rogue-Änderungen

Legen Sie die Aktion bei Rogue-Änderungen fest. Zum Beispiel erkennt CACF eine Änderung an einem CI, das Change-Spezifikationen aus aktiven Changes hat. Der Configuration Administrator möchte solche Requests ablehnen.

Gehen Sie wie folgt vor:

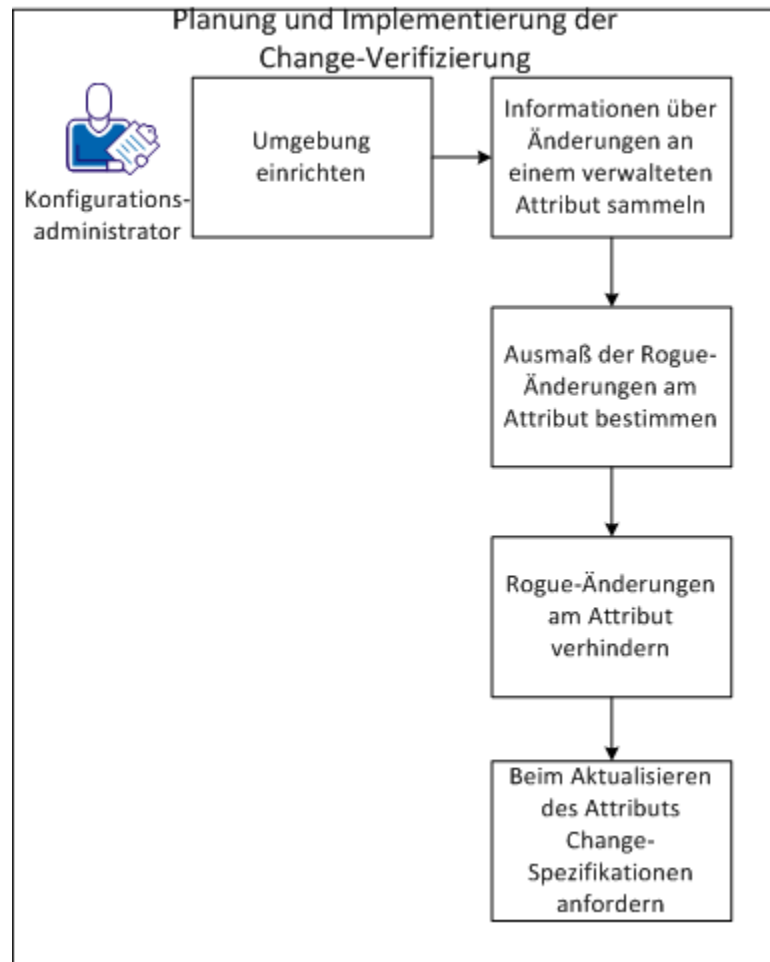
1. Erstellen Sie eine Verifizierungsrichtlinie, und geben Sie **Rogue NY Server** als Namen ein.
2. Füllen Sie die gewünschten Musterfelder aus.
3. Stellen Sie sicher, dass nur "Rogue-Einfügung" und "Rogue-Aktualisierung" als die Change-Ausrichtungsoptionen aktiviert sind.
4. Wählen Sie in der Drop-down-Liste "Aktualisierungsverhalten" *Aktualisierung nur zulassen, falls sie mit der Change-Spezifikation übereinstimmt*.
5. Wählen Sie in der Drop-down-Liste "Incident erstellen" "Ja" aus, und weisen Sie eine Vorlage zu.
6. Klicken Sie auf "Speichern".

Planen und Implementieren von Change-Verifizierung

Die Configuration Manager will Change-Verifizierung implementieren, damit die CMDB korrekte Daten enthält. Der Change Manager will dabei helfen, sicherzustellen, dass Changes richtig ausgeführt werden, und möchte die Anzahl sowie die Datenquellen von Rogue-Änderungen kennen. Die beiden Manager sind sich einig, dass die Implementierung von Change-Verifizierung der ein bedeutender Wert für die Organisation ist. Die Change Manager möchte dazu beitragen, sicherzustellen, dass Änderungen am Change Management-Prozess die Produktionsumgebung nicht schädigen.

Configuration Manager und Change Manager beschließen gemeinsam die Durchführung einer konservativen, schrittweisen Implementierung, was zur Folge hat, dass ein Configuration Administrator Richtlinien für bestimmte Lokationen sowie bestimmte CIs in diesen Lokationen implementiert. Dieses Szenario beschreibt Beispielphasen der Implementierung von Verifizierungsrichtlinien abzuschließen für eine umfangreichere Zielgruppe Ihrer Organisation.

Das folgende Diagramm zeigt, wie ein Configuration Administrator die Beispielsphasen abschließt, um die Change-Verifizierung zu implementieren:



1. [Einrichten der Umgebung](#) (siehe Seite 761).
2. [Sammeln von Informationen zu Änderungen an einem verwalteten Attribut](#) (siehe Seite 761).
3. [Bestimmen des Umfangs von Rogue-Änderungen am Attribut](#) (siehe Seite 763).
4. [Verhindern von Rogue-Änderungen am Attribut](#) (siehe Seite 764).
5. [Anfordern von Change-Spezifikationen beim Aktualisieren des Attributs](#) (siehe Seite 765).

Einrichten der Umgebung

Sie richten die Umgebung so ein, dass Configuration Administrators CIs jederzeit aktualisieren können. Der Configuration Administrator kann in der CMDB nach Bedarf CIs erstellen und aktualisieren, ohne einen Change angeben zu müssen, und es wird darauf vertraut, dass er korrekte CI-Daten angibt.

Gehen Sie wie folgt vor:

1. Erstellen Sie eine Verifizierungsrichtlinie namens **Richtlinie0.1** mit den folgenden Informationen:

- Geben Sie **1** als Sequenz ein.
- Geben Sie **Administrator erlauben, CIs jederzeit zu aktualisieren** als Beschreibung ein.
- Aktivieren Sie alle Change-Ausrichtungsoptionen.
- Geben Sie **Configuration Administrator** als Rollenmuster ein.
- Geben Sie **Web-Client** als MDR-Klassen-Muster ein.
- Geben Sie ein Sternchen (*) als CI-Name und -Klasse sowie für alle weiteren Muster ein.
- Wählen Sie "Alle verwalteten Attribute" als verwaltetes Attribut aus.

2. Wählen Sie "Attributaktualisierung zulassen" als Aktualisierungsverhalten aus.
3. Klicken Sie auf "Speichern".

Die Richtlinie wird aktiviert und erlaubt ausschließlich Configuration Administrators, CIs jederzeit zu aktualisieren.

Sammeln von Informationen zu Änderungen an einem verwalteten Attribut

Sie möchten Informationen zu Änderungen an einem spezifischen verwalteten CI-Attribut erfassen um zu identifizieren, welche CIs aktualisiert werden, was die Quelle der Änderungen ist, wer die Änderungen durchführt und welche Werte angegeben werden, um dadurch das Festlegen einer Verifizierungsstrategie für das Attribut und dazugehörige CIs zu erleichtern. Sie möchten zum Beispiel den Umfang aller Änderungen an der IP-Adresse (alarm_id) kennen und im CA SDM-Standardprotokoll (stdlog) festhalten. Das Erfassen dieser Informationen kann mehrere Wochen in Anspruch nehmen, je nach der Anzahl von Änderungen an Attributen in Ihrer Organisation.

1. Definieren Sie "IP-Adresse (alarm_id)" als verwaltetes Attribut.
2. Definieren Sie "Implementierung in Bearbeitung" und "Verifizierung in Bearbeitung" als verwaltete Change-Status in Ihrer Umgebung, und aktivieren Sie "Change-Verifizierung aktiv" für beide Zustände.

3. Erstellen Sie eine Verifizierungsrichtlinie namens "Richtlinie1.1" mit den folgenden Informationen:
 - Geben Sie **3000** als Sequenz ein.
 - Geben Sie **Alle Changes an IP-Adresse ins Protokoll schreiben** als Beschreibung ein.
 - Aktivieren Sie alle Change-Ausrichtungsoptionen.
 - Geben Sie ein Sternchen als CI-Name und -Klasse sowie für alle weiteren Muster ein.
 - Aktivieren Sie den Modus "Nur Protokoll".
4. Klicken Sie auf "Speichern".
5. Überprüfen Sie nach ein paar Wochen die stdlog-Protokolle, um die Quellen der Aktualisierungen anzuzeigen.

Zum Beispiel zeigt das Protokoll Rogue-CI-Aktualisierungen und Aktualisierungen mit übereinstimmenden Changes an.
6. Sie erkennen, dass Anwender in NY die IP-Adresse von CIs aktualisiert haben, ohne Changes zu erstellen.
7. Nachdem Sie Ihre Analyse abgeschlossen haben, deaktivieren Sie Richtlinie1.1, indem Sie diese Richtlinie bearbeiten und "Aktiv?" in "Inaktiv" ändern.

Bestimmen des Umfangs von Rogue-Änderungen am Attribut

Sie möchten den Umfang von Rogue-Änderungen am IP-Adressattribut bestimmen. Die Kenntnis des Umfangs von Rogue-Änderungen hilft Ihnen dabei, die Auswirkungen von Rogue-Änderungen auf Ihre Organisation zu verstehen. Zum Beispiel möchten Sie basierend auf Ihrer früheren Analyse mit der Option "Nur Protokoll" Incidents erstellen, wenn IP-Adressen, die mit "test" beginnen und sich in New York befinden, ohne einen Change zu benötigen. Teilen Sie den Change Managern in Ihrer Organisation mit, dass sie neue Incidents, die dieser Prozess erstellt, ignorieren können.

Gehen Sie wie folgt vor:

1. Führen Sie die folgenden anfänglichen Implementierungsaktionen durch:
 - Definieren Sie "Implementierung in Bearbeitung" als verwalteten Change-Zustand, und aktivieren Sie Option "Implementierungsstatus".
 - Definieren Sie "Verifizierung in Bearbeitung" als verwalteten Change-Zustand, und deaktivieren Sie die Option "Change nach Verifizierung hochstufen". .
 - Definieren Sie "IP-Adresse (alarm_id)" als verwaltetes Attribut, sofern dies nicht bereits definiert ist.
2. Erstellen Sie eine Verifizierungsrichtlinie namens Richtlinie2.1 mit den folgenden Informationen:
 - Geben Sie 3001 als Sequenz ein.
 - Geben Sie eine Beschreibung dieser Richtlinie ein. Geben Sie Beispielsweise **Rogue-Einfügungen und Rogue-Aktualisierungen werden dazu führen, dass Incidents erstellt werden. Alle anderen Änderungen werden nicht verhindert.**
 - Wählen Sie "Rogue-Einfügungen" und "Rogue-Aktualisierungen" als Ausrichtungen aus.
 - Wählen Sie aus der Drop-down-Liste "Verwaltetes Attribut" "IP-Adresse" aus.
 - Geben Sie **test*** als CI-Namen, **NY** als Lokation und ein Sternchen für alle weiteren Muster ein.
 - Wählen Sie aus den Aktionen für "Attributaktualisierung zulassen" "Ja" aus, damit ein Incident erstellt wird, sowie eine Incident-Vorlage.

3. Klicken Sie auf "Speichern".

Nachdem Sie diese Phase abgeschlossen haben, erstellt CACF Incidents für alle Computer in NY. Sie entdecken die folgenden Informationen, nachdem Sie die Incidents überprüft haben:

- Aus verschiedenen MDRs kommen unterschiedliche IP-Adressen für ein CI.
- Einige MDRs sind autorisiert, andere MDRs sind nicht autorisiert.
- Einige CIs sollten nicht auf Basis von Lokation, Familie, Name, Servicetyp, usw. verwaltet werden.

4. Der Change Manager bespricht sich mit anderen IT-Managern, um die CMDBs, CI-Detailformulare, Verifizierungsprotokolle und Attributnamen in Filtern zu überprüfen, um die Rogue-Daten zu sehen.
5. Ihre Organisation beschließt, den CI-Filter in Richtlinie 2.1 zu aktualisieren, um nur Server mit Priorität 1 zu verwalten.

Verhindern von Rogue-Änderungen am Attribut

Sie möchten Rogue-Änderungen am IP-Adressattribut verhindern, um dabei zu helfen, die CMDB-Datenintegrität zu sichern, und benötigen einen Change für diese Aktualisierung. Der Change muss das CI und eine Change-Spezifikation enthalten. Die IP-Adresse ist für die Durchführung nicht erforderlich. Die Change-Verifizierung geschieht auf CI- oder Change-Ebene und nicht auf Attributebene. Verhindern Sie zum Beispiel sämtliche Rogue-Aktualisierungen und verwenden Sie die Incident-Erstellung, um die Anwender zu verfolgen, die diese Änderungen anfordern.

Gehen Sie wie folgt vor:

1. Setzen Sie Richtlinie1.1 und Richtlinie2.1 auf "Inaktiv", um diese Richtlinien zu deaktivieren.
2. Erstellen Sie Richtlinie3.1 mit folgenden Informationen:
 - Geben Sie **3100** als Sequenz ein.
 - Geben Sie **Verhindert Rogue-Änderungen ohne Change** als Beschreibung ein.
 - Wählen Sie "Rogue-Aktualisierung" als Ausrichtung aus.
 - Geben Sie **test*** als CI-Namen, **NY** als Lokation und ein "Alle verwalteten Attribute" sowie ein Sternchen für alle weiteren Muster ein.
 - Wählen Sie die Aktion "Immer gesamte Transaktion abbrechen".
3. Klicken Sie auf "Speichern".
4. Erstellen Sie Richtlinie3.2 mit folgenden Informationen:
 - Geben Sie **3200** als Sequenz ein.
 - Geben Sie **Macht einen Change für IP-Adressänderungen erforderlich** als Beschreibung ein.
 - Wählen Sie "Changes ohne Spezifikationen" als Ausrichtung aus.
 - Geben Sie **test*** als CI-Namen, **NY** als Lokation und ein Sternchen für alle weiteren Muster ein.
 - Wählen Sie aus der Drop-down-Liste "Veraltetes Attribut" "IP-Adresse" aus.
 - Wählen Sie "Attributaktualisierung zulassen" als Aktion aus.
5. Klicken Sie auf "Speichern".

Diese Richtlinie verhindert Rogue-Änderungen, da für Änderungen immer Changes vorhanden sein müssen.

Die Configuration Manager sieht, dass auch nicht im Change definierte Daten aktualisiert werden, da Change-Spezifikationen für Änderungen auf Attributebene nicht erforderlich sind. So wird beispielsweise die Anforderung nach einer Erhöhung von "Installierter Speicher" bei gleichzeitiger Änderung der IP-Adresse nicht als Rogue-Änderung betrachtet, da ein Change vorhanden ist. Zusätzlich sollen Changes automatisch verifiziert und höhergestuft werden, und es soll automatisch festgestellt werden, wenn eine Verifizierung auf Attributebene stattfinden soll.

Anfordern von Change-Spezifikationen beim Aktualisieren des Attributs

Den Configuration Manager beunruhigt, dass Daten in der CMDB mehrere Aktualisierungen für nicht im Change angegebene Änderungen erhalten. Zum Beispiel ändert ein Anwender gleichzeitig den Wert für "Installierter Speicher" (phys_mem) und "IP-Adresse" (ip_address). In der vorherigen Phase betrachtet CACF diesen Request nicht als Rogue-Änderung, weil ein Change vorhanden ist.

Der Configuration Manager will die Change-Verifizierung auf Attributebene durchsetzen. Der Configuration Administrator erstellt eine Richtlinie, die die Verwendung von Change-Spezifikationen erforderlich macht, wenn IP-Adressen aktualisiert werden, sowie die Erstellung von Incidents, wenn keine Rogue-Aktualisierung versucht wird.

Gehen Sie wie folgt vor:

1. Der Configuration Manager teilt Change-Analysten mit, dass Änderungen an IP-Adressen eine Change-Spezifikation enthalten müssen.
2. Setzen Sie Richtlinie3.1 und Richtlinie3.2 auf "Inaktiv", um diese Richtlinien zu deaktivieren.
3. Erstellen Sie Richtlinie4.1 mit folgenden Informationen:
 - Geben Sie **4000** als Sequenz ein.
 - Geben Sie **Macht Change-Spezifikationen für IP-Adressänderungen erforderlich** als Beschreibung ein
 - Wählen Sie "Rogue-Einfügung", "Rogue-Aktualisierung" und "Changes ohne Spezifikationen" als Ausrichtung aus.
 - Geben Sie **test*** als CI-Namen, **NY** als Lokation und ein Sternchen für alle weiteren Muster ein.
 - Wählen Sie aus der Drop-down-Liste "Veraltetes Attribut" "IP-Adresse" aus.
 - Wählen Sie als Aktion "Immer gesamte Transaktion abbrechen".

4. Klicken Sie auf "Speichern".
5. Erstellen Sie Richtlinie4.2 mit folgenden Informationen:
 - Geben Sie **4100** als Sequenz ein.
 - Geben Sie **Macht Change-Spezifikationen für IP-Adressänderungen erforderlich**als Beschreibung ein
 - Wählen Sie "Changes ohne Spezifikationen" als Ausrichtung aus.
 - Geben Sie **test*** als CI-Name ns-und **NY** als Lokationsmuster ein.
 - Wählen Sie aus der Drop-down-Liste "Verwaltetes Attribut" "IP-Adresse" aus.
 - Wählen Sie als Aktion "Aktualisierung nur zulassen, falls sie mit der Change-Spezifikation übereinstimmt" aus.
6. Klicken Sie auf "Speichern".

Sie haben die erforderlichen Beispielphasen erfolgreich abgeschlossen und können die Change-Verifizierung in Ihrer Umgebung implementieren. Sie können die Change-Verifizierungsstrategie erweitern, um weitere Attribute, CIs, MDRs und Mandanten aufzunehmen.

Best Practices für Change-Verifizierung

Berücksichtigen Sie bei der Implementierung von Change-Verifizierung folgende Best Practices:

- Definieren Sie wenige Richtlinien.
- Vermeiden Sie die Verwendung von negativer Logik (Ausrufezeichen in Richtlinienmustern).
- CI-Aktualisierungen sollten mit einer kleinen Anzahl von Richtlinien übereinstimmen.
- Organisieren Sie Richtlinien in einer numerisch abgestuften Struktur.
- Testen Sie Change-Verifizierungsrichtlinie vor der Implementierung im Nur Protokoll-Modus.
- Vermeiden Sie, wenn möglich, Richtlinienüberschneidungen, wenn mehrere Richtlinien ein einzelnes Attribut verwalten, das aktualisiert wird.
- Beschränken Sie die Anzahl von Incidents, die CACF erstellt.
- Implementieren Sie die Archivierung und Bereinigung von CACF-Daten.

Weitere Informationen:

[Organisieren von Richtlinien](#) (siehe Seite 767)

[Hinweise zu Mandantenfähigkeit](#) (siehe Seite 768)

[CACF-Rollen und Zugriff auf Funktionen](#) (siehe Seite 768)

Organisieren von Richtlinien

Sie können verschiedene Strategien verwenden, um Richtlinien nachzuverfolgen. Wir empfehlen, einen mehrstufigen Ansatz zu verwenden. Steigern Sie die Nummern der Richtlinien jeweils um 100, um künftige Einfügungen weiterer Richtlinien zu ermöglichen.

Berücksichtigen Sie die folgenden Beispielebenen für diese Strategie:

Grundsätzliche Richtlinien

100,000-199,999

- Erlauben Sie Change-Administratoren, Einfügungen auszuführen
- Lassen Sie Einfügungen von MDR Class(xxxx) nicht zu
- Schließen Sie alle Test-CIs aus der Incident-Erstellung aus

Temporäre oder Übergangsrichtlinien

200,000-299,999: Massenladungsvorgänge der laufenden Woche

Anwendungsspezifische Richtlinien

- 301,000-301,999: Ausnahmen für die folgenden allgemeinen anwendungsspezifischen Richtlinien:
Zum Beispiel server1 in NY-Richtlinien
- 311,000-311,999: Richtlinien, die sich auf Lösungen von Servicetypen mit priority1 beziehen
- 320,000-320,999: Richtlinien, die sich auf NY beziehen
- 331.000-331.999: Richtlinien, die sich auf Lisle beziehen

Technologiespezifische Richtlinien

- 410,000-410,999: die sich auf Server beziehen
- 411.000-411.999: die sich auf Netzwerke beziehen

Standardrichtlinien

Sie können diese Richtlinien verwenden, wenn sich die zuvor genannten Richtlinien nicht auf Ihre Umgebung beziehen.

900,000-999,999: Standardrichtlinien, beispielsweise, dass alle Aktualisierungen an verwalteten Attributen (Alle verwalteten Attribut) eine Change-Spezifikation haben müssen.

Hinweise zu Mandantenfähigkeit

Beachten Sie die folgenden Informationen, wenn Sie CACF in einer Umgebung mit mehreren Mandanten verwenden:

- Verwaltete Attribute, Verifizierungsrichtlinien, Changes und Change-Spezifikationen sind unterliegen Mandanten.
- Alle Mandanten in der Hierarchie können alle CACF-Objekte anzeigen.
Wenn ein Mandant z. B. ein verwaltetes Attribut erstellt, kann diese Aktion einen Mandanten in der Hierarchie daran hindern, ein dupliziertes verwaltetes Attribut zu erstellen. Die Hierarchie benötigt eindeutige Richtliniensequenznummern.
- Um die Richtlinie zu bestimmen, die Änderungen an einem Attribut verwaltet, berücksichtigen Sie nur Richtlinien aus der Mandantenhierarchie des Objekts (CI).
- Ein untergeordneter Mandant kann eine Richtlinie erstellen, die den übergeordneten Mandanten überschreibt, indem er der lokalen Richtlinie eine niedrigere Sequenznummer zuweist.
- CACF beachtet nur Richtlinien auf der Ebene des Mandanten sowie der hierarchisch übergeordneten Mandanten.
- CACF berücksichtigt den Mandanten des Kontakts, der die Änderung durchführt, nicht.

Hinweis: Verifizierungsrichtlinien sind systemspezifisch und variieren nicht nach Anwender oder Rolle.

CACF-Rollen und Zugriff auf Funktionen

Die folgende Tabelle beschreibt die Standardrollen, die CACF verwendet:

Rolle/Funktionszugriff	Administration	CI	Incident/Problem/Request	Change
Administrator	Ändern	Ändern	Ändern	Ändern
Konfigurationsadministrator	Ändern	Ändern	Ändern	Ändern
Konfigurationsanalyst	Ansicht	Ändern	Ändern	Ändern
Konfigurations-Viewer	Keine	Ansicht	Ändern	Ansicht
Change Manager	Ansicht	Ändern	Ändern	Ändern
Service Desk-Administrator	Ändern	Ändern	Ändern	Ändern
CA Service Desk-Manager	Ansicht	Ändern	Ändern	Ändern
Systemadministrator	Ändern	Ändern	Ansicht	Ansicht
Level 1-Analyst	Ansicht	Ansicht	Ändern	Ansicht

Rolle/Funktionszugriff	Administration	CI	Incident/Problem/Request	Change
Level 2-Analyst	Ansicht	Ändern	Ändern	Ändern
Incident Manager	Ansicht	Ansicht	Ändern	Ändern
Problem Manager	Ansicht	Ansicht	Ändern	Ändern

Administration

Steht für Erstellen, Aktualisieren und Anzeigen von CACF-Verwaltung, Richtlinien und Attributmanagement.

CI

Steht für Erstellen, Aktualisieren und Anzeigen von CI- und Beziehungsattributdaten.

Incident/Problem/Request

Steht für Ändern und Anzeigen hervorstechende CACF-Issues einschließlich Rogue-Änderungen und inkorrektur Abweichungen bei der Durchführung von Changes.

Changes

Steht für Erstellen, Aktualisieren und Anzeigen von Change-Spezifikationen.

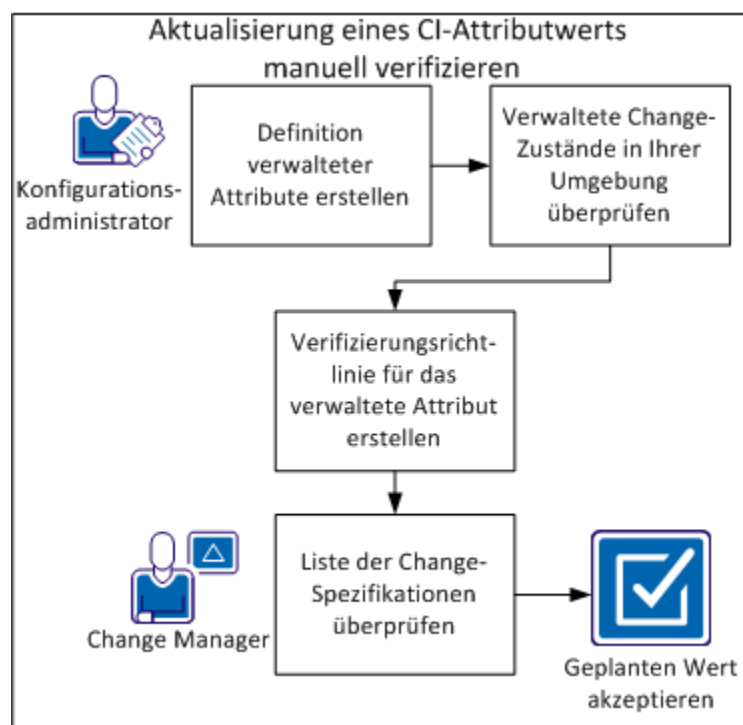
Zum Beispiel ermöglicht es die Change Manager-Rolle, CACF-Richtlinien anzeigen und Attribute zu verwalten, jedoch nicht, sie zu aktualisieren.

Wichtig! Aktualisierungszugriff auf den Change und seinen Status bestimmen, wer Change-Spezifikationen bearbeiten darf. Der Change-Administrator kann diesen Zugriff beispielsweise dem Change Manager gewähren.

Manuelles Verifizieren von aktualisierten Attributwerten

Der Configuration Administrator entscheidet, dass Ihre CA SDM-Umgebung eine Verifizierungsrichtlinie für das Attribut "Installierter Speicher" (phys_mem) benötigt. Der Configuration Administrator erstellt eine Definition als verwaltetes Attribut mit dem Status *Macht manuelle Verifizierung erforderlich*, da CA SDM keinen MDR hat, um den Wert zu erkennen. Der Configuration Administrator verifiziert die verwalteten Zustände und erstellt eine Verifizierungsrichtlinie. Der Change Manager zeigt einen Change an, der eine Aktualisierung am Wert "Installierter Speicher" eines CI erfordert, und dieser Change muss manuell verifiziert werden.

Das folgende Diagramm erklärt, wie ein Configuration Administrator eine Verifizierungsrichtlinie festlegt und wie der Change Manager eine Aktualisierung eines CI-Attributwerts manuell verifiziert:



1. [Erstellen einer Definition als verwaltetes Attribut](#) (siehe Seite 771).
2. [Überprüfen der verwalteten Change-Zustände in Ihrer Umgebung](#) (siehe Seite 772).
3. [Erstellen einer Verifizierungsrichtlinie für das verwaltete Attribut](#) (siehe Seite 772).
4. [Überprüfen der Liste der Change-Spezifikationen](#) (siehe Seite 774).
5. [Akzeptieren des Planwerts](#) (siehe Seite 775).

Erstellen einer Definition als verwaltetes Attribut

Der Configuration Administrator erstellt eine Definition als verwaltetes Attribut für das Attribut "Installierter Speicher" (phys_mem).

Gehen Sie wie folgt vor:

1. Klicken Sie auf der Registerkarte "Administration" auf "CA CMDB", "Konfigurationssteuerung", "Verwaltete Attribute".
2. Klicken Sie auf "Neu erstellen".
3. Geben Sie **phys_mem** als Attributname ein.
4. Geben Sie **Installierter Speicher** als Attributbeschriftung ein.
5. Wählen Sie in der Drop-down-Liste "Anfänglicher Verifizierungsstatus" *Macht manuelle Verifizierung erforderlich* aus.
6. (Optional) Aktivieren Sie die Option "Groß- /Kleinschreibung beachten", wenn Sie erzwingen möchten, dass beim Vergleich der Planwerte der Change-Spezifikation Groß- und Kleinschreibung berücksichtigt werden muss.

Standard: Deaktiviert

7. Klicken Sie auf "Speichern".
Das verwaltete Attribut wird gespeichert.

Überprüfen der verwalteten Change-Zustände in Ihrer Umgebung

Der Configuration Administrator überprüft die verwalteten Change-Zustände in der CA SDM-Umgebung. Change-Verifizierung wird initiiert, wenn sich der Status eines Change in einen Change-Zustand ändert, der durch CACF verwaltet wird, beispielsweise "Verifizierung in Bearbeitung".

Hinweis: Der Configuration Administrator kann anpassen, in welchem Zustand im Change-Lebenszyklus die Change-Verifizierung initiiert wird. Der Administrator kann auch anpassen, in welchen Zuständen Sie Change-Spezifikationen ändern können, wenn die Implementierung startet.

Gehen Sie wie folgt vor:

1. Klicken Sie auf der Registerkarte "Administration" auf "CA CMDB", "Konfigurationssteuerung", "Verwaltete Change-Zustände".
2. Klicken Sie auf "Implementierung in Bearbeitung", um die Details des verwalteten Status anzuzeigen.
3. Überprüfen Sie die Details des verwalteten Status.

Zum Beispiel beschließen Sie, zu erlauben, dass im Status "Implementierung in Bearbeitung" Change-Spezifikationen geändert werden. Zusätzlich aktivieren Sie "Change-Verifizierung aktiv". Das soeben aufgeführte Beispiel steht für einen aktiven Change-Verifizierungsprozess, in dem Sie Werte bearbeiten können, wenn der Change in den Status "Implementierung in Bearbeitung" gelangt.

4. Schließen Sie die Seite.

Erstellen einer Verifizierungsrichtlinie für das verwaltete Attribut

Die Verifizierungsrichtlinie gibt die CACF-Aktion an, die eintritt, wenn ein MDR einen Attributwert entdeckt, und versucht, die CMDB mit diesen Daten zu aktualisieren.

Gehen Sie wie folgt vor:

1. Klicken Sie auf der Registerkarte "Administration" auf "CA CMDB", "Konfigurationssteuerung", "Verifizierungsrichtlinien".
2. Klicken Sie auf "Neu erstellen", um die Detailseite zu öffnen.
3. Geben Sie **1000** als Richtliniensequenz ein.

Hinweis: Sie können im Einklang mit den Prioritäten der Verifizierungsrichtlinien in Ihrer Umgebung eine höhere oder niedrigere Zahl eingeben.

4. Geben Sie einen Richtliniennamen, beispielsweise **RAM-Management**, und eine kurze Beschreibung der Richtlinie ein.
5. Wählen in "Change-Ausrichtung" "Rogue-Einfügung" und "Rogue-Aktualisierung" aus.

6. Wenn Sie wollen, dass die Richtlinie ein spezifisches MDR daran hindert, das Attribut "Installierter Speicher" (phys_mem) zu aktualisieren, führen Sie die folgenden Aufgaben durch:
 - Wählen Sie "Installierter Speicher" als das verwaltete Attribut aus.
 - Geben Sie ein Rollenmuster ein, oder verwenden Sie ein Sternchen, um alle Rollen auszuwählen.
 - Geben Sie ein CI-Namensmuster ein, oder verwenden Sie ein Sternchen, um alle CIs auszuwählen.
 - Geben Sie ein Klassenmuster ein, oder verwenden Sie ein Sternchen, um alle Klassen auszuwählen.
 - Wählen Sie "Alten Attributwert beibehalten" als Aktualisierungsverhalten aus.

Hinweis: Wenn Sie Aktualisierungen an diesem Attribut nur durch Anwender erlauben möchten, die sich über die Webanwenderoberfläche angemeldet haben, geben Sie **Web-Client** als MDR-Namensmuster ein.
7. Klicken Sie auf "Speichern".
8. Schließen Sie die Seite.

Überprüfen der Liste der Change-Spezifikationen

Für einen Change mit Status "RFC" soll der Wert für das Attribut "Installierter Speicher" (phys_mem) in ein CI namens server1 geändert werden. Der Change Manager setzt den Verifizierungsstatus der Change-Spezifikation auf *Macht manuelle Verifizierung erforderlich*. Der Change Manager kann die Change-Spezifikation in CA SDM anzeigen.

Gehen Sie wie folgt vor:

1. Der Change Manager verschiebt den Change aus "RFC" in "Verifizierung in Bearbeitung".

Alle Change-Spezifikationen mit manueller Verifizierung ändern sich in "Manuelle Verifizierung aktiv".

2. Wählen Sie im Change auf der Registerkarte "Configuration Management" die Registerkarte "Change-Spezifikationen" aus.

Auf der Registerkarte sind alle Change-Spezifikationen rot hervorgehoben, um anzuzeigen, dass eine manuelle Verifizierung notwendig ist.

Hinweis: Sie können Change-Spezifikationen auch über die Registerkarte "Administration" anzeigen, indem Sie auf "CA CMDB", "Configuration Audit", "Change-Spezifikationen" klicken. Zusätzlich können Sie Change-Spezifikationen im CI anzeigen, indem Sie auf der Registerkarte "Zugehörige Tickets" die Registerkarte "Change-Spezifikationen" auswählen.

3. Suchen Sie nach Change-Spezifikationen mit dem Verifizierungsstatus *Manuelle Verifizierung ist erforderlich*.

Zum Beispiel haben die Change-Spezifikationen von Change 21 diesen Status.

4. Suchen Sie den entsprechenden Wert für das Attribut "Installierter Speicher" für das CI "server1".

Hinweis: Change-Spezifikationen, deren Verifizierung fehlgeschlagen ist, werden rot angezeigt, damit Change-Spezifikationen, die besonders beachtet werden müssen, leicht zu erkennen sind.

Akzeptieren des Planwerts

Der Change Manager sucht den richtigen Attributwert für das CI und trifft die entsprechende Entscheidung für den Change Request.

Gehen Sie wie folgt vor:

1. Öffnen Sie die Change-Spezifikation, um die Detailseite anzuzeigen.
2. Sie suchen das Attribut "Installierter Speicher" (phys_mem) für das CI und bestätigen den geplanten Wert.
3. Überprüfen Sie, dass sich der Change der Change-Spezifikation im Zustand "Verifizierung in Bearbeitung" befindet.
4. Klicken Sie auf "Geplanten Wert akzeptieren".

Der Verifizierungsstatus ändert sich in "Geplanter Wert akzeptiert".

Hinweis: Nachdem Sie auf "Akzeptieren" geklickt haben, wird das CI automatisch mit dem geplanten Wert aktualisiert.

Nun haben Sie einen verwalteten Attributwert erfolgreich manuell verifiziert.

Beispiel: Rogue-Aktualisierungen nur von einer bestimmten Lokation erlauben

In diesem Beispiel müssen ServersCIs in Ihrem New Yorker Büro repariert werden. Der Anbieter, der auch Ihre Server repariert, befindet sich in New York. Das Asset Manager benötigt, dass Ihre Organisation alle defekten Server nach New York sendet. Der Configuration Administrator möchte Rogue-Aktualisierungen an den CIs erlauben, wenn die Hardware in New York eintrifft. Der Configuration Administrator erstellt eine Verifizierungsrichtlinie für das Attribut "Wartungsanbieter", damit ein Service Desk-Analyst in New York sicherstellen kann, dass der Anbieter die Server empfängt.

Gehen Sie wie folgt vor:

1. Erstellen Sie das folgende verwaltete Attribut:
 - Geben Sie **vendor_repair** als Attributname ein
 - Wählen Sie in der Drop-down-Liste mit den anfänglichen Status "Verifizierung ausstehend" aus.
 - Geben Sie **Wartung** als Beschriftung und Beschreibung der Details des verwalteten Attributs ein.
2. Erstellen Sie den folgenden verwalteten Change-Status:
 - Geben Sie **Anbieterzurückstellung** als Change-Status ein.
 - Aktivieren Sie die Option "Change-Verifizierung aktiv".

3. Erstellen Sie die folgende Verifizierungsrichtlinie:
 - Wählen Sie "Rogue-Einfügung" und "Rogue-Aktualisierung" als Change-Ausrichtungen aus.
 - Geben Sie eine Sequenznummer für die Richtlinie ein.
Geben Sie zum Beispiel **201** ein.
 - Geben Sie **server*** als CI-Namensmuster ein.
 - Geben Sie **Server** als Klassenmuster ein.
 - Geben Sie **New York** als Lokationsmuster ein.
 - Wählen Sie in der Drop-down-Liste "Aktualisierungsverhalten" "Attributaktualisierung zulassen" aus.
4. Der Service Desk-Analyst erstellt einen Change und Change-Spezifikationen für die Server-CIs und gibt "New York" als Lokation an.
5. Der Service Desk-Analyst setzt den Change-Status auf "Anbieterzurückstellung".
6. Der Service Desk-Analyst aktualisiert die Lokation für die Server-CIs als "New York".
Zum Beispiel werden defekte Server aus Chicago nach New York gesendet, und der Service Desk-Analyst verifiziert, ob die Server in New York angekommen sind.
7. Der Service Desk-Analyst gibt die Anbieterinformationen in das CI ein.
Der Change wird geschlossen, wenn alle CI-Lokationen auf New York festgelegt sind und alle Change-Spezifikationen verifiziert wurden.

Beispiel: Durchführen eines Upgrade für Laptops in Ihrer Organisation

In diesem Beispiel will ein Asset Manager alle Laptops in Ihrer Organisation von Windows XP auf Windows 7 aktualisieren. Der Configuration Administrator erstellt eine Verifizierungsrichtlinie für das Attribut "Produktversion", um alle Laptops mit dem Betriebssystem Windows XP zu filtern. Der Configuration Administrator erstellt eine Definition als verwaltetes Attribut mit dem Status *Erkannten Wert verwenden*, verifiziert verwaltete Zustände und erstellt eine Verifizierungsrichtlinie. CA SDM empfängt von CA Configuration Automation CMDB-Aktualisierungen für Laptops, die eine Betriebssystemaktualisierung benötigen, und das Asset Management-Team führt die Upgrades durch.

Gehen Sie wie folgt vor:

1. Erstellen Sie das folgende verwaltete Attribut:
 - Geben Sie **product_version** als Attributname ein
 - Geben Sie **Produktversion** als Attributbeschriftung ein.
 - Wählen Sie in der Drop-down-Liste mit den anfänglichen Status "Erkannten Wert verwenden" aus.
 - Geben Sie eine Beschriftung und Beschreibung der Details des verwalteten Attributs ein.
2. Erstellen Sie die folgende Verifizierungsrichtlinie:
 - Geben Sie eine Sequenznummer ein, die auf den restlichen Richtlinien in Ihrer Organisation basiert.
Geben Sie zum Beispiel **101** ein.
 - Geben Sie **Windows* XP*** als CI-Namensmuster ein.
 - Geben Sie **Workstation** als Klassenmuster ein.
 - (Optional) Geben Sie ein Lokationsmuster ein, wenn Sie die Richtlinie zu einem bestimmten Büro in Ihrer Organisation zuordnen wollen.
 - Wählen Sie in der Drop-down-Liste "Aktualisierungsverhalten" Aktualisierung nur zulassen, falls sie mit der Change-Spezifikation übereinstimmt.
 - Wählen Sie in Drop-down-Liste "Incident" "Ja" aus.
3. Erstellen Sie einen Change und Change-Spezifikationen, die als verwaltetes Attribut "Produktversion" für alle Laptops-CIs "Windows 7" enthalten.
4. Verschieben Sie den Change in den Status "Implementierung wird durchgeführt", und warten Sie, bis Ihre Asset Management-Team, mit den Upgrades beginnt.

5. Wenn die Implementierungen abgeschlossen sind, verschieben Sie den Change in "Verifizierung in Bearbeitung".

CA Configuration Automation entdeckt Laptop-Informationen und importiert die Daten in die CMDB.
6. Zeigen Sie die Liste "Offene CACF-Incidents" für Abweichungen an, die durch CACF entdeckt wurden.
7. Wählen Sie einen Incident aus und überprüfen Sie die Laptop-Details, die CA Configuration Automation entdeckt hat.
8. Klicken Sie auf "Change Erstellen" und ordnen Sie das CI zum Ticket zu, und geben Sie in "Produktversion" Change-Spezifikationen für die ausstehenden Änderungen ein.

Warten Sie ab, bis Discovery verifiziert hat, dass alle verbleibenden Changes abgeschlossen wurden.
9. Wiederholen Sie bei Bedarf die Schritte 6-8 für neue durch CACF erstellte Incidents.

Beispiel: Sperren nicht verifizierter Changes

In diesem Beispiel will der Configuration Administrator nur eine CI-Aktualisierung für einen übereinstimmenden Change erlauben. Nur CIs der Server-Klasse, die sich in NY befinden, werden für verifizierte Changes aktualisiert. Durch jede Abweichung wird ein Incident erstellt.

Gehen Sie wie folgt vor:

1. Erstellen Sie eine Verifizierungsrichtlinie.
2. Führen Sie die folgenden Schritte aus:
 - a. Geben Sie eine Sequenznummer an.
 - b. Wählen Sie "Alle verwalteten Attribute" als verwaltetes Attribut aus.
 - c. Geben Sie **NY** als Lokationsmuster ein.
 - d. Geben Sie **Server** als Klassenmuster ein.
 - e. Wählen Sie als Aktualisierungsverhalten "Aktualisierung nur zulassen, falls sie mit der Change-Spezifikation übereinstimmt" aus.
 - f. Wählen Sie in Drop-down-Liste "Incident" "Ja" aus.
3. Speichern Sie die Richtlinie.

Beispiel: Erlauben einer CI-Aktualisierung, wenn kein übereinstimmender Change vorhanden ist

In diesem Beispiel will der Configuration Administrator Aktualisierungen für alle CIs mit Namen "test*" erlauben, auch, wenn kein übereinstimmender Change vorhanden ist. Diese Richtlinie akzeptiert Aktualisierungen von allen Anwendern mit einer administrativen Rolle.

Gehen Sie wie folgt vor:

1. Erstellen Sie eine Verifizierungsrichtlinie.
2. Führen Sie die folgenden Schritte aus:
 - a. Geben Sie eine Sequenznummer an.
 - b. Wählen Sie "Alle verwalteten Attribute" als verwaltetes Attribut aus.
 - c. Geben Sie **test*** als CI-Namensmuster ein.
 - d. Geben Sie **Administrator*** als Rollenmuster ein.
 - e. Wählen Sie "Attributaktualisierung zulassen" als Aktualisierungsverhalten aus.
3. Speichern Sie die Richtlinie.
4. Ein Anwender mit einer administrativen Rolle erstellt eine Change-Spezifikation für ein CI namens "test5".

Das CI wird erfolgreich aktualisiert.

Beispiel: Verschieben aller Aktualisierungen aus CA Configuration Automation in den TWA

In diesem Beispiel will der Configuration Administrator alle CI-Aktualisierungen aus CA Configuration Automation in den TWA verschieben. Diese Richtlinie aktualisiert das CI nicht in der CMDB, sondern schreibt alle Rogue-Änderungsdaten zur weitere Evaluierung in den TWA.

Gehen Sie wie folgt vor:

1. Erstellen Sie eine Verifizierungsrichtlinie.
2. Führen Sie die folgenden Schritte aus:
 - a. Geben Sie eine Sequenznummer an.
 - b. Wählen Sie "Alle verwalteten Attribute" als verwaltetes Attribut aus.
 - c. Wählen Sie "Rogue-Einfügung" und "Rogue-Aktualisierung" als Change-Ausrichtung aus.
 - d. Geben Sie **CCA** als MDR-Klassenmuster ein.

- e. Wählen Sie "Immer gesamte Transaktion abbrechen" als Aktualisierungsverhalten.
 - f. Wählen Sie für die Option "Daten in TWA schreiben" "Immer" aus.
3. Speichern Sie die Richtlinie.

Beispiel: Richtlinienergebnisse zu Testzwecken nur ins Protokoll schreiben

In diesem Beispiel will der Configuration Administrator eine neue Richtlinie testen, bevor er Sie in Ihrer CMDB-Umgebung implementiert. Die Option "Nur Protokoll" erlaubt es CACF, die potenziellen CI-Auswirkungen der Richtlinie in die standardmäßige Protokolldatei schreiben.

Gehen Sie wie folgt vor:

1. Erstellen Sie eine Verifizierungsrichtlinie.
2. Geben Sie die Information für die Ausrichtung, Filter und Aktion ein.
3. Aktivieren Sie die Option "Nur Protokoll".
4. Speichern Sie die Richtlinie.
5. Zeigen Sie die standardmäßige Protokolldatei an, nachdem Sie CI-Aktualisierungen ausgeführt haben, die mit den Richtlinienspezifikationen und Filterkriterien übereinstimmen, um die Ausführung der Richtlinie zu simulieren.

Beispiel: Ablehnen einer CI-Aktualisierung

In diesem Beispiel möchte der Configuration Aktualisierungen aus einem MDR namens "Cohesion" ausschließlich für das Attribut "IP-Adresse" (alarm_id) ablehnen. Diese Richtlinie aktualisiert die IP-Adresse des CI in der CMDB nicht, andere Attribute können jedoch aktualisiert werden. CACF schreibt alle Attribute zur weiteren Evaluierung in den TWA.

Gehen Sie wie folgt vor:

1. Fügen Sie IP-Adresse (alarm_id) zur Liste der verwalteten Attribute hinzu.
2. Erstellen Sie eine Verifizierungsrichtlinie.
3. Führen Sie die folgenden Schritte aus:
 - a. Geben Sie eine Sequenznummer an.
 - b. Wählen Sie "IP-Adresse" als verwaltetes Attribut aus.
 - c. Wählen Sie "Rogue-Einfügung" und "Rogue-Aktualisierung" als Change-Ausrichtung aus.
 - d. Geben Sie **Cohesionals** MDR-Muster ein.

- e. Wählen Sie "Alten Attributwert beibehalten" als Aktualisierungsverhalten aus.
 - f. Wählen Sie für die Option "Daten in TWA schreiben" "Immer" aus.
4. Speichern Sie die Richtlinie.

Beispiel: Erlauben von Changes ohne Spezifikationen

In diesem Beispiel will der Configuration Administrator Changes, die von Anwendern ohne Angabe von Spezifikationen erstellt wurden, als vertrauenswürdig behandeln. Diese Richtlinie nimmt an, dass der CI-Text sämtliche Änderungen akkurat beschreibt, und lässt die CI-Aktualisierung zu.

Gehen Sie wie folgt vor:

1. Erstellen Sie eine Verifizierungsrichtlinie.
2. Führen Sie die folgenden Schritte aus:
 - a. Geben Sie eine Sequenznummer an.
 - b. Wählen Sie "Alle verwalteten Attribute" als verwaltetes Attribut aus.
 - c. Wählen Sie "Changes ohne Spezifikationen" als Ausrichtung aus.
 - d. Wählen Sie "Attributaktualisierung zulassen" als Aktualisierungsverhalten aus.
3. Speichern Sie die Richtlinie.

Beispiel: Verboten von Changes ohne Spezifikationen

In diesem Beispiel will der Configuration Administrator Changes, die von Anwendern ohne Angabe von Spezifikationen erstellt wurden, als *nicht* vertrauenswürdig behandeln. Diese Richtlinie ignoriert Changes ohne Spezifikationen und erstellt Incidents.

Gehen Sie wie folgt vor:

1. Erstellen Sie eine Verifizierungsrichtlinie.
2. Führen Sie die folgenden Schritte aus:
 - a. Geben Sie eine Sequenznummer an.
 - b. Wählen Sie "Alle verwalteten Attribute" als verwaltetes Attribut aus.
 - c. Wählen Sie "Changes ohne Spezifikationen" als Ausrichtung aus.

- d. Wählen Sie "Immer gesamte Transaktion abbrechen" als Aktualisierungsverhalten.
 - e. Wählen Sie in der Drop-down-Liste "Incident erstellen" "Ja" aus, und wählen Sie eine Incident-Vorlage aus.
3. Speichern Sie die Richtlinie.

Beispiel: Erlauben von Rogue-Einfügungen aus ausgewählten Quellen

In diesem Beispiel will der Configuration Administrator neue CIs aus ausgewählten Quellen erlauben. Die z/OS-MDRs können CIs erstellen, ohne einen Change zu benötigen.

Gehen Sie wie folgt vor:

1. Erstellen Sie eine Verifizierungsrichtlinie.
2. Führen Sie die folgenden Schritte aus:
 - a. Geben Sie eine Sequenznummer an.
 - b. Wählen Sie "Alle verwalteten Attribute" als verwaltetes Attribut aus.
 - c. Wählen Sie "Rogue-Einfügung" als Ausrichtung aus.
 - d. Geben Sie **z/OS** als MDR-Klassenmuster ein.
 - e. Wählen Sie "Attributaktualisierung zulassen" als Aktualisierungsverhalten aus.
3. Speichern Sie die Richtlinie.

Beispiel: Erlauben einer Rogue-Aktualisierung für ein CI, dass nicht zur Produktion gehört

In diesem Beispiel will der Configuration Administrator Aktualisierungen am IP-Adressattribut aus dem Spectrum-MDR erlauben, doch der Name darf nicht mit *PROD* beginnen.

Gehen Sie wie folgt vor:

1. Erstellen Sie eine Verifizierungsrichtlinie.
2. Führen Sie die folgenden Schritte aus:
 - a. Geben Sie eine Sequenznummer an.
 - b. Wählen Sie "IP-Adresse" (alarm_id) als verwaltetes Attribut aus.
 - c. Wählen Sie "Rogue-Aktualisierung" als Ausrichtung aus.
 - d. Geben Sie **!PROD*** als CI-Namensmuster ein.

- e. Geben Sie **Spectrum** als MDR-Klassenmuster ein.
 - f. Wählen Sie "Attributaktualisierung zulassen" als Aktualisierungsverhalten aus.
3. Speichern Sie die Richtlinie.

Kapitel 17: Verwalten von MDRs

Dieses Kapitel beschreibt das Definieren von MDRs und Importdaten, das Zuordnen von CIs zurück zu ihrer Quelle, das Definieren von Startparametern, das Starten von Zurück-zur-Quelle-MDR und das Verwenden von MDRs zum Zuordnen und Anzeigen von föderierten CI-Informationen.

Dieses Kapitel enthält folgende Themen:

[Was ist ein MDR?](#) (siehe Seite 785)

[MDR Launcher](#) (siehe Seite 787)

[Definieren einer URL zum Starten eines MDR](#) (siehe Seite 788)

[Einrichten eines CA APM-MDR-Providers](#) (siehe Seite 790)

[Starten im Kontext von CA CMDB an CA APM](#) (siehe Seite 790)

[Eigenschaften von Configuration Items, die MDR-Zusammenschluss unterstützen](#) (siehe Seite 791)

[CA Cohesion ACM MDRs](#) (siehe Seite 793)

[Mit GRLoader](#) (siehe Seite 798)

[Namenskonventionen und Einschränkungen für Configuration Items](#) (siehe Seite 798)

[Namenskonventionen für system_name](#) (siehe Seite 799)

[Verwenden des CMDBf-Viewers](#) (siehe Seite 801)

[Aktualisieren von Metadatendateien für die CMDBf-Zuordnung](#) (siehe Seite 801)

Was ist ein MDR?

Die Configuration Management Database Federation (CMDBf), eine Arbeitsgemeinschaft mit Vertretern von CA, IBM, HP, Microsoft und anderen Unternehmen, definiert ein Management Data Repository (MDR) als etwas, das Informationen über Configuration Items sammelt.

Um die Beziehung zwischen einem MDR und seinen CIs herzustellen, gehen Sie beim Implementieren des MDR Launcher wie folgt vor:

1. Definieren Sie das MDR.
2. Definieren Sie die CIs, die auf dieses MDR verweisen.

Ein CI kann sich nicht auf ein nicht vorhandenes MDR beziehen. Sie können jedoch ein CI definieren, ohne seine MDR-Zuordnung zu definieren. Sie können die MDR-Informationen später während einer Aktualisierung hinzufügen oder ändern, um von den Fähigkeiten des MDR Launcher zu profitieren.

Das gleiche CI kann von mehreren MDRs erkannt werden. Nachdem das CI erkannt wurde, versucht jedes MDR, dieses zu verwalten. Ein MDR kann die folgenden Aktionen ausführen:

- Erkennen ausführlicher Attribute zum CI
- Versuchen, den CI-Zustand zu ändern

Beispiel: Ein von mehreren MDRs erkanntes CI

Ein CI wird sowohl von der Netzwerkmanagement-Software als auch von der Asset-Verwaltungssoftware erkannt.

- Die Netzwerkmanagement-Software verwaltet Informationen zur Netzwerkkonfiguration und Netzwerktopologie.
- Die Asset-Verwaltungssoftware enthält Informationen zu Kosten, Wertminderung, Lizenzierung und Wartungsverträgen für dieses spezifische CI.

MDR-Klassen und MDR-Namen

Ein IT-Unternehmen kann viele MDRs umfassen. Jedes MDR hat ein als *MDR-Namen* (*mdr_name*) bezeichnetes Kennzeichen. Da es üblich ist, dass ein MDR den Namen des Host-Servers als *mdr_name* verwendet, muss dem *mdr_name* eine *MDR-Klasse* (*mdr_class*) hinzugefügt werden. So kann jedes einzelne MDR eindeutig identifiziert werden, und mehrere MDRs können auf demselben Host-Server liegen.

CA Cohesion ACM ist ein Discovery-Tool für Unternehmen, das eng in CA CMDB integriert ist. Jedes CA Cohesion ACM MDR, das für CA CMDB definiert wurde, muss **Cohesion** als *mdr_class* aufweisen.

Hinweis: Weitere Informationen über CA Cohesion ACM finden Sie in der Online-Hilfe von CA Cohesion ACM. Informationen zur Integration von CA Cohesion ACM und CA CMDB finden Sie im *CA Cohesion ACM-Implementierungshandbuch*.

Wie ergänzt ein MDR CA SDM?

Ein MDR enthält in der Regel ausführlichere CI-Informationen als CA CMDB. Ein einzelnes MDR jedoch nimmt in der Regel keine anderen MDRs wahr. Auch die Beziehungen eines bestimmten CI zu anderen CIs werden vernachlässigt, vor allem, wenn diese in anderen MDRs enthalten sind. CA CMDB eignet sich besonders für die Verwaltung solcher Umgebungen, da sich das Programm darauf konzentriert, CIs unabhängig von ihrer MDR-Quelle zu verwalten.

CA CMDB ist nicht darauf ausgelegt, alle Attribute für alle CIs zu speichern. Stattdessen können Sie damit die wichtigsten Attribute zusammenfassen, um diese zentral zu verwalten. Attribute unter der Kontrolle von Change Management eignen sich hervorragend für die Einbindung in CMDB. Auf Attribute, die CA CMDB nicht verwaltet, können Sie mit der Funktion zum Starten von MDR zugreifen. Außerdem bietet CA CMDB den CMDBf-Viewer, der den Vergleich der Attribute dieses CI nebeneinander über mehrere CMDBs und MDRs ermöglicht.

Definition eines MDR für CA SDM

Auf der Registerkarte "Administration" können Sie ein MDR für CA CMDB definieren.

Bevor Sie ein CI in ein MDR importieren können, muss das MDR definiert werden. Versuche, ein föderiertes CI in ein nicht vorhandenes MDR zu importieren, schlagen fehl.

Hinweis: Anweisungen zum Definieren eines MDR finden Sie im *Implementierungshandbuch*.

MDR Launcher

Der MDR Launcher ist ein offenes Integrationstool, mit dem Sie Daten aus allen MDRs mit Hilfe einer Webseite ohne jeglichen Code anzeigen können. Mit dem MDR Launcher kann jeder, der ein CI anzeigt, zusätzliche Details zu diesem einsehen und dieses steuern (vorausgesetzt, das MDR unterstützt diese Kontrolle).

Im Folgenden sind einige Verwendungsmöglichkeiten des MDR Launcher zusammengefasst:

- CA Cohesion ACM von der Seite "Hardware.Server" aus starten, um eine Änderung zu überprüfen
- Eine Anbieter-Webseite vom Configuration Item-Detail "Klimaanlage" aus aufrufen, um Diagnoseinformationen und Incident-Meldungen einzusehen.
- Das Vertragsverwaltungssystem von einem Vertrags-Configuration Item aus starten, um Vertragsdetails einzusehen.
- Den CA-Service von einem SLA-CI aus starten, um Service Level Agreements einzusehen, bevor Änderungen vorgenommen werden
- CA Remote Control von einem Server-Configuration Item aus starten, um den Server zu übernehmen, damit Probleme diagnostiziert und beseitigt werden können.

Definieren einer URL zum Starten eines MDR

CA CMDB startet eine Webseitensitzung mit dem Quell-MDR über einen URL, um den MDR Launcher zu betreiben. Sie definieren die von CA CMDB verwendete URL.

So definieren Sie eine URL für ein MDR:

1. Klicken Sie auf die Registerkarte "Verwaltung".
2. Öffnen Sie im linken Bereich CA CMDB und anschließend die MDR-Management-Baumstruktur.
3. Klicken Sie auf "MDRs Liste".
Die Seite "Management Data Repository (MDR) - Liste" wird angezeigt.
4. Klicken Sie auf ein existierendes MDR (oder erstellen und speichern Sie ein neues).
Die Seite "MDR-Providerdefinition" wird angezeigt.
5. Klicken Sie auf "Bearbeiten".
Die Seite "MDR-Definition aktualisieren" wird angezeigt.
6. Vervollständigen Sie die folgenden Parameter:

Hostname

Gibt die Netzwerkadresse oder den DNS-Namen des Webserver an, auf dem Webseiten für das MDR liegen.

Port

Gibt die Port-Nummer an, die vom Webserver "Hostname" verwendet wird.

Pfad

Gibt den Pfad zur Webseite und die Seite selbst an.

Parameter

Gibt alle Parameter an, die zur Identifizierung des gewünschten Configuration Item für das MDR verwendet werden. CA CMDB stellt diese Informationen für das MDR bereit.

Benutzer-ID

Gibt die Benutzer-ID an, sofern einer gemeinsam genutzten Benutzer-ID der Zugriff auf MDR gewährt wird.

Shared Secret

Gibt Informationen an, die zwischen CA CMDB und dem MDR freigegeben sind. Für CA Cohesion MDRs muss der hier angegebene Wert mit dem Wert übereinstimmen, der in der CA Cohesion-Eigenschaftendatei für den Wert `com.cendura.security.oneclickauth.secret` angegeben ist.

CMDBf-Namespace

Gibt die föderierte Asset-ID ("`federated_asset_id`") an, die der Abfrage als lokale ID zugeordnet wird. Für CA CMDB ist dieser Wert "`http://cmdb.ca.com/r1`".

CMDBf Timeout

(Optional) Gibt das Zeitlimit für eine CMDBf-Endpunktabfrage an. Der Standardwert ist zehn (10) Sekunden.

CMDBf-ENDPUNKT

Gibt den Endpunkt des Abfrage-Service im MDR an. Erforderlich für CMDBf-Viewer und beim Abrufen aktualisierter MDR-Daten. Wenn Sie CA CMDB als einen MDR-Provider verwenden, ist der Wert "`http://cmdb_hostname:cmdb_port/axis/services/QueryPort`".

Speichern Sie die Definition.

Die URL ist damit definiert.

Hinweis: Zusätzlich kann die URL Ersetzungsvariablen enthalten, um das Configuration Item weiter an das MDR anzupassen. Weitere Informationen finden Sie im *Implementierungshandbuch*.

Einrichten eines CA APM-MDR-Providers

Sie können ein MDR einrichten, das als CA APM-Provider fungieren soll.

Gehen Sie wie folgt vor:

1. Klicken Sie auf der Registerkarte "Administration" auf "CA CMDB" > "MDR-Management" > "MDRs - Liste".
2. Klicken Sie auf "Neu erstellen", um das CA APM-MDR festzulegen.
Die MDR-Providerdefinition wird angezeigt.
3. Geben Sie die folgenden obligatorischen MDR-Provider-Informationen ein:
 - Schaltflächenname - Geben Sie "APM" oder anderen gültigen Schaltflächennamen an. Empfohlen wird der Schaltflächenname "APM".
 - MDR-Name - Geben Sie "APM" für CA Asset Portfolio Management r11.3.4 bzw. "ITAM" für CA APM r12.6 an.
 - MDR-Klasse - Geben Sie "GLOBAL" an.
 - Hostname - Gibt den CA APM-Servernamen mit Hilfe der Netzwerkadresse oder des DNS-Namens des CA APM-Webservers an.
 - URL für Starten im Kontext - Gibt `http://{hostname}:{port}/{path}?{parameters}` an und muss nicht geändert werden.

Auf dem MDR-Provider-Formular werden für den Pfad und die Parameterwerte automatisch die obligatorischen CA APM-Informationen für das Starten im Kontext angegeben.

4. Klicken Sie auf "Speichern".

Der CA APM-MDR-Provider ist nun eingerichtet.

Hinweis: Weitere Informationen zum MDR Launcher finden Sie im *Implementierungshandbuch*.

Starten im Kontext von CA CMDB an CA APM

Der MDR Launcher von CA CMDB unterstützt das Starten im Kontext mit CA APM, wenn CA APM und CA CMDB die gleiche MDB nutzen. Die CA CMDB-Benutzeroberfläche bietet auf der Registerkarte "Attribute" im CI-Detailformular eine Schaltfläche für das Starten im Kontext, wenn der Anwender eine spezielle CA APM-MDR-Providerdefinition erstellt.

Die CA APM-MDR-Definition umfasst alle Funktionen eines traditionellen MDR. Die CA CMDB-Funktion zur Versionskontrolle unterstützt ferner das Starten im Kontext direkt aus einem Attributprotokolleintrag, der mit jeder CA APM-Änderung verknüpft ist.

Wichtig! Im Unterschied zu anderen MDRs wird das CA APM-MDR automatisch mit jedem CI oder Asset verknüpft. Die MDR-Klasse "GLOBAL" und der MDR-Name "APM" werden verwendet, um das MDR für CA Asset Portfolio Management r11.3.4 zu identifizieren. Die MDR-Klasse "GLOBAL" und der MDR-Name "ITAM" dienen zum Identifizieren des MDR für CA APM-r12.6. Die Verwendung des CA APM-MDR ist uneingeschränkt mit anderen MDRs kompatibel, sogar für das gleiche CI.

Eigenschaften von Configuration Items, die MDR-Zusammenschluss unterstützen

Configuration Item-Eigenschaften (Attribute) identifizieren Assets für den MDR-Zusammenschluss.

Föderierte Anlagen-ID

Personen sind bei verschiedenen Organisationen unter verschiedenen Kennungen bekannt. Sie können anhand der folgenden Kennungen identifiziert werden:

- einmaliger Spitzname für Ihre engen Freunde
- Führerschein (einmalige ID zu Ihrer Person)
- Wehrdienstnummer (zum Beispiel ein Dienstaussweis)
- Sozialversicherungsnummer
- Steuernummer

Jede dieser eindeutigen Kennungen gehört zu Ihnen. Trotzdem ist jede Kennung nur dann gültig, wenn Sie damit dem entsprechenden Repository beschrieben werden.

Genauso kann ein CI mehrere Kennungen haben, die es mit seinen Quell-MDRs verknüpfen. Jedes Configuration Item wird mit Hilfe einer einzigen Kennung genau von einem MDR erkannt. Diese Kennung heißt *Föderierte Asset-ID*. Der Prozess, bei dem ein CI mit einem oder mehreren MDRs verknüpft wird, heißt *CI-Zuordnung*.

Die Zuordnung geschieht, wenn Configuration Items in die MDB geladen werden. Hierfür gibt es zwei Möglichkeiten:

- Definieren der CI-Zuordnung mit der Administrations-Benutzeroberfläche
- Laden der CIs mit Hilfe des GRLoader-Dienstprogramms

MDR-Name

Anhand des MDR-Namens wird das MDR beim Exportieren von Daten mit XML und GRLoader für CA CMDB identifiziert. Das MDR hat in der Regel eigene Namenskonventionen für seine Identifizierung. Meistens bestehen diese aus einer Kombination aus Hostservernamen plus einem identifizierenden Instanznamen oder einer identifizierenden Instanznummer. Da auf einem bestimmten Host nur ein MDR existiert, wird als MDR-Name oft der Hostservername festgelegt. **Für CMDBf-Viewer erforderlich.**

Wichtig! Der MDR-Name für CA Asset Portfolio Management Version 11.3.4 ist APM, und der MDR-Name für CA APM r12.6 ist ITAM. Beide Produkte werden unterstützt. Vor deren Implementierung sollten Sie aber die Produktverfügbarkeit unter "supportconnect.ca.com" überprüfen.

MDR Class

Die MDR-Klasse wird vom Kunden definiert, um MDRs zu gruppieren.

Hinweis: für eine CMDBf-Überprüfung wird eine MDR-Klasse von CMDBf benötigt.

Wichtig! Der MDR-Name muss zusammen mit der MDR-Klasse in Ihrem Unternehmen eindeutig sein.

MDR-Definition bei der Installation von CA Cohesion ACM

Für CA Cohesion ACM MDRs gelten die folgenden Voraussetzungen:

- Der in der MDR-Definition auf dem CA CMDB-Server angegebene "mdr_name" muss genau dem Wert des Attributs com.cendura.installation.name in der Datei "cendura.properties" auf dem CA Cohesion ACM-Zielservers entsprechen.
- CA Cohesion ACM MDRs müssen als MDR-Klasse "Cohesion" verwenden.
- Das MDR muss den Hostnamen und die Port-Nummer des CA Cohesion ACM-Servers angeben.

Bearbeiten Sie den folgende Abschnitt der Datei "cendura.properties", um den MDR Launcher auszuführen:

```
# -- Configure One-Click Authentication --
com.cendura.security.oneclickauth.secret=shared_secret
com.cendura.security.oneclickauth.scheme=
com.cendura.security.oneclickauth.user=user_id
```

Wichtig! Der in "cendura.properties" angegebene geheime Schlüssel muss mit dem *gemeinsamen geheimen Schlüssel* in der MDR-Definition übereinstimmen.

Der MDR Launcher meldet sich mit der in der Eigenschaftendatei angegebenen *userid* an und erbt ihre Sicherheitsattribute. Überprüfen Sie, ob dieser Benutzer über ausreichende Berechtigungen verfügt, um Funktionen wie z. B. Aktualisieren für die Attribute eines CIs zu verwenden.

Hinweis: Weitere Informationen zum Erstellen eines Benutzers, Festlegen von Sicherheitsoptionen für diesen und Anpassen der Eigenschaftendatei finden Sie im *CA Cohesion ACM-Implementierungshandbuch*.

CA Cohesion ACM MDRs

CA Cohesion ACM MDRs müssen vor dem Importieren von Daten von einem CA Cohesion ACM-Server definiert werden. Ein CA Cohesion ACM MDR muss als MDR-Klasse "Cohesion" angegeben.

Beispiel: Cohesion1-MDR-Definition

In der folgenden Cohesion1-MDR-Definition gibt die XML als MDR-Namen *cohesion_server* und als MDR-Klasse *Cohesion* an. Diese Werte sind für die zu importierenden CIs erforderlich.

Button Name

Cohesion1

MDR-Name

cohesion_server

MDR-Klasse

Cohesion

Aktiv?

Aktiv

Eigentümer

CMDBAdmin

Beschreibung

CA Cohesion ACM-Server in Chicago

Hostname

cohesion_server

Port

8090

Pfad

CAisd/html/cmdb_cohesion.html

Parameter

hostname={hostname}+port={port}+family={family}+name={name}+secret={password}+federated_asset_id={federated_asset_id}

userid

cohesion_userid

Shared Secret

Chicago01

Im Kontext zu startende URL

http://cmdb_hostname:8080/{path}?{parameters}

Da es sich um einen Cendura-Server handelt, sollten die oben genannten Werte zusätzlich mit den Werten in der Datei "cendura.properties" auf diesem Server übereinstimmen, wie das folgende Beispiel zeigt:

```
com.cendura.security.oneclickauth.secret=Chicago01
com.cendura.installation.name=cohesion_server
```

Sie können die Syntax der URL ändern, um mit besonderen Anforderungen umzugehen.

Manuelles Verknüpfen eines MDR mit einem CI

Sie können MDRs manuell mit einem CI verknüpfen, indem Sie die Option "Föderierte CI-Zuordnung" auf der CA CMDB-Registerkarte "Administration" verwenden. Diese befindet sich in der Baumstruktur unter "MDR-Management".

Bevor Sie ein CI mit einem MDR verknüpfen, gehen Sie wie folgt vor:

1. Erstellen Sie die MDR-Definition (sofern noch nicht vorhanden).
2. Erstellen Sie die CI-Definition (sofern noch nicht vorhanden).
3. Identifizieren Sie die eindeutige föderierte Asset-ID des CI, das Sie mit dem MDR verbinden möchten. Diese ID ist MDR-spezifisch, daher würde eine detaillierte Beschreibung den Rahmen dieses Handbuchs sprengen.

Hinweis: Weitere Informationen zur Identifizierung der föderierten Asset-ID finden Sie in der MDR-Dokumentation.

Automatischer Import aus CA Cohesion

Sie können CIs direkt aus CA Cohesion ACM importieren, indem Sie einen Bericht von CA Cohesion ACM ausführen, der Hostname, Port, Benutzer-ID und Kennwort für einen CA CMDB-Server festlegt. Solange das MDR in CA CMDB definiert ist, generiert CA Cohesion automatisch die XML zur Erstellung von CIs und Beziehungen mit den notwendigen Informationen zum Ausführen des MDR Launch auf einem CI. Der Bericht importiert die CIs automatisch in CA CMDB.

Hinweis: Weitere Informationen zum Exportieren von Configuration Items aus CA Cohesion ACM finden Sie in der Online-Hilfe, die Sie über die Registerkarte "Berichtsvorlagen" unter "Berichte" aufrufen können.

Zuordnung von CI zu MDR

Da jedes MDR ein `federated_asset_id` verwendet, um ein CI zu identifizieren, kann ein CI mit mehreren MDRs in Bezug gesetzt werden. Ein `federated_asset_id` muss nicht für alle MDRs eindeutig sein. Allerdings muss es innerhalb eines MDR eindeutig sein. Jedes MDR muss eine eindeutige MDR-Klasse und einen eindeutigen MDR-Namen haben.

Wichtig: Wenn ein CI oder ein MDR-Provider inaktiv wird, werden alle mit dem CI oder MDR-Provider verknüpften föderierten CI-Zuordnungen ebenfalls inaktiv.

Verfahren Sie nach der Erstellung einer MDR-Datenproviderdefinition wie folgt:

1. Erstellen Sie ein CI in CMDB, das auf einen MDR verweist.
2. Überprüfen Sie, ob die MDR-Definition funktioniert.

Da nur im Kontext eines CI gestartet werden kann, ist es nicht möglich, die MDR-Definition direkt zu testen, denn sie steht in keinem CI-Kontext.

Sie können die Liste "Föderierte CI-Zuordnung" auf der Registerkarte "Administration" im Knoten "Föderierte CI-Zuordnung" anzeigen.

Um ein Configuration Item in einem bestimmten MDR-Kontext einsehen zu können, klicken Sie auf die Schaltfläche "MDR Launch".

Das Ziel-MDR wird im Kontext des geöffneten Konfigurationselements gestartet.

Beispiel: Configuration Item-Zuordnung

1. Klicken Sie auf die Registerkarte "Verwaltung".
2. Navigieren Sie zu "MDR-Management" > "Föderierte CI-Zuordnung".

Die Liste der Föderierten Configuration Item-Zuordnungen wird angezeigt.

3. Geben Sie "server1" in das Feld "CI-Name" ein.

Die folgenden Spalten zeigen die Werte:

Föderierte Anlagen-ID

1000234

1000235

Name des Konfigurationselements

Server1

Server1

MDR-Provider

Cohesion1

Cohesion2

Aktiv

Aktiv

Aktiv

Sowohl der Cohesion1-MDR-Provider als auch das Cohesion2-MDR-Provider wissen von der Existenz von server1. Das Beispiel zeigt, dass beide Provider unabhängig voneinander dem Server eine eindeutige ID zugeordnet haben.

4. Klicken Sie auf den CI-Namen "server1".

Die Seite "server1 Configuration Item - Detail" wird mit den Startschaltflächen "Cohesion1" und "Cohesion2" angezeigt.

5. Klicken Sie auf eine der Schaltflächen zum Starten eines MDR-Providers.

Daraufhin werden weitere Details zur CI-Familie angezeigt.

Verwalten der MDR-Definition

Die Verwaltung von MDR-Definitionen ist ein flexibler Prozess. Sie können die Parameter in einer MDR-Definition sogar ändern, wenn CIs darauf verweisen. Zum Beispiel können Sie den Schaltflächennamen, den Hostnamen, die Benutzer-ID, den gemeinsamen geheimen Schlüssel und andere Einstellungen ändern, nachdem das MDR definiert und die CIs geladen wurden.

CA Cohesion ACM-Bericht

CA Cohesion ACM bietet eine Möglichkeit zum Planen von wiederkehrenden Berichten. Mit dieser Option wird es einfacher, CMDB mit den Daten im CA Cohesion ACM-MDR zu synchronisieren. Häufige Fehler wie ungültige Kennwörter (weil das Kennwort geändert wurde oder abgelaufen ist) können einen erfolgreichen Datenimport verhindern. Aktivieren Sie die Option "Benachrichtigung" im CA CMDB-Exportbericht in CA Cohesion ACM, um über Fehler unterrichtet zu werden, die während der Datenausführung im Hintergrund des Datenimportvorgangs auftreten können. Wenn ein Importfehler auftritt, erhalten Sie eine E-Mail-Benachrichtigung. Wenn Sie den Cohesion-Bericht als geplante Aufgabe im Hintergrund laufen lassen, ist es ratsam, die Option "Benachrichtigung" zu aktivieren.

Hinweis: Informationen zum Planen der regelmäßigen Ausführung des CA CMDB-Exportberichts finden Sie im *CA Cohesion ACM-Produkthandbuch*.

Mit GRLoader

Wenn Sie GRLoader verwenden, um ein CI zu laden, müssen Sie die folgenden Felder in der XML-Datei ausfüllen, damit der MDR startet:

- <mdr_class>
- <mdr_name>
- <federated_asset_id>

Die Werte für <mdr_name> und <mdr_class> in der XML-Datei müssen mit den Werten in der MDR-Definition übereinstimmen.

Wichtig! Der MDR-Name und die MDR-Klasse müssen mit Hilfe der CA CMDB-Verwaltungsoberfläche definiert werden, bevor CIs, die auf das MDR verweisen, importiert werden können. Wenn das MDR nicht in der XML definiert ist, wird das CI nicht importiert.

GRLoader unterstützt das Importieren von CIs und CI-Beziehungen aus Kalkulationstabellen im XLS- und XLSX-Format. Um CI-Daten in CA SDM zu laden, müssen Sie die Quelldaten als XML-Dateien oder Microsoft-Excel-Kalkulationstabellen formatieren.

Hinweis: Weitere Informationen zur Verwendung von GRLoader zum Laden von Kalkulationstabellendaten finden Sie im *technischen CA CMDB-Referenzhandbuch*.

Namenskonventionen und Einschränkungen für Configuration Items

Für Configuration Items gelten folgende Namenskonventionen und Einschränkungen:

- Name des Konfigurationselements

Dies ist der gängige Name oder Anzeigename, der in allen CI-Listen verwendet wird. Die Gesamtlänge des Namens darf 255 Zeichen nicht überschreiten. Der CI-Name muss nicht einmalig sein, es wird jedoch empfohlen, einen global einmalig CI-Namen zu wählen. In Situationen in denen der Name von einem MDR bestimmt wird, ist es ratsam, dass MDR-Administratoren beim Ausfüllen dieses Feldes auf Lesbarkeit achten.
- Software-Configuration Items

Befolgen Sie bei Drittanbietersoftware die gleichen Namenskonventionen für CIs wie für die Namen, die Sie manuell auf der Registerkarte "Administration" erstellen. Durch Abstimmen der Namenskonventionen können von CA Cohesion ACM erkannte CIs mit den manuell erstellten CIs abgeglichen werden. Wenn diese Konvention nicht eingehalten wird, besteht die Möglichkeit, mehrere CIs zu erstellen, auch wenn nur eine Softwareinstanz läuft.

- Verwenden des Attributs "Systemname"

Das Attribut "Systemname" verknüpft ein *einzelnes* Configuration Item (CI) eindeutig mit einem bestimmten Hostnamen.

Wenn mehrere CIs importiert werden, die denselben Systemnamen als ein vorhandenes CI angeben, wird durch die Abstimmung sichergestellt, dass das Ergebnis nur ein CI enthält.

Beispiel

Die folgenden Ausgabezeilen zeigen die Erstellung eines Server-CI (Provider), eines Software-CI (abhängig) und eine Ausführungsbeziehung (*runs*) zwischen diesen. Die entstehende Beziehung stellt einen Server dar, auf dem Apache-Software ausgeführt wird.

```
CI: Name: Server1      Class: Server  Systemname: Server1
CI: Name: Apache1     ON Server1    Class: Software
Beziehung: Server1 führt Apache1 aus  AUF Server1
```

Namenskonventionen für system_name

Für Software-CIs und alle MDRs werden die folgenden Benennungsstandards empfohlen, damit andere MDRs problemlos mit CA Cohesion ACM und miteinander integriert und CIs richtig abgeglichen werden können. CA Cohesion ACM folgt den gleichen Standards.

System_name

Identifiziert Software-CIs eindeutig. Geben Sie beim Definieren einer Beziehung, die ein Software-CI umfasst, den gleichen system_name wie in dieser CI-Definition an. Wenn mehrere Instanzen derselben Softwareversion im Verzeichnis auf denselben Hostnamen installiert sind, muss der system_name geändert werden, so dass er eindeutig ist. Die Gesamtlänge vom system_name darf 255 Zeichen nicht überschreiten, da es sonst zu fehlerhaften Daten kommen kann.

System_name muss eine eindeutige Kennung für diese Softwareinstanz auf einem einzelnen Host sein.

Verwenden Sie die folgende Syntax:

hostname | softwarename | version | business-application

Senkrechter Strich (|)

Trennt die verschiedenen Felder in der Verkettung der Syntax, damit der Benutzer die Suchfunktion verwenden kann.

hostname

Gibt den Hostnamen auf, auf dem die Software liegt.

softwarename

Gibt einen allgemeinen Namen für die Software an.

version

Gibt die Version der Software an (falls verfügbar).

business-application

Gibt eine eindeutige Kennung für diese Softwareinstanz auf *hostname* an. Wenn die Softwareinstanz mit einer Geschäftsanwendung oder einem Service verknüpft ist, trägt der Kennzeichner den Namen dieses Service. Wenn Sie die *Geschäftsanwendung* nicht ermitteln können, können Sie die Software anhand des Installationsverzeichnisses identifizieren. Wenn die Gesamtlänge dieses Feldes 255 Zeichen überschreitet, verkürzen Sie sie mit Ellipsen (...) auf eine Gesamtlänge von maximal 255 Zeichen.

Beispiele: Anwenden der Funktion "Benutzeroberfläche-Suche"

Mit der Funktion "Benutzeroberfläche-Suche" können Sie Software-Configuration Items suchen, wie die folgenden Beispiele zeigen:

Anwendungsfall	Name	System_name
Alle Software-Configuration Items auf dem Host finden	xxx	Xxx%
Alle Softwareinstanzen finden	yyy	yyy%
Alle Softwareinstanzen finden	yyy Version 123.0	yyy% % % 123.0%

In der Ergebnisliste der oben genannten Suche sieht der Benutzer nur das Feld "Name".

mac_address	Null.	- Ungeeignet für Software
asset_num	Null	- Ungeeignet für Software
serial_number	Null	- Ungeeignet für Software
dns_name	Null	- Ungeeignet für Software

Verwenden des CMDBf-Viewers

CA SDM stellt den CMDBf-Viewer bereit, um die Ergebnisse der CI-Föderation in den MDRs anzuzeigen. Klicken Sie auf einer CI- Detailseite (oder in der CI-Liste in dem CI-Kontextmenü) auf den CMDBf-Viewer, um die CI-Attribute der föderierten CMDBs und MDRs parallel anzuzeigen. Auf der Seite der föderierten Ansicht können Sie auf "Abrufen" klicken, um die Information der föderierten MDRs zu aktualisieren. Zur besseren Lesbarkeit können CA CMDB-Metadatendateien MDR-Attributnamen und CA CMDB-Attributnamen abstimmen.

Hinweis: Diese Funktion erfordert MDRs, die Abfragen unterstützen. Konfigurieren Sie die MDR-CMDBf-Endpunkte entsprechend, um ihre Ergebnisse in der föderierten Ansicht anzuzeigen. Weitere Informationen finden Sie im *Implementierungshandbuch*.

Wenn das CI keine föderierten Daten aufweist, zeigt der Viewer nur CA CMDB-Attribute an.

Aktualisieren von Metadatendateien für die CMDBf-Zuordnung

Um die Lesbarkeit von Attributsvergleichen zu verbessern, können Sie CA CMDB-Metadatendateien verwenden, um von MDR-Attributnamen in CA CMDB-Attributnamen zu übersetzen. Für alle MDR-Attribute, für die keine CA CMDB-Zuordnung existiert, zeigt die föderierte Ansicht den vom MDR gesendeten Attributnamen an. Metadaten können für CMDBf-Datenanbieter definiert werden, um die folgenden Vorgänge auszuführen:

- Anzeigen von MDR-Attributwerten unter Verwendung von CA CMDB-Attributnamen.
- Verhindern, dass MDR-Provider-Attribute in der föderierten Ansicht angezeigt werden.
- Definieren von MDR-Provider-Attributen, die keine CA CMDB-Entsprechungen haben.

Sie definieren Metadaten, indem Sie die Datei "cmdb_metadata_federation_viewer_site_attr.html" verwenden. Diese Datei enthält Anweisungen zur Aktualisierung der Datei. Metadaten können sich auf alle CMDB-Familien (übliche Attribute) oder familienspezifische Attribute beziehen.

Um externe MDR-Attributnamen CA CMDB-Beschriftungen zuzuordnen, aktualisieren Sie das entsprechende Formular "cmdb_metadata_extensionable.html". Verwenden Sie hierfür die folgenden Felder im Makro "cmdbmetadata":

- `mdr_attr` – Der Name des zu übersetzenden MDR-Attributs.
- `mdr_name` – Der Name des MDR, der übersetzt wird. Reguläre Ausdrücke werden unterstützt.

Beispiel: Zuordnen von Attributen

Die folgenden drei Metadatenanweisungen definieren Metadaten, die das CA CMDB-Attribut "phys_mem" mit dem Provider-Attribut "mdr_memory" für alle Provider mit dem Namen "myMdr" gleichsetzen. Außerdem wird "physical_memory" mit "phys_mem" für alle anderen Provider gleichgesetzt.

```
<macro name=cmdbMetadata attr="phys_mem" provider_attr="mdr_memory"
provider_name="myMdr">
<macro name=cmdbMetadata attr="phys_mem" provider_attr="mdr_memory"
provider_name_regexp="MDR.*">
<macro name=cmdbMetadata attr="phys_mem" provider_attr="physical_memory"
provider_name_regexp=".*">
```

Beispiel: Ausblenden von Attributen

Die folgende Metadatenanweisung blendet das MDR-Provider-Attribut "widget_cost" für alle Provider mit dem Namen "myMdr" aus.

```
<macro name=cmdbMetadata hide_provider_attr="YES" provider_attr="widget_cost"
provider_name="myMdr">
```

Beispiel: Einrichten einer Attributbeschriftung

Die folgende Metadatenanweisung definiert den Attributnamen "ext_mem_capacity" unter Verwendung der Beschriftung "External Memory Capacity" unter der Kategorie "Attribute" im CMDBf-Viewer.

```
<macro name=cmdbMetadata attr="ext_mem_capacity" category="Attributes"
heading="External Memory Capacity" help="Total external memory">
```

Weitere Informationen:

[Anzeigen von MDR-Attributwerten mit CA CMDB-Attributnamen](#) (siehe Seite 803)

[Ausblenden von Attributen des MDR-Providers](#) (siehe Seite 804)

[Definieren von MDR-Attributen ohne CA CMDB-Entsprechungen](#) (siehe Seite 805)

[Definieren von Metadaten des CMDBf-Datenanbieters](#) (siehe Seite 805)

Anzeigen von MDR-Attributwerten mit CA CMDB-Attributnamen

Metadaten können eine Verbindung zwischen MDR-Provider-Attributen und CA CMDB-Attributen herstellen, so dass sie zusammen angezeigt werden, um Unterschiede zu sehen und Beschriftungen gemeinsam zu nutzen. Standardmäßig werden MDR-Attribute ohne Zuordnung in dem Viewer als **Nicht in CMDB** angezeigt.

cmdbMetadata-Makroargumente, um ein CA CMDB-Attribut mit einem MDR-Provider-Attribut gleichzusetzen, umfassen folgende Elemente:

- attr – CA CMDB Attributname
- provider_attr – Attributname des MDR-Providers
- provider_name – Name des MDR-Providers
- provider_name_regexp – regulärer Ausdruck des MDR-Providernamens

provider_name oder provider_name_regexp sind erforderlich.

Beispiel: Verknüpfen Sie MDR-Attribute mit CA CMDB-Attributnamen

Je eine der weiter unten aufgeführten drei Metadatenanweisungen führt je eine der drei folgenden Aktionen aus (in der aufgeführten Reihenfolge):

- Gleichsetzen des CA CMDB-Attributs "phys_mem" mit dem Provider-Attribut "mdr_memory" für alle Provider mit dem Namen "myMdr".
- Gleichsetzen des CA CMDB-Attributs "phys_mem" mit dem Provider-Attribut "mdr_memory" für alle Providernamen, die mit "MDR" anfangen.
- Gleichsetzen von "physical_memory" mit "phys_mem" für alle anderen Provider.

```
<macro name=cmdbMetadata attr="phys_mem" provider_attr="mdr_memory"
provider_name="myMdr">
<macro name=cmdbMetadata attr="phys_mem" provider_attr="mdr_memory"
provider_name_regexp="MDR.*">
<macro name=cmdbMetadata attr="phys_mem" provider_attr="physical_memory"
provider_name_regexp=".*">
```

Ausblenden von Attributen des MDR-Providers

Einige MDR-Provider-Attribute müssen nicht in der föderierten Ansicht angezeigt werden. Metadaten von einem MDR-Provider können für einen bestimmten MDR-Provider ausgeblendet werden. Diese Option ist nur für MDR-Provider-Attribute verfügbar, aber nicht für CA CMDB-Attribute.

cmdbMetadata-Makroargumente zum Ausblenden eines Provider-Attributs umfassen die folgenden Elemente:

- `hide_provider_attr` - "YES" – Blendet das MDR-Provider-Attribut aus
- `provider_attr` – Attributname des MDR-Providers
- `provider_name` – Name des MDR-Providers
- `provider_name_regexp` – regulärer Ausdruck des MDR-Providernamens

`provider_name` oder `provider_name_regexp` sind erforderlich.

Beispiel: Blenden Sie ein MDR-exklusives Attribut aus

Die folgende Metadatenanweisung kann verwendet werden, um das MDR-Provider-Attribut "widget_cost" für alle Provider mit der Bezeichnung "myMdr" auszublenden.

```
<Macro name=cmdbMetadata hide_provider_attr="YES" provider_attr="widget_cost"
provider_name="myMdr">
```


Definieren von MDR-Attributen ohne CA CMDB-Entsprechungen

Sie können Beschriftungen und Hilfetext für MDR-Provider-Attribute definieren, die keinen anderen CA CMDB-Attributen entsprechen. Attribute werden in der föderierten Ansicht mit "Nicht in der Familie" beschriftet.

cmdbMetadata-Makroargumente zur Definition eines MDR-Provider-Attributs umfassen die folgenden Elemente:

- attr – CA CMDB Attributname
- category – Name der Kategorie, wo das Attribut angezeigt wird
- heading – Kopfzeilenbeschriftung für das Attribut
- help – Kurzbeschreibung des Attributs

Beispiel: Definieren Sie ein MDR-exklusives Attribut

Die folgende Metadatenanweisung definiert den Attributnamen "ext_mem_capacity" unter Verwendung der Beschriftung "External Memory Capacity" unter der Kategorie "Attribute" in der föderierten Ansicht.

```
<macro name=cmdbMetadata attr="ext_mem_capacity" category="Attributes"
heading="External Memory Capacity" help="Total external memory">
```

Definieren von Metadaten des CMDBf-Datenanbieters

In der zusammenfassenden Ansicht können Sie bestimmen, wie Daten dargestellt werden.

So definieren Sie Metadaten für CMDBf-Viewer

1. Verwenden Sie Web Screen Painter, um die Datei "cmdb_metadata_federation_viewer_site_attr.html" zu öffnen.
2. Entscheiden Sie, welche Metadatenänderungen erforderlich sind.

Hinweis:In der Datei sind Vorlagen verfügbar.

3. Kopieren Sie die gewünschte Vorlage und ersetzen Sie die erforderlichen Argumente entsprechend den Anweisungen in der Datei.
4. Speichern und veröffentlichen Sie die Änderungen.

Kapitel 18: Change Management

Dieses Kapitel enthält folgende Themen:

[Change Management in CA SDM](#) (siehe Seite 807)
[Change-Management-Komponenten](#) (siehe Seite 808)
[Anzeigen des Change-Kalenders](#) (siehe Seite 809)
[CAB-Zuständigkeiten](#) (siehe Seite 810)
[Zuständigkeiten des Change Managers](#) (siehe Seite 811)
[Definieren der Aufgaben für die Rolle des Change Managers](#) (siehe Seite 813)
[Change-Kategorien, Status und Risikoebenen](#) (siehe Seite 814)
[Anzeigen des Change-Scoreboards](#) (siehe Seite 815)
[Definieren von gespeicherten Abfragen für Changes](#) (siehe Seite 815)
[Konfigurieren von Change Manager-Optionen](#) (siehe Seite 817)
[Change-Kalender](#) (siehe Seite 817)
[So planen Sie Changes:](#) (siehe Seite 830)
[So planen Sie Change-Fenster:](#) (siehe Seite 835)
[Konfliktanalyse und Konflikterkennung](#) (siehe Seite 839)
[CA Workflow-Visualisierung](#) (siehe Seite 840)
[Change-Management-Prozessdefinition für CA Workflow](#) (siehe Seite 842)
[CAB-Konsole und Berichterstattung](#) (siehe Seite 865)
[Risikobewertung](#) (siehe Seite 871)
[Auswirkungs-Explorer](#) (siehe Seite 875)

Change Management in CA SDM

Change Management für CA SDM bietet eine Reihe von Funktionen für Change Manager, Change-Koordinatoren und Mitglieder des Change Advisory Boards (CAB) zur Koordinierung der Überprüfung und Genehmigung der Changes für CI-Komponenten und -Services. Change Manager können zum Beispiel alle Änderungen an CI-Komponenten und -Diensten überprüfen und genehmigen, um sicherzustellen, dass keine neuen Sicherheitsrisiken in die Produktionsumgebung eingeführt werden. Der Change Manager leitet das CAB und ist für die endgültige Genehmigung der Change Requests verantwortlich.

Change Management umfasst die folgenden Funktionen:

- Nachverfolgen der ITIL-Prozesse, die IT-Changes mit dem Incident-/Problem-Management verknüpfen
- Anzeigen von Service-Management-Informationen für ein CI; zum Beispiel, die Anzahl von für ein CI protokollierten Changes, Change-Implementierungsdaten und mehr
- Erkennen von Konflikten, wenn mehrere Changes gleichzeitig Änderungen an denselben CIs erfordern

- Erstellen und Speichern von Change-Fenstern im Change-Kalender
- Erstellen eines Change in der Kalenderansicht
- Bewerten der Risiken, die mit einem Change in Verbindung stehen

Hinweis: Ausführlichere Informationen zu Change Management-Verfahren finden Sie unter "Change Management" in der *Online-Hilfe*.

Change-Management-Komponenten

Change Management umfasst die folgenden Komponenten:

Change-Kalender

Zeigt eine [graphische <Ansicht von Change-Events](#) (siehe Seite 817), einschließlich aller geplanten, fehlgeschlagenen und laufenden Change Requests für CIs und Services in einer konfigurierbaren [Kalenderansicht](#) (siehe Seite 830), an. Der Kalender zeigt darüber hinaus Ausfallfenster an, in denen keine Changes erfolgen dürfen. Anwender können in den Tages-, Wochen- und Monatsansichten über das Kontextmenü einen Change erstellen. Diese Funktion wird von Change Managern, Level 2-Analysten und CAB-Mitgliedern verwendet.

Change-Scheduler

Zeigt [geplante Zeiträume](#) (siehe Seite 836) im Change-Kalender an, in denen CI-Changes stattfinden können oder nicht stattfinden können. Der Change-Manager verwendet diese Funktion, um Change-Ablaufpläne und CI-Zuordnungen während des Zeitraums anzuzeigen und zu erstellen.

Konfliktanalyse und Konflikterkennung

Analysieren Sie Changes, um potenzielle Implementierungskonflikte zu bestimmen, die das Risiko eines Fehlers erhöhen könnten. Diese Funktion wird vom Change Manager verwendet.

Workflow-Visualisierung

Zeigt den Genehmigungsprozess für Change Requests an. Diese Funktion wird vom Change Manager verwendet.

CAB-Konsole und Berichterstattung

Zeigt ein [Dashboard](#) (siehe Seite 865) an, das schnelle Online-Genehmigungen der Changes, die eine CAB-Genehmigung erfordern, ermöglicht.

In CA SDM kann der Change Manager Berichte mit Details über die vorgeschlagenen Change Requests für die CAB-Überprüfung generieren und diese Berichte elektronisch an alle CAB-Mitglieder verteilen.

Hinweis: Anwender mit geeigneten Privilegien können vordefinierte Kompatibilitäts-, Prognose-, Trend- und Volumenberichte für das Change Management in BusinessObjects Infoview mit CA Business Intelligence anzeigen.

Risikobewertung

Bietet die Möglichkeit, an jeden abgesendeten Change Request Risikoanalysen anzuhängen. Mithilfe der Option "Risikoumfrage" können Sie Umfragen erstellen, um Risiken zu bewerten und mit Change-Kategorien zu verknüpfen. Die Risikoumfrage führt eine Reihe von einfachen und Multiple-Choice-Fragen auf.

Auswirkungs-Explorer

Zeigt CI-zu-CI Beziehungen für CIs an, die an einen Change angehängt sind. Auswirkungs-Explorer wird auf der Seite "Change-Detail" gestartet, um die [Auswirkungsanalyse](#) (siehe Seite 875) auf Anfrage zu ermöglichen. Diese Funktion wird vom Change Manager verwendet.

Change-Verifizierung

Stellt sicher, dass Änderungen richtig ausgeführt werden und keine unautorisierten Änderungen auftreten, damit die CMDB eine wirklichkeitsgetreue und aktuelle Darstellung aller verwalteter CIs enthält.

Anzeigen des Change-Kalenders

CA SDM kann verschiedene Change Management-Funktionen (entsprechend den Standards ITIL und COBIT) starten, über die Changes angezeigt und erstellt werden können, nach dem ein Tag im *Change-Kalender* ausgewählt wurde. Neue Changes werden automatisch für den ausgewählten Tag geplant.

Der Change-Kalender berichtet über Konflikte, Fehlanpassungen, und potenzielle Risiken bei geplanten Changes, Changes und CIs. Informieren Sie sich mit Hilfe des Kalenders über bevorstehende Changes, ihre möglichen Auswirkungen auf die IT-Umgebung, usw.

So zeigen Sie den Change-Kalender an:

1. Klicken Sie auf die Registerkarte "Change-Kalender".
Die Filterfelder von "Change-Kalender" werden angezeigt.
2. Vervollständigen Sie die Suchfelder, um eine Kalenderansicht anzuzeigen, die den Ablaufplan für die Changes von Interesse zeigt.
3. Klicken Sie auf "Suche".

Im Change-Kalender werden Informationen angezeigt, die Ihren Suchkriterien entsprechen.

CAB-Zuständigkeiten

Das Change Advisory Board (CAB) koordiniert die Überprüfung und die Genehmigung bzw. Ablehnung der Changes für CI-Komponenten und -Services. CAB-Mitglieder sind verantwortlich für folgende Aufgaben:

- Überprüfen aller wesentlichen Changes an Produktionssystemen
- Teilnahme an allen relevanten CAB-Besprechungen, die vom Change Manager als obligatorisch eingestuft wurden
- Überprüfen aller abgesendeten Change Requests auf ihre Auswirkungen, die für die Implementierung erforderlichen Ressourcen und die laufenden Kosten.
- Beteiligung an der Planung und Koordination des Change-Kalenders
- Sicherstellen, dass alle Changes angemessen bewertet und priorisiert werden
- Beteiligung an den Überprüfungen nach Abschluss der Installation

Weitere Informationen:

[Funktionsweise der CAB-Prozessdefinitionen](#) (siehe Seite 810)

[Zuweisen von Mitgliedern zur CAB-Gruppe](#) (siehe Seite 811)

Funktionsweise der CAB-Prozessdefinitionen

Die CAB ist dafür verantwortlich, alle größeren Changes an Produktionssystemen zu überprüfen. CAB-Mitglieder werden darüber benachrichtigt, dass ein Change Request ihre Genehmigung erfordert, und sie führen folgende Schritte aus:

1. Sie lassen alle Change Requests auflisten, die das CAB überprüfen muss
2. Sie öffnen die CAB-Konsole und zeigen der Informationen an, die im Request enthalten sind
3. Sie prüfen Geschäftsrechtfertigung, Implementierungsplan, Configuration Items und die begleitende, mit dem Request verknüpfte, Dokumentation und entscheiden dann über die Genehmigung bzw. die Ablehnung
4. Sie genehmigen den Change oder lehnen ihn ab. Der nächste Change in der Liste wird dann automatisch angezeigt.

Die Person, die den Change anfordert, wird automatisch darüber benachrichtigt, dass der CAB-Status für den Change Request aktualisiert wurde.

Weitere Informationen:

[CAB-Zuständigkeiten](#) (siehe Seite 810)

Zuweisen von Mitgliedern zur CAB-Gruppe

Über die Seite "Mitglieder aktualisieren" können Sie einer CAB-Gruppe Mitglieder zuweisen.

So weisen Sie der CAB-Gruppe Mitglieder zu:

1. Wählen Sie auf der Seite "Gruppe - Detail" die Registerkarte "Mitglieder".
2. Klicken Sie auf "Mitglieder aktualisieren".
Die Seite "Kontakte - Suche" wird angezeigt.
3. Geben Sie die Suchkriterien ein, um die gewünschten Kontakte anzuzeigen, und klicken Sie auf "Suchen".
Die Seite "Mitglieder aktualisieren" wird angezeigt und führt die Kontakte auf, die den Suchkriterien entsprechen.
4. Wählen Sie aus der Liste auf der linken Seite die Kontakte aus, die Sie dieser Gruppe zuweisen möchten. Halten Sie die STRG-Taste gedrückt, während Sie mit der linken Maustaste klicken, um mehrere Elemente auszuwählen.
5. Wenn Sie alle gewünschten Kontakte ausgewählt haben, klicken Sie auf die Auswahl Schaltfläche (≥>).
Die ausgewählten Kontakte werden zur Mitgliederliste auf der rechten Seite verschoben.
6. Klicken Sie auf "OK".
Die Seite "Gruppe - Detail" wird angezeigt. Die ausgewählten Kontakte sind in der Registerkarte "Mitglieder" aufgeführt.

Zuständigkeiten des Change Managers

Change Manager sind für den gesamten Change Management-Prozess im Unternehmen sowie für die letzte Genehmigungsstufe von Changes zuständig. Change Manager generieren Berichte über die Analyse der Change Management-Metriken und übernimmt folgende Aufgaben:

- Change Manager überprüfen Change Requests und fügen nach Bedarf die zu benachrichtigenden Personen und die Genehmigenden hinzu
- Change Manager vereinfachen die Lösung von Issues, z. B. indem sie Konflikte erkennen und bestehende Konflikte im Kalender planen

- Change Manager überprüfen die Installation sowie die Backout- und Fallback-Pläne auf Zugriffsmöglichkeiten und Korrektheit.
- Change Manager sind sich der Risiken von Changes bewusst und stellen sicher, dass Changes die geeignete Risikoebene erhalten
- Change Manager überwachen Changes im Hinblick auf ihre jeweiligen Bereiche, um sicherzustellen, dass sie den technischen Anforderungen des Change Management genügen.
- Change Manager vertreten ihre jeweiligen Bereiche und kommunizieren die Auswirkungen hoch riskanter Changes bei den wöchentlichen CAB-Besprechungen
- Change Manager vermitteln bei Überprüfungen (bei abgeschlossener Installation für Probleminstallationen) und fehlgeschlagenen Changes
- Change Manager dienen als Eskalationsstelle für Anforderer, zu benachrichtigende Personen, Genehmigende, Implementierer und Support-Gruppen

Weitere Informationen:

[Funktionsweise der Rolle des Changes Managers](#) (siehe Seite 812)

Funktionsweise der Rolle des Changes Managers

Change Manager sind verantwortlich für die Überwachung von Changes an der Betriebsumgebung und müssen sicherstellen, dass sich die Mitarbeiter an die Geschäftsrichtlinien und -Prozesse halten. Mit dem Change-Kalender kann die Lösung von Issues wie beispielsweise Change-Konflikten ermöglicht werden, indem bestimmte Ausfalltage und Zeiträume ohne Aktivität geplant werden, während derer ein CI oder ein Satz von CIs geändert werden kann. Change Manager können außerdem folgende Schritte ausführen:

1. Beaufsichtigen der CAB-Konsole, über die schnelle Online-Genehmigungen von Changes und Change Requests verwaltet werden
2. Organisieren von CABs mit für die entsprechenden Changes geeigneten Mitgliedern und das Durchführen regelmäßig geplanter CAB-Besprechungen zur Überprüfung eingehender Changes
3. Erstellen von Berichten mit Details über die vorgeschlagenen Change Requests für die CAB-Überprüfung und das elektronische Verteilen der Berichte an alle CAB-Mitglieder
4. Durchführen von Echtzeit-Überprüfungen aller Change Requests und Aktualisieren der Datensätze mit den während den CAB-Besprechungen gefällten CAB-Entscheidungen
5. Verwendung von BusinessObjects Infoview zur Verwaltung von Kompatibilitäts-, Prognose-, Trend- und Volumenberichten und zur Erstellung von Berichten auf Anfrage

6. Vertreten des eigenen Bereichs und Kommunizieren der Auswirkungen hoch riskanter Changes bei den wöchentlichen CAB-Besprechungen
7. Überprüfen der Risiken von Changes und Sicherstellen, dass Changes eine geeignete Risikoebene zugewiesen wird.

Definieren der Aufgaben für die Rolle des Change Managers

Sie können Aufgaben für die Rolle des Change Managers definieren.

So definieren Sie Aufgaben für die Rolle des Change Managers:

1. Wählen Sie auf der Registerkarte "Administration" die Optionen "Sicherheits- und Rollenmanagement" > "Rollenmanagement" > "Rollen - Liste" aus.

Die Seite "Rollenliste" wird angezeigt.

2. Wählen Sie die Rolle "Change Manager" aus.

Die Seite "Rolle - Detail für den Change Manager wird angezeigt.

3. Klicken Sie auf "Bearbeiten".

Die Seite "Rolle aktualisieren" für den Change Manager wird angezeigt.

4. Konfigurieren Sie mit den folgenden Registerkarten und Feldern Aufgaben und Zugriffsberechtigungen für die Rolle des Change Managers:

- Autorisierung
- Funktionszugriff
- Web-Schnittstelle
- Knowledge Management
- KT-Dokumentsichtbarkeit
- Registerkarten
- Berichts-Webformulare
- 'Los'-Ressourcen
- Mandanten-Lesezugriff
- Mandanten-Schreibzugriff

5. Klicken Sie auf "Speichern" und "Fenster schließen".

Der Datensatz für die Rolle des Change Managers wurde aktualisiert.

Hinweis: Weitere Informationen über die Registerkarten, die auf der Seite "Rolle - Detail" des Change Managers angezeigt werden, finden Sie unter "Rollenmanagement" in der *Online-Hilfe*.

Change-Kategorien, Status und Risikoebenen

Sie können definieren, wie Changes in Ihrer Serviceumgebung funktionieren. Sie können die Standardwerte bearbeiten, die in CA SDM installiert sind, oder eigene definieren.

So verwalten Sie Change-Standardwerte:

1. Wählen Sie auf der Registerkarte "Administration" die Option "Service Desk" > "Changes" aus.
2. Erweitern Sie den Change-Knoten, und wählen Sie *eine* der folgenden Optionen aus:
 - Kategorien
 - Change-Typen
 - Schließungscodes
 - Konfliktstatus
 - Risikoebene
 - Risikoumfrage
 - Status
 - Statuscode der Workflow-Aufgabe
 - Workflow-AufgabentypenDie Listenseite für das ausgewählte Element wird angezeigt.
3. Wählen Sie das zu bearbeitende Element aus.
Die Seite "Details aktualisieren" wird angezeigt.
4. Verwenden Sie die unten auf der Registerkarte verfügbaren Schaltflächen, um zu definieren, wie Changes in Ihrer Umgebung funktionieren.
5. Klicken Sie auf "Speichern" und "Fenster schließen".
Das aktualisierte Element wird in der Liste angezeigt.

Anzeigen des Change-Scoreboards

Im Change-Scoreboard werden die Changes, Konflikte und geplanten Aufgaben angezeigt, die Level 2-Analysten, Change Managern, Change-Koordinatoren oder CAB-Mitgliedern zugewiesen werden. Anwender können ihre zugewiesenen und nicht zugewiesenen Datensätze nach Priorität sortiert anzeigen.

So zeigen Sie das Change-Scoreboard an:

1. Navigieren Sie im CA SDM-Scoreboard zu "Changes".
2. Erweitern Sie die Ordner, um verschachtelte Ordner für folgende Elemente anzuzeigen:
 - Zugewiesene oder nicht zugewiesene offene und geschlossene Elemente
 - Gelöste oder nicht gelöste Konflikte
 - Geplante Aufgaben, die heute oder nächste Woche starten.
3. Wählen Sie den Ordner für die anzuzeigenden Elemente aus.
Die Listenseite wird angezeigt.
4. (Optional) Klicken Sie auf "Filter anzeigen", und füllen Sie eines oder mehrere der Felder aus, um Suchkriterien anzugeben, die die Liste auf die gewünschten Kommentare beschränken.
5. Klicken Sie auf "Suchen".
Auf der Listenseite werden Zusammenfassungen der Elemente angezeigt, die Ihren Suchkriterien entsprechen.
6. (Optional) Klicken Sie auf die Schaltfläche "In Liste bearbeiten", um weitere Felder anzuzeigen, die mit einem Element verbunden sein können.

Definieren von gespeicherten Abfragen für Changes

Das Definieren von gespeicherten Abfragen, die Benutzern im Change-Scoreboard zur Verfügung stehen, ist eine administrative Aufgabe. Sie können die mit CA SDM installierten vordefinierten gespeicherten Abfragen ändern oder eigene definieren.

So definieren Sie eine gespeicherte Abfrage für einen Change:

1. Wählen Sie auf der Registerkarte "Administration" die Option "Service Desk" > "Anwendungsdaten" > "Gespeicherte Abfragen" aus.
Die Seite "Gespeicherte Abfragen - Liste" wird angezeigt.

2. Wählen Sie die gespeicherte Abfrage aus, die Sie bearbeiten möchten.
Die Seite "Gespeicherte Abfrage - Detail" wird angezeigt.
3. Klicken Sie auf "Bearbeiten".
Die Seite "Gespeicherte Abfrage aktualisieren" wird angezeigt.
4. Bearbeiten Sie die Feldwerte wie gewünscht.
5. Klicken Sie auf "Speichern" und "Fenster schließen".
Die aktualisierte gespeicherte Abfrage wird in der "Gespeicherte Abfrage - Liste" angezeigt.

Beispiel: Definieren einer gespeicherten Abfrage zur Aufführung von Changes, die einem CAB zugewiesen wurden, dem der angemeldete Benutzer angehört

In diesem Beispiel wird gezeigt, wie Sie eine gespeicherte Abfrage erstellen können, die nur solche Changes aufführt, die einem CAB zugewiesen wurden, dem der angemeldete Benutzer angehört.

So erstellen Sie die gespeicherte Abfrage:

1. Navigieren Sie das Scoreboard zur Seite "Gespeicherte Abfrage aktualisieren".
2. Bearbeiten Sie die Feldwerte wie folgt:
 - a. Wählen Sie "Scoreboard-Verwendung" aus.
 - b. Setzen Sie "Typ" auf "Change".
 - c. Geben Sie die WHERE-Klausel ein:

```
cab.[group]group_list.member IN (@cnt.id) AND active = 1
```
3. Klicken Sie auf "Speichern" und "Fenster schließen".
Die gespeicherte Abfrage wird in der "Gespeicherte Abfrage - Liste" angezeigt.

Weitere Informationen:

[CAB-Konsole und Berichterstattung](#) (siehe Seite 865)

Konfigurieren von Change Manager-Optionen

Sie können Optionen für die Rolle des Change Managers konfigurieren.

So konfigurieren Sie Change Manager-Optionen:

1. Wählen Sie auf der Registerkarte "Administration" die Option "Optionsmanager".
2. Erweitern Sie den Change Manager-Knoten.

Die Optionsliste wird angezeigt.

3. Klicken Sie mit der rechten Maustaste auf die gewünschte Option, und wählen Sie "Bearbeiten" aus dem Kontextmenü aus.

Die Seite "Option aktualisieren" wird angezeigt.

4. Bearbeiten Sie die Option nach Bedarf.
5. Klicken Sie auf "Speichern" und "Fenster schließen".

Die aktualisierte Option wird auf der "Optionen - Liste" angezeigt.

Change-Kalender

Der *Change-Kalender* bietet eine grafische Ansicht von Change-Events mit Zeiten für den Beginn und das Ende der Implementierung. Mit dieser Kalenderansicht des Change-Zeitplans können Analytiker und Manager rasch erkennen, wann Events auftreten und wie sie sich auf die Umgebung, Organisation, und Ressourcen auswirken.

Im Kalender können Sie in den Tages-, Wochen- und Monatsansichten Changes erstellen und globale Change-Fenster für geplante Changes anzeigen. Gibt es mehrere Change-Fenster in einem Monat, werden sie gruppiert, z. B. als eine einzige Gruppe "Sperrfenster". Navigieren Sie tiefer in eine Wochen- oder Tagesansicht, oder zeigen Sie Einblendinformationen an, um die einzelnen Fensterdetails zu sehen.

Hinweis: Sie können nur Change-Ablaufpläne und keine Change-Fenster [exportieren](#) (siehe Seite 819).

Weitere Informationen:

[Hinzufügen von Ablaufplaninformationen zu einem Change](#) (siehe Seite 818)

[iCalendar-Event-Vorlagen](#) (siehe Seite 818)

[Exportieren von Ablaufplänen in iCalendar](#) (siehe Seite 819)

[Ablaufplan-Ansichten](#) (siehe Seite 820)

[Konfigurieren von Planungsansichten](#) (siehe Seite 822)

Hinzufügen von Ablaufplaninformationen zu einem Change

Sie können Ablaufplaninformation hinzufügen, wenn Sie einen Change erstellen oder bearbeiten.

So fügen Sie Ablaufplaninformationen hinzu:

1. Führen Sie eine der folgenden Aktionen aus:
 - Klicken Sie auf "Datei" > "Neuer Change".
 - Öffnen Sie einen Change und klicken Sie auf "Bearbeiten".
2. Füllen Sie die folgenden erforderlichen Felder aus:

Typ

Gibt den ITIL-Change-Typ als "Standard", "Normal" oder "Notfall" an. Ein Standardwert kann für eine Change-Kategorie definiert werden, die CA SDM benutzt, um neue Changes der Kategorie zu initialisieren.

Startdatum des Ablaufplans

Gibt das Startdatum des Changes an.

Dauer

Gibt die Dauer des Change im Format 00:00:00 an.

Der Ablaufplan enthält nur Changes mit einem nichtleeren Ablaufplandatum und -dauer. Der Typ ist nützlich, um Changes im Ablaufplan zu gruppieren, aber hat keine direkten Auswirkungen auf die Planung.

3. Fahren Sie mit dem Erstellen des Changes fort.
 4. Wenn Sie fertig sind, klicken Sie auf "Speichern".
- Die Ablaufplaninformationen werden dem Change hinzugefügt.

iCalendar-Event-Vorlagen

iCalendar-Event-Vorlagen kontrollieren die Informationen, die in das iCalendar-Format exportiert wird.

Die folgenden vordefinierten Vorlagen werden mit CA SDM installiert:

- Change-Ablaufplan
- Knowledge-Ablaufplanerstellung
- Knowledge-Ablaufplan abgelaufen

- Knowledge-Ablaufplanüberprüfung
- Knowledge-Ablaufplanstart

Hinweis: Sie können die vordefinierten iCalendar-Event-Vorlagen bearbeiten, aber Sie können sie nicht löschen und auch keine neuen erstellen.

Wichtig! Die Variable "SchedExpMaximum" in "web.cfg" steuert die für Exporte maximal zulässige Anzahl von Events. Eine Erhöhung des Standardwerts (1000) könnte zu einer Systeminstabilität führen. Wenn Sie versuchen, mehr Events zu exportieren als in "SchedExpMaximum" angegeben, erscheint eine Meldung mit einer Ablehnung Ihrer Exportanfrage.

Exportieren von Ablaufplänen in iCalendar

Mit CA SDM können Sie Changes im standardmäßigen iCalendar-Format exportieren. Dieser Datenaustausch ermöglicht es Ihnen, Change-Ablaufpläne in viele gebräuchliche Kalenderanwendungen einschließlich Microsoft Outlook und Lotus Notes zu importieren.

Hinweis: Wenn Sie beim Exportieren von Ablaufplänen die Option "Offen" statt "Speichern" wählen, dann kann dies bei einigen Kalenderprogrammen dazu führen, dass die Datei nicht richtig importiert wird. Um dieses Problem in Knowledge Management- und Change-Ablaufplänen zu vermeiden, wählen Sie anstelle der Option "Öffnen" die Option "Speichern". Nachdem Sie die exportierte Datei gespeichert haben, importieren Sie sie über die Schnittstelle mit dem Kalenderprogramm. Sie können nur Changes exportieren, keine Change-Fenster (Sperrung und Wartung).

Wichtig! Es werden die Daten der aktuellen Ansicht exportiert. Wenn Sie einen anwenderspezifischen Datenbereich exportieren wollen, z. B. 32 Tage, dann müssen Sie den Export in der Listenansicht durchführen. Ansonsten wird die Ansicht auf einen Monat oder eine Woche gekürzt und es werden nur die Daten dieses Zeitraums exportiert.

So zeigen Sie den Change-Kalender an

1. Klicken Sie auf die Registerkarte "Change-Kalender".
Die Filterfelder von "Change-Kalender" werden angezeigt.
2. Füllen Sie die Suchfelder so aus, dass eine Kalender- oder Listenansicht angezeigt wird, die die gewünschten Changes enthält.

3. Klicken Sie auf "Exportieren".

Die Seite "Exportieren des Ablaufplans" wird angezeigt.

Wichtig! Die Variable "SchedExpMaximum" in "web.cfg" steuert die für Exporte maximal zulässige Anzahl von Events. Eine Erhöhung des Standardwerts (1000) könnte zu einer Systeminstabilität führen. Wenn Sie versuchen, mehr Events zu exportieren als in "SchedExpMaximum" angegeben, erscheint eine Meldung mit einer Ablehnung Ihrer Exportanfrage.

4. Geben sie den Speicherort ein, wo sie die iCalendar-Datei ablegen wollen.

Eine iCalendar-Datei, die alle Events der aktuellen Ansicht enthält, wird an dem angegebenen Speicherort abgelegt.

Ablaufplan-Ansichten

CA SDM stellt die folgenden Ablaufplan-Ansichten bereit:

Liste

Zeigt eine Listenseite mit den Start- und Enddaten im Ablaufplan an.

Monat

Zeigt einen Kalender für einen vollen Monat an.

Die Anzeige zeigt Changes in Gruppen an, die einen oder mehrere Changes enthalten können. Sie können detaillierte Informationen zu den Changes in einer Gruppe sehen, indem Sie den Mauszeiger über die Gruppe bewegen, indem Sie ALT+Right-nach-rechts drücken, wenn der Fokus auf der Gruppe liegt, oder indem Sie die Gruppe klicken, um die Inhalte für eine bestimmte Anzahl von Tagen anzuzeigen.

Woche

Zeigt eine volle Woche in einer einzelnen Spalte an, wobei der erste Tag derjenige ist, der als erster Wochentag festgelegt wurde.

Die Ansicht zeigt Changes individuell an und schließt detaillierte Informationen über jeden während einer Woche geplanten Change ein.

Tag

Zeigt Changes für einen einzelnen Tag an.

Die Ansicht zeigt Changes individuell an und schließt detaillierte Informationen über jeden während eines Tages angefragten Change ein.

n Tage

Zeigt Changes für die in einer Dropdown-Auswahl angegebene Anzahl von Tagen an.

Die Ansicht zeigt Changes individuell an und schließt detaillierte Informationen über jeden während der ausgewählten Tage angefragten Change ein.

Navigieren innerhalb der Ablaufplan-Ansichten

Sie können die Pfeil- und Tabulatortasten verwenden, um innerhalb der Ablaufplan-Ansichten zu navigieren. Die folgenden Tastenkombinationen sind verfügbar:

Registerkarte

Navigiert zu einem späteren Datum. Verwenden Sie diese Taste um von der letzten Zelle im Ablaufplan zur Schaltfläche "Suche" zu navigieren.

Umschalt+Tab

Navigiert zu einem vorherigen Datum. Verwenden Sie diese Taste um von der ersten Zelle im Ablaufplan zur Schaltfläche "Nächster Monat" zu navigieren.

Umschalt+Pfeiltaste

Navigiert in Pfeilrichtung von Datum zu Datum durch den Kalender.

Pfeil nach rechts

Zeigt für das ausgewählte Datum oder Event das Kontextmenü an. Wenn es kein Kontextmenü gibt, navigiert es zum nächsten höheren Datum (vergleichbar mit "Umschalt+Pfeil nach rechts").

Alt+Pfeil nach rechts

Zeigt ein Informationsfenster für das ausgewählte Datum oder Event an. Wenn es kein Informationsfenster gibt, navigiert es zum nächsten höheren Datum (vergleichbar mit "Umschalt+Pfeil nach rechts").

Pfeiltaste nach unten

Navigiert zum nächsten Event in der aktuellen Zelle. Wenn es keine Events in der aktuellen Zelle gibt, oder wenn bereits das letzte Event ausgewählt ist, navigiert es zum Datum in der nächsten Zelle nach unten (vergleichbar mit "Umschalt+Pfeil nach unten").

Pfeiltaste nach oben

Navigiert zum vorherigen Event in der aktuellen Zelle. Wenn kein Event ausgewählt ist, navigiert es zum Datum in der nächsten Zelle aufwärts (vergleichbar mit "Umschalt+Pfeil nach oben").

Hotkeys zur Kalender-Ansicht

Jede Ablaufplaner-Ansicht unterstützt Hotkeys für die Schaltflächen in dieser Ansicht. Folgende Hotkeys werden unterstützt:

Alt+0

In die Listenansicht wechseln

Alt+1

In die Tagesansicht wechseln

Alt+7

In die Wochenansicht wechseln

Alt+3

In die Monatsansicht wechseln

Alt+9

In die *n*-Tage-Ansicht wechseln

Alt+<

Zum vorherigen Zeitraum in der aktuellen Ansicht gehen

Alt+>

Zum nächsten Zeitraum in der aktuellen Ansicht gehen

Konfigurieren von Planungsansichten

Sie konfigurieren die monatlichen und wöchentlichen Planungsansichten, indem Sie "pdm_macro"-Anweisungen im Abschnitt <head> der HTML-Formulare angeben, die den Ablaufplan definieren. Es wird empfohlen, das Quellansicht von Web Screen Painter zu benutzen, um diese Formulare zu bearbeiten.

Jedes Formular, das einen Ablaufplan anzeigt, muss Folgendes enthalten:

- Ein "schedConfig"-Makro
- Mindestens ein schedAttr-Makro
- Mindestens ein schedGroup-Makro

Die Konfigurationsmakros befinden in einer separaten Quelldatei, die von einer pdm_include-Anweisung in der Hauptquelldatei referenziert wird. Diese ermöglicht Ihnen, Ihren Ablaufplan zu konfigurieren, ohne die Hauptquelldatei zu ändern.

Die Konfigurationsmakros für das Change-Kalender-Formular "list_chgsched.html" befinden sich beispielsweise in der Datei "list_chgsched_config.html". Für den Knowledge-Lebenszyklus-Ablaufplan können Sie die Datei "list_kdsched_config.html" mit denselben Makros ändern.

Sie können list_chgsched_config.html und list_kdsched_config.html im folgenden Verzeichnis finden:

\$NX_ROOT\bopcfg\www\html\web\analyst\

schedAttr-Makro – Gespeichertes Attribut angeben

Das schedAttr-Makro gibt ein Attribut an, das für jedes Element gespeichert wird, welches für die Liste ausgewählt ist. Gespeicherte Attribute stehen für Popup-Infos in der Monatsansicht, für die detaillierten oder zusammenfassenden Informationen in Ansichten außer der Monatsansicht und in der setSchedEvents()-JavaScript-Funktion zur Verfügung. Folgende Werte sind gültige Makroargumente:

attr=xxxx

(Obligatorisch) Gibt ein Attribut aus dem Objekt auf dem Ablaufplan an, z. B. ein Change oder Knowledge-Dokument. Attribute mit Punkten sind zulässig. Der Schlüsselwort-Attributname "CInn" kann auf dem Change-Kalender verwendet werden, um anzugeben, dass die ersten mit dem Change verknüpften *nn*-Cls in die gespeicherten Informationen aufgenommen werden sollen.

Hinweis: Dieses Argument ist das einzige erforderliche Argument für das schedAttr-Makro.

attrRef=.COMMON_NAME|xxxx

Speichert das Attribut der referenzierten Tabelle, die für ein SREL-Attribut gespeichert wird (und für Nicht-SREL-Attribute ignoriert wird). Dem angegebene Attributname muss ein Punkt vorangestellt werden.

Standard: .COMMON_NAME

label=

Zeigt eine Beschriftung für das Attribut auf der n-Tage-Ansicht an.

Standard: der Majic DISPLAY_NAME des Attributs

ident=1|0

Gibt an, ob das Attribut als Kennzeichen für das Objekt fungieren soll (z. B. eine Referenznummer für einen Change). Kennzeichen-Attribute werden ohne eine Bezeichnung vor dem Gruppennamen in Popup-Infos und der n-Tage-Ansicht angezeigt.

Standard: 0

detail=1|0

Gibt an, ob das Attribut in die Detailinformationen aufgenommen wird, die in anderen Ansichten als der Monatsansicht angezeigt werden. Detailinformationen sind die Informationen, die angezeigt werden, wenn das Kontrollkästchen "Nur Zusammenfassung" für die Ansicht nicht aktiviert ist.

Standard: 1

hoverInfo=1|0

Gibt an, ob das Attribut im Popup-Info enthalten ist, welche in der Monatsansicht angezeigt wird, wenn der Mauszeiger über eine Gruppe bewegt wird oder der Benutzer Alt+Pfeil-nach-rechts drückt, wenn der Schwerpunkt auf der Gruppe liegt.

Standard: 0

summary=1|0

Gibt an, ob das Attribut in die Detailinformationen aufgenommen wird, die in anderen Ansichten als der Monatsansicht angezeigt werden. Detailinformationen sind die Informationen, die angezeigt werden, wenn das Kontrollkästchen "Nur Zusammenfassung" für die Ansicht nicht aktiviert ist.

Standard: 0

Hinweis: CA SDM zeigt Attribute in der Zusammenfassungs-, der Detail- oder der Popup-Info in derselben Reihenfolge wie ihre schedAttr-Makros an.

"schedConfig"-Makro – Konfigurieren von Schichten

Das "schedConfig"-Makro gibt an, dass ein Formular einen Ablaufplan enthält und grundlegende Konfigurationsinformationen bietet. Folgende Werte sind gültige Makroargumente:

autosearch=1|0

Gibt an, ob das Ablaufplanformular erneut Daten vom Server laden soll oder nicht, wenn der Anwender eine Ansicht außerhalb des derzeit ausgewählten Datumsbereichs auswählt. Die Festlegung des Werts auf 1 (Standard) hat zur Folge, dass das Formular automatisch sucht, wenn der Anwender eine Ansicht mit einem oder mehr Tagen außerhalb des Datumsauswahlbereichs des Suchfilters auswählt. Bei der Festlegung des Werts auf 0 muss der Anwender die Schaltfläche "Suche" drücken, um die Suche zu starten.

defaultView=0|1|7|30|99

Gibt die Standardansicht für den Suchfilter als 0 (Liste), 1 (Tag), 7 (Woche), 30 (Monat), oder 99 (n-Tage) an.

Die Angabe für defaultView wirkt sich nur auf die anfängliche Anzeige des Suchfilters aus. Sobald der Ablaufplan angezeigt wird, stimmt CA SDM automatisch die Ansichtsauswahl des Filters auf die aktuelle Ansicht ab.

Standard: 30

firstday=0|1|2|3|4|5|6|7

Gibt den ersten Wochentag in der Monatsansicht als eine Zahl zwischen 0 (Sonntag) und sechs (Samstag) an.

Standard: 0

export=xxx|0

Gibt den Codenamen der Vorlage an, der für den Export in das iCalendar-Format verwendet wird. Durch Festlegen des Werts auf 0 wird angegeben, dass die Exportfunktion und die Export-Schaltfläche deaktiviert sind.

Standard: ChangeSchedule

legend=1|2|0

Gibt die Lokation der Ablaufplanlegende an, die den Namen und die Formatierung der Gruppen im Ablaufplan anzeigt. Sie können den Wert auf 1 einstellen, um die Legende über dem Ablaufplan zu platzieren, oder auf 2, um die Legende unter dem Ablaufplan zu platzieren. Setzen Sie den Wert auf 0, um die Legende zu deaktivieren.

Standard: 2

maxGroups=0/n

Gibt die größtmögliche Anzahl von Gruppen an, die in einer einzigen Zelle der Kalendermonatsansicht angezeigt werden sollen.

Wenn mehr als maxGroups für einen einzelnen Tag geplant sind, zeigt CA SDM nur die erste maxGroups-1 an und ersetzt die letzte durch einen "...nn zusätzliche Changes"-Hyperlink, über den der Anwender den Mauszeiger führen oder darauf klicken kann, damit die komplette Liste zu sehen ist. Setzen Sie den Wert auf 0, um die Funktion zu deaktivieren und eine unbegrenzte Anzahl von Events in einer Kalenderzelle zu ermöglichen.

Standard: 4

nday=(n,n,...)

Gibt die Auswahlen für die Dropdown-Liste für die n-Tage-Ansicht an.

Die Angabe ist eine Liste von Tageszählungen, die in die Dropdown-Liste aufgenommen werden sollen; die Angabe von 0 bedeutet, dass die n-Tage-Dropdown-Liste vom Ablaufplan ausgeschlossen ist. Der erste angegebene Wert ist der Standard für die Dropdown-Liste.

Standard: (3,7,14,28)

round=(hr,min)|0

Gibt an, ob das Start- und Enddatum des Ablaufplans gerundet werden soll, wenn Changes oder Knowledge-Dokumente in Gruppen zusammengestellt werden. Geben Sie "round=0" an, um das Runden zu deaktivieren.

Standardmäßig gruppiert das Start- und Enddatum des Ablaufplans Objekte. Alle CA SDM-Daten beinhalten eine Uhrzeit, und ohne Auf- bzw. Abrundung befänden sich Objekte mit einem Zeitabstand von weniger als einer Minute in separaten Gruppen. Die Auf- bzw. Abrundung legt die Gruppe nach der Anpassung des Startdatums auf eine frühere Stunde oder Minute und des Enddatums auf eine spätere Stunde oder Minute fest.

Der Wert der Rundung gibt entweder eine Stunde oder eine Minute (aber nicht beide) an. Uhrzeiten werden auf das nächste Vielfache des angegebenen Werts gerundet. Beispiel:

round=(0,15) rundet auf die nächste Viertelstunde auf

round=(0,30) rundet auf die nächste halbe Stunde auf

round=1 rundet auf die nächste Stunde auf

round=12 rundet auf den nächsten halben Tag (12:00 oder 24:00) auf

round=24 rundet auf den nächsten Tag auf

Standard: (0,15)

timefmt=24hr|([am],[pm])

Gibt das Format der Uhrzeiten in den Kalenderansichten des Ablaufplans an.

Der Standardwert 24 St. gibt an, dass die Uhrzeiten im 24-Stunden-Format (0:01 - 23:59) angezeigt werden. Der alternative Wert (am,pm) gibt ein Suffix für Uhrzeiten am Vormittag oder Nachmittag oder für beide an.

Hinweis: Alle schedConfig-Argumente sind optional.

Makro "schedGroup" – Ereignisgruppe angeben

Das schedGroup-Makro gibt den Namen und Farbcodierung einer Gruppe von Elementen an. Die Monatsansicht führt alle Elemente in einer Gruppe in ein einzelnes Ereignis zusammen. Ansichten mit Ausnahme der Monatsansicht zeigen einzelne Elemente im Format für die Gruppe, zu der sie gehören. Folgende optionale Werte sind gültige Makroargumente:

grpname=xxx

(Obligatorisch) Gibt den Namen der Gruppe an. Das Makro weist der Gruppe automatisch eine Zahl zu und weist die Zahl einer JavaScript-Variablen mit einem Namen in der Form schedGroup_xxx zu, wobei xxx der Name der Gruppe ist. Diese Variable kann in der setSchedEvents()-JavaScript-Funktion benutzt werden, um ein der Gruppe angehöriges Ereignis zu erstellen.

Hinweis: Dieses Argument ist das einzige obligatorische Argument für das schedGroup-Makro.

label=xxx

Gibt für die Gruppe eine Bezeichnung an. Falls angegeben, wird die Bezeichnung in allen Ansichten angezeigt.

legend=xxx|0

Zeigt eine Beschreibung der Gruppe für die Legende an, die unten im Ablaufplan angezeigt wird. Gruppen erscheinen in der Legende, wenn mindestens ein Beispiel der Gruppe in der aktuellen Ansicht existiert. Durch die Angabe von 0 wird die Gruppe immer von der Legende ausgeschlossen.

Standard: 0

color=schwarz|Farbe

Gibt die Farbe des Texts in Elementen dieser Gruppe an. Sie können die Farbe im CSS-Format angeben: entweder eine gültige Web-Farbe oder einen Hexadezimalwert mit einem vorangestellten Rautezeichen.

Beispiel: Geben Sie entweder "#FF0000" oder "rot" für Rot ein.

Standard: schwarz

bgcolor=weiß|Farbe

Gibt die Hintergrundfarbe von Elementen dieser Gruppe an. Sie können die Hintergrundfarbe im CSS-Format angeben: entweder eine gültige Web-Farbe oder einen Hexadezimalwert mit einem vorangestellten Rautezeichen.

Beispiel: Geben Sie entweder "#FF0000" oder "rot" für Rot ein.

Standard: weiß.

style=normal|fett|kursiv

Formatiert Text dieser Gruppe normal, fett oder kursiv.

Standard: normal

Konfigurieren von Ausfall- und Wartungsfenstern im Change-Kalender

Sie bearbeiten die Anweisungen "PDM_MACRO" in "list_chgsched_config.html", um Farben, Bezeichnungen, Legenden und Symbole für Change-Fenster zu ändern.

Hinweis: Wenn Sie Makros "schedGroup" verwenden, um die Gestaltung von Fenstern im Change-Kalender zu ändern, müssen Sie auch die Datei *schedule.css* aktualisieren, wenn die Gestaltung mit dem Change-Scheduler übereinstimmen soll.

So konfigurieren Sie Change-Fenster:

1. Öffnen Sie das Formular *list_chgsched_config.html* in einem Texteditor oder in WSP.

Diese Datei befindet sich in folgendem Verzeichnis:

```
$NX_ROOT\bopcfg\www\html\web\analyst\
```

2. Ändern Sie in dem Makro "schedGroup" die folgenden "PDM_MACRO"-Anweisungen:

Für Wartungsfenster:

```
<PDM_MACRO NAME=schedGroup grpname=maintWindow  
  bgcolor=lightgreen  
  label="Maintenance"  
  legend="Maintenance Window"  
  icon= "confirmation_12.png">
```

Für Ausfallfenster:

```
<PDM_MACRO NAME=schedGroup grpname=blackoutWindow style=italic color=white  
  bgcolor=black  
  label="Blackout"  
  legend="Blackout Window"  
  icon= "warning_12.png">
```

bgcolor

Gibt die Hintergrundfarbe des Zeitfensters an.

label

Kennzeichnet die Fensterbezeichnung als Ausfall- oder Wartungsfenster.

Legende

Gibt den Text der Legende an, wie sie im Change-Kalender angezeigt wird.

icon

Gibt eine optionale URL zu einer 12x12-Pixel-Webgrafik an.

Dieses Symbol wird mit einem Change oder einer Gruppe im Change-Kalender angezeigt, wenn der Change vollständig innerhalb eines Wartungsfensters liegt oder sich mit einem Ausfallfenster überschneidet.

3. Speichern Sie das Formular.

Die Change-Fenster werden konfiguriert.

Die JavaScript-Funktion "setSchedEvents()"

Die JavaScript-Funktion "setSchedEvents()" erstellt Events im Ablaufplan. Ändern Sie diese Funktion, wenn Sie neue Gruppenobjekte anzeigen möchten. Die vordefinierten Gruppenobjekte werden standardmäßig angezeigt.

CA SDM ruft "setSchedEvents()" je einmal für jedes Objekt (Change oder Knowledge-Dokument) auf, das über den Suchfilter des Ablaufplans ausgewählt wurde. Die Funktion erstellt Events für das Objekt durch Aufrufen einer zweiten Funktion, schedEvent() und Weitergeben der Gruppen-ID, des Startdatums und des Enddatums des Event.

Die Funktion kann eine beliebige Anzahl von Events (einschließlich Null) für ein Objekt erstellen. Die Standardfunktion "setSchedEvents()" für den Change-Kalender ("list_chgsched.html") erstellt je ein Event pro Change und gruppiert Changes nach dem Change-Typ. Diese Funktion wird folgendermaßen kodiert:

```

1.      Funktion "setSchedEvents( chg )"
2.      {
3.      var grpnum;
4.      switch( chg["chgtype"] - 0 ) {
5.          case 100: grpnum = schedGroup_std; break;
6.          case 300: grpnum = schedGroup_emer; break;
7.          default: grpnum = schedGroup_norm; break;
8.      }
9.      chg. schedEvent (grpnum, chg["sched_start_date"], chg["sched_end_date"]);
10.     }
```

Der "case"-Parameter gibt die Change-Typ-ID an. Eine Liste der Fall-IDs finden Sie unter Erstellen von Change-Typen.

Die Funktion hat ein einzelnes Argument eines JavaScript-Objekts, das die von schedAttr-Makros angegebenen Attribute enthält. Die "switch"-Anweisung in Zeile 4 bis 8 untersucht das "chgtype"-Attribut des Change und weist die richtige Gruppennummer aus einer der "schedGroup_xxxx"-Variablen zu, die von früheren "schedGroup"-Makros definiert wurden. In Zeile 9 wird die Funktion "schedEvent()" aufgerufen, um ein Event im Ablaufplan zu erstellen, wobei die zuvor zugewiesene Gruppennummer und das Start- und Enddatum für den Ablaufplan übergeben werden. Die Daten sind im Argumentobjekt verfügbar, da sie in früheren schedAttr-Makros angegeben wurden.

So planen Sie Changes:

Sie können den Ablaufplan aller Configuration Items anzeigen, die mit einem Change verknüpft sind. Es empfiehlt sich, Informationen zu planen, wenn Sie einen Change erstellen, bearbeiten oder anzeigen bzw. wenn Sie den Ablaufplan für Changes aktualisieren. Das Anzeigen des Ablaufplans kann Ihnen helfen, Planungskonflikte zu vermeiden.

Gehen Sie folgendermaßen vor, um einen Ablaufplan zu aktualisieren und anzuzeigen:

1. Erstellen oder öffnen Sie einen Change.
2. Verknüpfen Sie CIs mit dem Change.

Hinweis: Wenn Sie keinen CI mit dem Change verknüpfen, wird ein Fehler angezeigt, wenn Sie auf die Schaltfläche "Scheduler" klicken.

3. Klicken Sie auf "Ablaufplaner anzeigen".

Der Change-Scheduler wird mit den folgenden Ansichten angezeigt:

Täglich

(Standardwert) Zeigt den Zeitraum des Changes für das ausgewählte Datum und die ausgewählte Uhrzeit an. Ist kein Datum mit dem Change verknüpft, wird standardmäßig der aktuelle Tag angezeigt.

Wöchentlich

Zeigt den Zeitraum des Changes in der aktuellen Woche an und schließt das Startdatum der Implementierung ein, welches Sie zum Anfangsdatum des Change-Kalenders konfigurieren können.

Hinweis: Die Zeitdauer des Ablaufplans bestimmt die Länge der Schattierung im Ablaufplan. Wenn Sie zum Beispiel einen Change mit einer Zeitdauer von zwei Stunden erstellen, zeigt die hellgelbe Schattierung im Scheduler einen Zeitraum von zwei Stunden an.

4. (Optional) Klicken Sie auf einen CI, um dessen Details anzuzeigen. Zeigen Sie mit der Maus auf den CI-Namen, um dessen vollen Namen anzuzeigen.
5. (Optional) Ändern Sie das Implementierungsstartdatum oder die Dauer.
 - a. Klicken Sie auf "Ablaufplan anzeigen", um eine Vorschau des aktualisierten Ablaufplans zu sehen.
 - b. Klicken Sie auf "Ablaufplan aktualisieren", um den Ablaufplan zu aktualisieren.

Hinweis: Sie können den Ablaufplan nur im Bearbeitungsmodus ändern.

6. Speichern Sie den Change.
7. Aktualisieren Sie den Change-Kalender, um globale und CI-bezogene Change-Fenster anzuzeigen.

Beispiel: Verwenden des Change-Schedulers

Im folgenden Beispiel wird gezeigt, wie Sie mit Hilfe des Change-Schedulers einen Change erstellen.

1. Wählen Sie auf der Registerkarte "Service Desk" die Optionen "Datei", "Neuer Change" aus.

Die Seite "Neuen Change erstellen" wird angezeigt.

2. Wählen Sie auf der Registerkarte "Config. Items" aus.

Die Seite "Configuration Item - Suche" wird angezeigt.

3. Erstellen und Suchen nach CIs

4. Fügen Sie auf der Seite "Betroffene Configuration Items aktualisieren" dem Change CIs hinzu.

5. Klicken Sie auf "OK".

Die Seite "Neuen Change erstellen" wird aktualisiert.

6. Klicken Sie auf die Schaltfläche "Scheduler".

Die Seite "Ablaufplan für Change" wird angezeigt.

7. Wählen Sie eine Ansicht aus, und folgen Sie *einer* der folgenden Vorgehensweisen:

- Klicken Sie in die Tabellenzellen, um das Startdatum des Ablaufplans zu ändern.
- Klicken Sie auf Startdatum des Ablaufplans, um die Datumshilfe zu öffnen.

8. Ändern Sie die Dauer, und klicken Sie auf "Ablaufplan anzeigen".

Im Ablaufplan wird eine Vorschau Ihrer Changes angezeigt.

9. Klicken Sie auf "Ablaufplan aktualisieren".

Der Ablaufplan wird gemäß Ihren Changes aktualisiert.

10. Speichern Sie den Änderungsauftrag.

Festlegen der maximalen Anzahl von CIs

Sie können die maximale Zahl der CIs, die im Change-Scheduler angezeigt werden, festlegen.

So legen Sie die maximale Anzahl der CIs fest:

1. Öffnen Sie die Datei *NX.env*.

Diese Datei befindet sich in folgendem Verzeichnis:

`$NX_ROOT\`

2. Ändern Sie den Wert von `@NX_CHANGE_SCHEDULER_MAX_CI_CNT` auf die gewünschte maximale Anzahl.

Hinweis: Standardmäßig ist die Variable auf 100 gesetzt. Wenn Sie die maximale Anzahl der CIs auf einen Wert über 100 festlegen, werden nur die ersten 100 sowie eine Warnung angezeigt.

3. Speichern Sie die Datei *NX.env*, und starten Sie CA SDM neu.

Die maximale Anzahl der CIs ist festgelegt.

Beispiel: Legen Sie die maximale Zahl der CIs auf 25 fest.

In dem folgenden Beispiel werden nur die ersten 25 CIs im Change-Scheduler angezeigt.

```
@NX_CHANGE_SCHEDULER_MAX_CI_CNT=25
```

Ändern der Hintergrundfarbe der Change-Zeit

Sie können die Hintergrundfarbe der Change-Zeitleiste ändern. Ändern Sie die folgenden Zeilen in der Datei *schedule.css*, um die Farbe der grünen Change-Zeitleiste zu ändern.

So ändern Sie die Hintergrundfarbe:

1. Öffnen Sie die Datei *schedule.css*.

Diese Datei befindet sich in folgendem Verzeichnis:

`$NX_ROOT\bopcfg\www\wwwroot\css`

Wichtig! `$NX_ROOT\sdk` enthält auch eine Datei mit dem Namen "schedule.css", die hilfreiche Anmerkungen zur Verwendung von css enthält.

2. Geben Sie in den folgenden Zeilen den gewünschten Farb-Code ein:

```
td.noBorderBackColor{border-left:none;border-right:none;background-color:#F6E3CE;}
td.withBorderBackColor{border-right:none;border-left:1px
solid;background-color:#F6E3CE;}
```

3. Speichern Sie *schedule.css*.

Im folgenden Beispiel ist die Hintergrundfarbe der Change-Zeitleiste "#FF0000".

Beispiel: Ändern Sie die Hintergrundfarbe der Change-Zeitleiste zu "#FF0000".

```
td.noBorderBackColor{border-left:none;border-right:none;background-color:#FF0000;
}
td.withBorderBackColor{border-right:none;border-left:1px
solid;background-color:#FF0000;}
```

Ändern der Farben von Change-Fenstern im Change-Scheduler

Sie können die Farben ändern, die Change-Fenster kennzeichnen, indem Sie Zeilen in *schedule.css* ändern.

Hinweis: Wenn Sie *schedule.css* ändern, um die Gestaltung von Fenstern im Change-Scheduler zu ändern, müssen Sie auch die Makros "schedGroup" ändern, die vom Change-Kalender verwendet werden, wenn dessen Gestaltung mit dem Scheduler übereinstimmen soll.

So ändern Sie die Hintergrundfarbe:

1. Öffnen Sie *schedule.css* in einem Texteditor.

Diese Datei befindet sich in folgendem Verzeichnis:

\$NX_ROOT\bopcfg\www\wwwroot\css

2. Geben Sie in den folgenden Zeilen den gewünschten Farb-Code ein:

```
.schedConflict { background-color: #ff0000; font-size: 4px }  
.schedBusy { background-color: #0176ff; font-size: 4px}  
.schedCurrent { background-color: #008000; font-size: 4px; }  
.schedMW { background-color: #40ff40; font-size: 4px; }  
.schedBW { background-color: black; font-size: 4px; }  
.schedNone {font-size: 4px; }  
.schedDialog { width: 100%; height: 4px; margin-left: 0px; margin-right: 0px;  
margin-top: 4px; margin-bottom: 4px; }
```

3. Speichern Sie *schedule.css*.

Die Hintergrundfarbe ist nun geändert.

Weitere Informationen:

["schedConfig"-Makro – Konfigurieren von Schichten](#) (siehe Seite 824)

So planen Sie Change-Fenster:

Sie können Change-Fenster planen und sie im Change-Kalender anzeigen.

Wartungsfenster legen Zeiträume fest, in denen CI-Änderungen auftreten sollten, und *Sperrfenster* legen Zeiträume fest, in denen CI-Änderungen *nicht* auftreten sollten. Mit Change-Fenstern können Sie Changes so planen, dass ihre Auswirkungen auf kritische Geschäftsprozesse minimiert werden. CA SDM kann Change-Fenster auf globaler Ebene oder auf Systemebene implementieren.

Gehen Sie folgendermaßen vor, um Change-Fenster zu planen:

1. Zeigen Sie den Change-Kalender an, um die gewünschten Positionen der Change-Fenster festzulegen.
2. Erstellen Sie geeignete Change-Fenster für Ihre Organisation.

Wartungsfenster

Zeigt einen geplanten Zeitraum an, in dem ein CI oder eine Gruppe von CIs geändert werden können. Da Changes u. U. Ausfallzeiten verursachen, können diese Fenster verwendet werden, um Unterbrechungen von kritischen Geschäftsprozessen zu minimieren. Im Allgemeinen sollten geplante Changes innerhalb eines Wartungsfensters auftreten.

Sperrfenster

Zeigt einen geplanten Zeitraum an, in dem keine CI-Changes auftreten sollen. Dieses Sperrfenster kann auf einen reduzierten Supportzeitraum (z. B. an einem Feiertag), ein Unternehmens-Event oder eine kritische Geschäftszeit, wie z. B. das Ende des Geschäftsjahres, verweisen. Im Allgemeinen sollten geplante Changes nur außerhalb von Sperrfenstern auftreten.

Fenster für globale Changes

Zeigt ein Sperr- oder Wartungsfenster an, das für Ihre ganze Organisation gilt. Zum Beispiel möchten Sie ein [globales](#) (siehe Seite 839) Sperrfenster mit Namen "Feiertag" von November bis Januar in der ostamerikanischen Zeitzone erstellen. Dieses Sperrfenster erlaubt mit Ausnahme von Notfall-Changes *keine* Changes zwischen diesen beiden Daten. Globale Change-Fenster sind keinen bestimmten CIs zugeordnet, weil sie sich auf alle CIs beziehen.

3. (Optional) Geben Sie die Wiederholungsmuster für Change-Fenster an.
4. Öffnen Sie den Change-Kalender.

In der Legende werden die Symbole und Farben dargestellt, die die Change-Fenster im Ablaufplan kennzeichnen.

5. Erstellen Sie Changes, die mit CIs verknüpft sind.
6. Aktualisieren Sie den Change-Kalender mit dem Change-Scheduler.

Hinweis: Weitere Informationen zur Erstellung von Change-Fenstern finden Sie in der *Online-Hilfe*.

Anzeigen von Change-Fenstern

Sie können Change-Fenster im Change-Kalender anzeigen, um zu erkennen, wann ihre zugeordneten CIs geändert werden können und wann nicht.

So zeigen Sie Change-Fenster an:

1. Klicken Sie auf der Registerkarte "Administration" auf "Service Desk" > "Change" > "Change-Fenster".

Die Liste "Change-Fenster" wird angezeigt.

2. Wählen Sie das gewünschte Change-Fenster aus.

Das Change-Fenster wird angezeigt.

3. (Optional) Klicken Sie auf "Bearbeiten".

Sie können das Change-Fenster ändern.

4. Speichern oder schließen Sie das Fenster.

Die Seite "Fenster - Details" wird angezeigt.

Zuordnen eines CIs zu einem Wartungsfenster

Um zu kontrollieren, wann ein CI gewartet wird, können Sie dieses CI einem Wartungsfenster zuordnen.

So ordnen Sie ein CI einem Wartungsfenster zu:

1. Navigieren Sie zur Seite "Change-Fenster – Details".
2. Klicken Sie auf die Registerkarte "Verknüpfte CIs".
Die Liste "Verknüpfte CIs" wird angezeigt.
3. Klicken Sie auf "Configuration Items aktualisieren".
Die CI-Suchseite wird angezeigt.
4. Geben Sie Informationen über die erforderlichen CIs an.
5. Klicken Sie auf "Suchen".
Die Seite "Verfügbare CIs" wird angezeigt.
6. Bewegen Sie die erforderlichen CIs aus der Liste "Verfügbare CIs" in die Liste "Verknüpfte CIs".
7. Klicken Sie auf "OK".
Die Seite "Change-Fenster Details" wird angezeigt.
8. Klicken Sie auf "Speichern".
Das CI wird mit einem Wartungsfenster verknüpft.

Das Change-Fenster, die CIs und die ausgewählten Fensterverknüpfungen werden gespeichert.

Anzeigen von zugeordneten CIs

Um festzulegen, auf welche Weise ein CI während bestimmter Zeiträume betroffen sein kann, können Sie die CIs anzeigen, die nicht-globalen Wartungsfenstern zugeordnet sind.

So zeigen Sie die einem Wartungsfenster zugeordneten CIs an:

1. Navigieren Sie zur Seite "Change-Fenster – Details".
2. Klicken Sie auf die Registerkarte "Zugeordnete CIs".
Die zugeordneten CIs werden angezeigt.

Erstellen eines Beispiel-Sperrfensters

Im folgenden Beispiel wird ein Sperrfenster erstellt, um anzuzeigen, dass Ihre Organisation für einen bestimmten Zeitraum keine Changes plant. Dieses Ausfallfenster soll 48 Stunden dauern und jeden Freitag um 18.00 Uhr beginnen.

Gehen Sie wie folgt vor:

1. Klicken Sie auf der Registerkarte "Administration" auf "Service Desk" > "Change" > "Change-Fenster".

Die Liste "Change-Fenster" wird angezeigt.

2. Klicken Sie auf "Neu erstellen".

Die Seite "Neues Change-Fenster erstellen" wird angezeigt.

3. Füllen Sie die entsprechenden Felder wie folgt aus:

- a. Geben Sie **Freitag_Sperrfenster** als Fensternamen ein.
- b. Wählen Sie den Typ "Sperrung" aus.
- c. Wählen Sie den Status "Aktiv" aus.
- d. Wählen Sie den kommenden Freitag und 18:00 Uhr aus der Datumshilfe als Startdatum aus.
- e. Wählen Sie den kommenden Sonntag und 18:00 Uhr aus der Datumshilfe als Enddatum aus.
- f. Wählen Sie Ihre Zeitzone aus.
- g. (Optional) Geben Sie eine Beschreibung für das Sperrfenster ein.
- h. Wählen Sie auf der Registerkarte "Wiederholungsmuster" die Option "Wöchentlich" aus.
 - Setzen Sie die Wiederholung auf jede **1** Woche.
 - Wählen Sie ein Datum aus, an dem die Wiederholung enden soll.

4. Speichern und schließen Sie das Sperrfenster.
5. Aktualisieren Sie die "Change-Fenster - Liste".
6. Öffnen und aktualisieren Sie den Change-Kalender.

Das Sperrfenster wird im Ablaufplan angezeigt.

Erstellen eines globalen Wartungsfensters

Erstellen Sie ein globales Wartungsfenster für Ihre Organisation. Zum Beispiel möchten Sie Wartungsfenster *nicht* nach Server oder CI definieren, und Sie möchten globale Changes an Wochenenden durchführen.

Gehen Sie wie folgt vor:

1. Navigieren Sie zur Seite "Change-Fenster – Liste".
2. Klicken Sie auf "Neu erstellen".
3. Die Seite "Neues Change-Fenster erstellen" wird angezeigt.
4. Geben Sie die benötigten Werte in die Felder für das Wartungsfenster ein bzw. passen Sie sie wie gewünscht an.
5. Legen Sie als Typ für das Fenster "Wartung" fest.
6. Stellen Sie sicher, dass das Kontrollkästchen "Global" aktiviert ist.

Hinweis: Globale Wartungsfenster können nicht CIs zugeordnet werden.

7. Geben Sie das Anfangsdatum, das Enddatum, und die Zeitzone ein.
8. Klicken Sie auf "Speichern".

Das globale Wartungsfenster wird gespeichert.

Konfliktanalyse und Konflikterkennung

Die Konfliktanalyse erkennt und zeigt Konflikte, die auftreten, wenn eine Implementierung von zwei oder mehr Changes an einem Configuration Item zur gleichen Zeit geplant ist. Dem Change Management-Team stehen die folgenden Möglichkeiten zur Auswahl, um mit Planungskonflikten umzugehen:

- Verwenden des Change-Kalenders zur Anzeige von Konflikten zwischen Change und CI sowie Durchführen der erforderlichen Anpassungen zur Verringerung der voraussichtlichen Auswirkungen
- Suchen und Erkennen von Konflikten in einem Protokoll

Hinweis: Weitere Informationen zum Umgang mit Planungskonflikten finden Sie in der *Online-Hilfe*.

CA Workflow-Visualisierung

CA Workflow Visualization lässt Sie den Fortschritt von Change-Workflow Aufgaben überwachen. Der Prozess-Viewer stellt jeden Schritt des CA Workflow-Prozesses grafisch dar, einschließlich vollständiger und unvollständiger Schritte sowie der aktuellen Position des Workflow-Fortschritts.

Der Prozess-Viewer zeigt den Status und den Pfad eines <WF>-Prozesses an, wenn dieser mit einer Change- bzw. Issue-Kategorie oder einem Anfrage-/Incident-/Issue-Bereich verknüpft ist.

So visualisieren Sie den Workflow:

Visualisieren Sie den Workflow folgendermaßen:

1. Verknüpfen Sie einen CA Workflow-Prozess mit einer Change-Kategorie.
2. Erstellen Sie mit Hilfe dieser Change-Kategorie eine Change-Reihenfolge.
3. Klicken Sie auf der Registerkarte "Workflow-Tasks" auf die Schaltfläche "Prozess anzeigen", um den Prozess-Viewer zu starten.

Hinweis: Weitere Informationen über das Verknüpfen von CA Workflow-Prozessen mit Kategorien oder Bereichen finden Sie in der *Online-Hilfe*.

Beispiel: Verwenden des Prozess-Viewers

In diesem Beispiel wird gezeigt, wie Sie mit Hilfe einer Standard-Change-Kategorie den Prozess-Viewer auf Ihrem System einsetzen, nachdem Sie CA Workflow installiert und die Optionen aktiviert haben.

1. Wählen Sie auf der Registerkarte "Administration" die Option "Service Desk" > "Changes" > "Kategorien" aus.

Die Seite "Change-Kategorien - Liste" wird angezeigt.

2. Wählen Sie "Add.IT.Other" aus der Spalte "Symbol" aus.

Die Seite "Add.IT.Other Change-Kategorie - Detail" wird angezeigt.

3. Klicken Sie auf "Bearbeiten".

Die Seite "Add.IT.Other - Change-Kategorie aktualisieren" wird angezeigt.

4. Klicken Sie auf die Registerkarte "Workflow".

Aktivieren Sie das Kontrollkästchen "CA Workflow".

Das Fenster "Workflow-Definitionen - Liste" wird angezeigt.

5. Wählen Sie "PC-Auftrag - Service Desk Version 12.9".

Das Feld "CA Workflow-Definitionsname" wird mit dem Prozessnamen ausgefüllt.

6. Klicken Sie auf "Speichern".

Die Seite "Change-Kategorie - Detail" wird aktualisiert.

7. Schließen Sie das Fenster.

8. Erstellen Sie und speichern Sie einen Change mit Hilfe der Kategorie "Add.IT.Other".

Auf der Registerkarte "Workflow-Tasks" wird der Prozess "PC-Auftrag - Service Desk Version 12.9" und die Liste der Arbeitselemente angezeigt.

9. Klicken Sie auf der Registerkarte "Workflow-Tasks" auf die Schaltfläche "Prozess anzeigen".

Der Prozess-Viewer wird angezeigt.

Hinweis: Sie können den aktualisierten Fortschritt der Workflow-Aufgaben anzeigen, indem Sie den Prozess-Viewer aktualisieren.

Change-Management-Prozessdefinition für CA Workflow

Die Change-Management-Prozessdefinition verwaltet Standard-, Normal-, oder Notfall-Changes. Als Teil des CA Workflow verwaltet die Change-Management-Prozessdefinition alle Change-Aufgaben vom ersten Change-Request mit Hilfe der Prüfung nach der Implementierung. Sobald eine Aufgabe abgeschlossen ist, aktualisiert die Change-Management-Prozessdefinition den Change-Status und das Aktivitätsprotokoll. Die Change-Management-Prozessdefinition informiert auch den Kontakt oder die Gruppe per E-Mail über Aufgaben, die abgeschlossen werden müssen.

Die Change-Management-Prozessdefinition schließt die folgende Funktionen ein:

- Analysiert den Change-Typ und das zugehörige Risikoniveau, um die notwendige Genehmigungsstufe für Change-Implementierungen festzulegen.
- Stellt eine Mustergrundlage als Grundlage für das Change Management bereit.
- Steht im Einklang den ITIL-v3-Standards für Risikoabschätzung, Auswirkungs- und Konfliktanalyse, und Genehmigungen sowohl durch den Change Manager Change als auch durch den CAB.
- Enthält die folgenden CA SDM-Change-Management-Funktionen:
 - Risikobewertungsumfrage
 - Geschäftsfall
 - Konfliktanalyse
 - Auswirkungsanalyse
 - Schließungscodes
 - Statuscodes
 - Change-Typ
 - CAB- und CAB-Zustimmungs-Flags

Weitere Informationen:

[CA Workflow](#) (siehe Seite 407)

Komponenten der Change-Management-Prozessdefinition

Die Change-Management-Prozessdefinition besteht aus folgenden Komponenten:

- **Change-Management-Prozessdefinition** - Die Prozessdefinition, die den gesamten Change-Prozess verwaltet. Alle Aktivitäten und Unteraktivitäten richten sich nach den aktuellen bewährten Praktiken zur Verarbeitung von Ausnahmen von CA Workflow. Der Dateiname der Prozessdefinition lautet *r12_Change_Mgmt_[en_language].xml*. Zum Beispiel lautet der englische Name der Prozessdefinition "r12_Change_Mgmt_en_US.xml".

Hinweis: Informationen zu den bewährten Praktiken von CA Workflow finden Sie unter

https://support.ca.com/irj/portal/anonymous/phpdocs?filePath=0/7956/7956_tecdoc.html.

- **Prozessdefinition Get Group Mem and Notify** - Ein Baustein, der E-Mail-Benachrichtigungen für Gruppen verwaltet. Die Prozessdefinition "Get Mem and Notify" akzeptiert den Gruppen-UUID als Eingabe. Je nach Benachrichtigungs-Flag kann die Prozessdefinition "Get Mem and Notify" eine E-Mail an jedes Gruppenmitglied oder nur an den Manager der Gruppe schicken. Der Dateiname der Prozessdefinition lautet *r12_Get_Group_Mem_Notify_[en_language].xml*. Zum Beispiel lautet der Dateiname der englischen Prozessdefinition "r12_Change_Mgmt_en_US.xml".
- **Akteur "Get Group Mem and Notify"** - Ein Akteur, der die Prozessdefinition "Get Mem and Notify" aufruft. Der Dateiname des Akteurs lautet *r12_Get_Group_Mem_Notify_Actor_[en_language].xml*. Zum Beispiel lautet der englische Name des Akteurs "r12_Get_Group_Mem_Notify_Actor_en_US.xml".
- **Date and Time Convert** - Ein Akteur, der Datum und Uhrzeit als Eingaben akzeptiert und eine lesbare Zeichenkette aus Datum und Uhrzeit für die Felder "Geplantes Startdatum" und "Geplantes Enddatum" auf den Genehmigungsformularen bereitstellt. Der "Date and Time Convert"-Akteur ist ein CA Workflow-JavaScript-Akteur. Der Dateiname des Akteurs lautet *r12_Date_Time_Convert_Actor_[en_language].xml*. Zum Beispiel lautet der englische Dateiname des Akteurs "r12_Date_Time_Convert_Actor_en_US.xml".

Einrichten der Change Management-Vorgangsdefinition

Zum Einrichten der Change Management-Vorgangsdefinition gehen Sie wie folgt vor:

1. [Überprüfen Sie mithilfe von CA Workflow die Dokumentation](#) (siehe Seite 844) zu Aktivitätsknoten, Unteraktivitäten und Benachrichtigungen.
2. Erstellen Sie die [CAB- und Implementierungsgruppen](#) (siehe Seite 845), die für die Verwaltung des Change-Vorgangs verantwortlich sind.

3. [Erstellen Sie Kontakte](#) (siehe Seite 847), und weisen Sie diese den CAB- oder Implementierungsgruppen zu.
4. [Konfigurieren Sie E-Mail-Benachrichtigungen](#) (siehe Seite 845) für die Change Management-Vorgangsdefinition.
5. Wenn Sie nicht den standardmäßigen Tomcat-Server-Port 8090 verwenden, [konfigurieren Sie den Tomcat-Server](#) (siehe Seite 848) für die entsprechende Kommunikation zwischen CA Workflow und CA SDM.
6. [Konfigurieren Sie einen oder mehr Change-Kategorien](#) (siehe Seite 848) die Change-Management-Vorgangsdefinition zu benutzen.
7. [Installieren Sie die Option "Kategorie-Standardwerte"](#) (siehe Seite 849) im Optionsmanager.

Anzeigen der Dokumentation über Aktivitätsknoten und Attribute

Da alle Aktivitätsknoten und Attribute innerhalb der Change-Management-Prozessdefinition dokumentiert sind, können Sie CA Workflow benutzen, um Informationen über Aktivitätsknoten und Attribute anzuzeigen. Im Bedarfsfall können Sie den Fluss der Prozessdefinition ändern, um diesen an Ihre Organisation anzupassen.

Hinweis: Informationen zur Anzeige von Aktivitätsknoten und Attributen finden Sie in der CA Workflow-Dokumentation.

So zeigen Sie die Dokumentation über Aktivitätsknoten und Attribute an:

1. Öffnen Sie die Change Mgmt - Service Desk r12.1-Prozessdefinition in der CA Workflow-Anwendung.
Die Change-Management-Prozessdefinition erscheint in CA Workflow.
2. Doppelklicken Sie auf einen Aktivitätsknoten.
Nun wird der Aktivitätsknoten geöffnet.
3. Überprüfen Sie auf der Registerkarte "Eigenschaften" das Feld "Beschreibung" auf zusätzliche Details über den Knoten.
4. Verlassen Sie die Eigenschaften des Aktivitätsknotens.
5. (Optional) Navigieren Sie im unteren Fenster der Prozessdefinition zur Registerkarte "Attribute".
6. Doppelklicken Sie auf das Attribut oder bewegen Sie den Mauszeiger darüber.
Nun wird die Seite "Attribut" mit Informationen über das Attribut geöffnet.

Anzeigen von Unteraktivitäten

Die Change-Management-Prozessdefinition benutzt verschiedene CA Workflow-Unteraktivitäten, um den Arbeitsablauf zu vereinfachen. Während der Arbeit mit der Change-Management-Prozessdefinition können Sie die Unteraktivitäten im Bedarfsfall prüfen und anpassen.

So zeigen Sie Unteraktivitäten an:

1. Öffnen Sie die Change Mgmt - Service Desk r12.1-Prozessdefinition in der CA Workflow-Anwendung.

Die Change-Management-Prozessdefinition erscheint in CA Workflow.

2. Klicken Sie mit der linken Maustaste auf einen Knoten mit einem Plussymbol (+) und wählen Sie "Registerkarte öffnen" oder "Inline anzeigen".

Der Details zur Unteraktivität werden auf einer neuen Registerkarte oder neben den Prozessdefinitionsaktivitäten angezeigt.

Einrichten von E-Mail-Benachrichtigungen für Change Management-Kontakte

Das System versendet E-Mail-Benachrichtigungen über Change-Aufgabenzuweisungen und Statusänderungen. Zur weiteren Überprüfung enthalten E-Mail-Benachrichtigungen Verknüpfungen zu der Arbeitsliste oder dem Change. Da die Change Management-Vorgangsdefinition E-Mail-Benachrichtigungen versendet, ist eine E-Mail-Konfiguration erforderlich.

Zum Einrichten von E-Mail-Benachrichtigungen für Change Management-Kontakte gehen Sie wie folgt vor:

1. Wählen Sie auf der Registerkarte "Administration" die Optionen "Optionsmanager" > "E-Mail".

Die Optionsliste wird angezeigt.

2. Konfigurieren Sie die E-Mail-Optionen je nach den Anforderungen Ihrer Organisation.

Hinweis: Informationen zum Konfigurieren von E-Mail finden Sie in der *Online-Hilfe*.

Erstellen von Change Management-Vorgangsgruppen

Wenn Sie Change Management-Vorgangsgruppen erstellen, die für Genehmigungen und weitere Aufgaben zuständig sind, berücksichtigen Sie folgende Punkte:

- Sie können einen beliebigen Gruppennamen verwenden, solange die CA SDM- und CA EEM-Namen übereinstimmen.
- Der Gruppenname in CA SDM muss außerdem mit dem Gruppenordnernamen in CA EEM übereinstimmen.

- Jede Gruppe muss mehr als ein Mitglied haben.
- Die Gruppenmitglieder in CA SDM und CA EEM stimmen überein. Wenn z. B. die CAB-Gruppe von CA SDM vier Mitglieder hat, hat die CAB-Gruppe von CA EEM dieselben Mitglieder.

Hinweis: Informationen zum Erstellen von CA SDM- und CA EEM-Gruppen finden Sie in der *Online-Hilfe* und der CA EEM-Dokumentation.

Zum Erstellen von Change Management-Gruppen gehen Sie wie folgt vor:

1. Wählen Sie auf der Registerkarte "Administration" die Optionen "Sicherheits- und Rollenmanagement" > "Gruppen".

Die Seite "Gruppe - Suche" wird angezeigt.

2. Klicken Sie auf "Neu erstellen".

Die Seite "Neue Gruppe erstellen" wird angezeigt.

3. Erstellen Sie die folgenden Gruppen in CA SDM:

- **CAB-Gruppe:** Eine CAB-Gruppe, die der Change-Kategorie oder dem Change zugeordnet ist.
- **Implementierungsgruppe:** Eine Implementierungsgruppe, die der Change-Kategorie oder dem Change zugewiesen ist.

4. Klicken Sie auf "Speichern".

Die Seite "Gruppe - Detail" wird angezeigt.

5. Erstellen Sie dieselben Gruppen in CA EEM.

Weitere Informationen:

[Verwalten von CAB-Gruppen](#) (siehe Seite 866)

[Zuweisen von CAB-Gruppen](#) (siehe Seite 868)

Erstellen von Change-Management-Prozess-Kontakten

Wenn Sie mit der Change-Management-Prozessdefinition arbeiten, erstellen Sie Kontakte, die während des Change-Prozesses für Genehmigungen und zusätzliche Aufgaben verantwortlich sind. Sie weisen den [Change-Management-Prozess-Gruppen](#) (siehe Seite 845) auch Kontakte zu.

Um die Change-Management-Prozess-Kontakte zu erstellen, gehen Sie folgendermaßen vor:

1. Wählen Sie auf der Registerkarte "Administration" die Option "Sicherheits- und Rollenmanagement" > "Kontakte" aus.
Die Seite "Kontakt – Suche" wird angezeigt.
2. Klicken Sie auf "Neu erstellen".
Das Fenster "Neuen Kontakt erstellen" wird angezeigt.
3. Erstellen Sie die folgenden Kontakte mit gültigen E-Mail-Adressen und weisen Sie sie den entsprechenden Gruppen zu:
 - **Angefordert von** - Ein oder mehrere Kontakte, die den Change Request absenden
 - **Change Manager** - Kontakt, der als Manager der Implementierungsgruppe fungiert. Die Implementierungsgruppe kann nur einen Change Manager haben.
 - **CAB-Manager** - Kontakt, der als Manager der CAB-Gruppe fungiert. Die CAB-Gruppe kann nur einen CAB-Manager haben.Die Registerkarte " Kontaktdetails - Gruppen" listet die aktuellen Gruppenzuweisungen auf.
4. Setzen Sie auf der Registerkarte "Mitglieder" der Detailseite für die Implementierungsgruppe den Manager-Flag für den Change Manager und den CAB-Manager.
5. Klicken Sie auf "Speichern".
Die Registerkarte "Mitglieder" zeigt für folgende Kontakte "Manager-Ja" an:
 - Change Manager
 - CAB Manager
6. Erstellen Sie dieselben Kontakte in CA EEM und weisen Sie sie den CA EEM-Gruppen zu.

Hinweis: Die Kontaktnamen können einen beliebigen gültigen Benutzernamen oder eine beliebige gültige Systemanmeldung verwenden. Informationen zum Erstellen von CA SDM- und CA EEM-Kontakten finden Sie in der *Online-Hilfe* und der CA EEM-Dokumentation.

Angabe eines Ausweichports für den CA Workflow-Tomcat-Server

Wenn der CA Workflow-Tomcat-Server auf einem anderen Port als dem Standard-Port 8090 läuft, konfigurieren Sie den Port so, dass CA Workflow mit CA SDM kommuniziert.

So geben Sie einen Ausweichport für den CA Workflow-Tomcat-Server an:

1. Öffnen Sie die CA Workflow-Anwendung.
Nun wird die Seite "CA Workflow" angezeigt.
2. Klicken Sie auf die Registerkarte "Akteure".
Es wird die Liste mit den Akteurtypen/Akteuren angezeigt.
3. Wählen Sie "JavaScript" > "USD_Initializer" aus.
Es wird die Seite "Aktivitätsoptionen CA Workflow" angezeigt.
4. Doppelklicken Sie auf "Globale Attribute abrufen".
Es wird die Seite für den JavaScript-Betrieb angezeigt.
5. Tragen Sie als WFTomcatPort-Wert den neuen, von CA Workflow-Tomcat verwendeten Port ein.
6. Klicken Sie auf "OK".
Der Tomcat-Server ist so konfiguriert, dass CA Workflow mit CA SDM kommuniziert.

Konfiguration der Change-Kategorie

Wenn Sie die Change-Kategorie für die Change-Management-Prozessdefinition angeben, startet jeder neue Change, der die Kategorie verwendet, automatisch die Change-Management-Prozessdefinition. Alle vorkonfigurierten Change-Kategorie-Werte werden automatisch im Change eingegeben.

So konfigurieren Sie die Change-Kategorie:

1. Wählen Sie auf der Registerkarte "Administration" "Service Desk Manager" > "Changes" > "Kategorien" aus.
Die Seite "Change-Kategorien - Liste" wird angezeigt.
2. Erstellen oder öffnen Sie eine bestehende Change-Kategorie.
Die Seite "Change-Kategorie – Detail" wird angezeigt.
3. Klicken Sie auf der Registerkarte "Workflow" auf "CA Workflow verwenden".
4. Klicken Sie auf die Verknüpfung "CA Workflow-Definition".
Nun wird das Fenster "CA Workflow-Definitionen - Liste" angezeigt.
5. Klicken Sie auf "Change Mgmt - Service Desk r12.1".
6. Klicken Sie auf "OK".
Die Seite "Change-Kategorie – Detail" wird angezeigt.

7. (Optional) Weisen Sie CAB, Gruppe und Risikoumfrage zu.
8. Klicken Sie auf "Speichern".

Der nächste neue Change, der diese Kategorie verwendet, startet automatisch die Change-Management-Prozessdefinition mit den Werten in der Change-Kategorie.

Hinweis: Information zum Erstellen oder Bearbeiten von Change-Kategorien finden Sie in der *Online-Hilfe*.

Installieren Sie die Option "Category_Defaults" im Optionsmanager

Die Option "Category_Defaults" verwendet Kategoriefelder, um die CAB-Gruppe und die Risikoumfrage auf dem Change auszufüllen. Die CAB-Gruppe, die Sie für eine Kategorie angeben, wird beispielsweise auf allen neuen Changes angezeigt, die diese Kategorie verwenden.

So installieren Sie die Option "Category_Defaults" im Optionsmanager

1. Wählen Sie auf der Registerkarte "Administration" die Optionen "Optionsmanager" > "Change Manager" > "Category_Defaults".

Das Fenster "Optionen - Liste" wird angezeigt.

2. Klicken mit der rechten Maustaste auf "Edit Category_Defaults" ("Category_Defaults" bearbeiten).

Die Seite "Optionen aktualisieren" für "Category_Defaults" wird angezeigt.

3. Klicken Sie auf "Installieren".
4. Starten Sie die CA SDM-Dienste neu.

Neue Changes enthalten automatisch Werte aus der Kategorie.

Funktionsweise der Change Management-Prozessdefinitionen

Wenn ein Anforderer einen Change mit einer Kategorie speichert, die die Change-Management-Prozessdefinition verwendet, wird die Change-Management-Prozessdefinition automatisch aufgerufen.

Die folgenden Schritte beschreiben, wie die Change-Management-Prozessdefinition in CA SDM funktioniert:

1. Der Anforderer öffnet und speichert einen Change, der die folgende Information beinhaltet:

Angefordert von

Identifiziert die Person, die den Change öffnete.

Änderungskategorie

Identifiziert die Change-Kategorie.

Typ

Identifiziert den Change-Typ wie beispielsweise Standard-, Normal-, oder Dringende Changes. Der Typ kann auch als Teil des Workflow-Prozesses aktualisiert werden.

Summary/Description

Beschreibt den Grund für den Change.

Geplantes Startdatum

Gibt das Startdatum an.

Dauer

Gibt die geschätzte Zeit für den Change an.

CIs

Identifiziert mindestens ein betroffenes CI.

Die Change-Management-Prozessdefinition wird gestartet. Der Anforderer erhält eine E-Mail-Benachrichtigung zum Abschluss der Risikobewertungsumfrage.

2. Der Anforderer überprüft den Change und schließt die [Risikobewertungsumfrage](#) (siehe Seite 857) ab, die beschreibt, wie sich der Change auf Server, Anwendungen und Anwender auswirkt.

Die Change-Management-Prozessdefinition analysiert die Antworten, um das Risiko zu ermitteln und sicherzustellen, dass der Change dem entsprechenden Prozesspfad folgt. Der Anforderer erhält eine E-Mail-Benachrichtigung zur Ausführung der Konflikt- und Auswirkungsanalyse.

3. Während der [Konflikt- und Auswirkungsanalyse](#) (siehe Seite 858) sucht der Anforderer nach Planungskonflikten und analysiert die Auswirkung des Change auf CIs.

Der Anforderer erhält eine E-Mail-Benachrichtigung zum Durchführen einer Change-Analyse.

4. Während der [Change-Analyse](#) (siehe Seite 859) identifiziert und übermittelt der Anforderer den Change-Typ, den Grund für den Change, die Geschäftsauswirkung und die allgemeine Auswirkung des Change.

Der Change Manager erhält eine E-Mail-Benachrichtigung zur Genehmigung des Change. Wenn der Change ein hohes Risiko bedeutet, erhält die CAB-Gruppe auch eine Benachrichtigung.

5. Der Change Manager überprüft die Änderungsanalyse und gibt Kommentare über die Prüfung ein. Der Change Manager [genehmigt den Change, lehnt ihn ab oder markiert ihn als unvollständig](#) (siehe Seite 858).

Das System aktualisiert die Change-Detailseite dementsprechend und antwortet mit einer der folgenden Aktionen:

- Wenn der Change genehmigt und keine CAB-Zustimmung benötigt wird, erhält die Implementierungsgruppe eine Benachrichtigung. Der Change zeigt "Status - Genehmigt" an.
- Wenn der Change genehmigt wird und zusätzliche CAB-Genehmigungen benötigt werden, erhalten der CAB-Manager und Mitglieder eine Benachrichtigung zur Genehmigung. Der Change zeigt "Status - Genehmigung in Bearbeitung" an.
- Wenn der Change abgelehnt wird, zeigt der Change "Status - Abgelehnt" an.
- Wenn der Change als unvollständig markiert ist, zeigt der Change "Status - Unvollständig".

6. Für genehmigte Changes bestätigt ein Mitglied der Implementierungsgruppe den [Beginn der Implementierung](#) (siehe Seite 862) und implementiert den Change.

Der Change zeigt "Status - Implementierung in Bearbeitung" an.

7. Wenn die Arbeit abgeschlossen ist, schließt der Implementierungs-Manager die [Prüfung nach der Implementierung](#) (siehe Seite 864) (PIR) ab, um Details über das Ergebnis des Change zu beschreiben.

CA Workflow schließt den Change. Der Change zeigt einen Abschluss-Code und "Status - Implementiert" an.

Weitere Informationen:

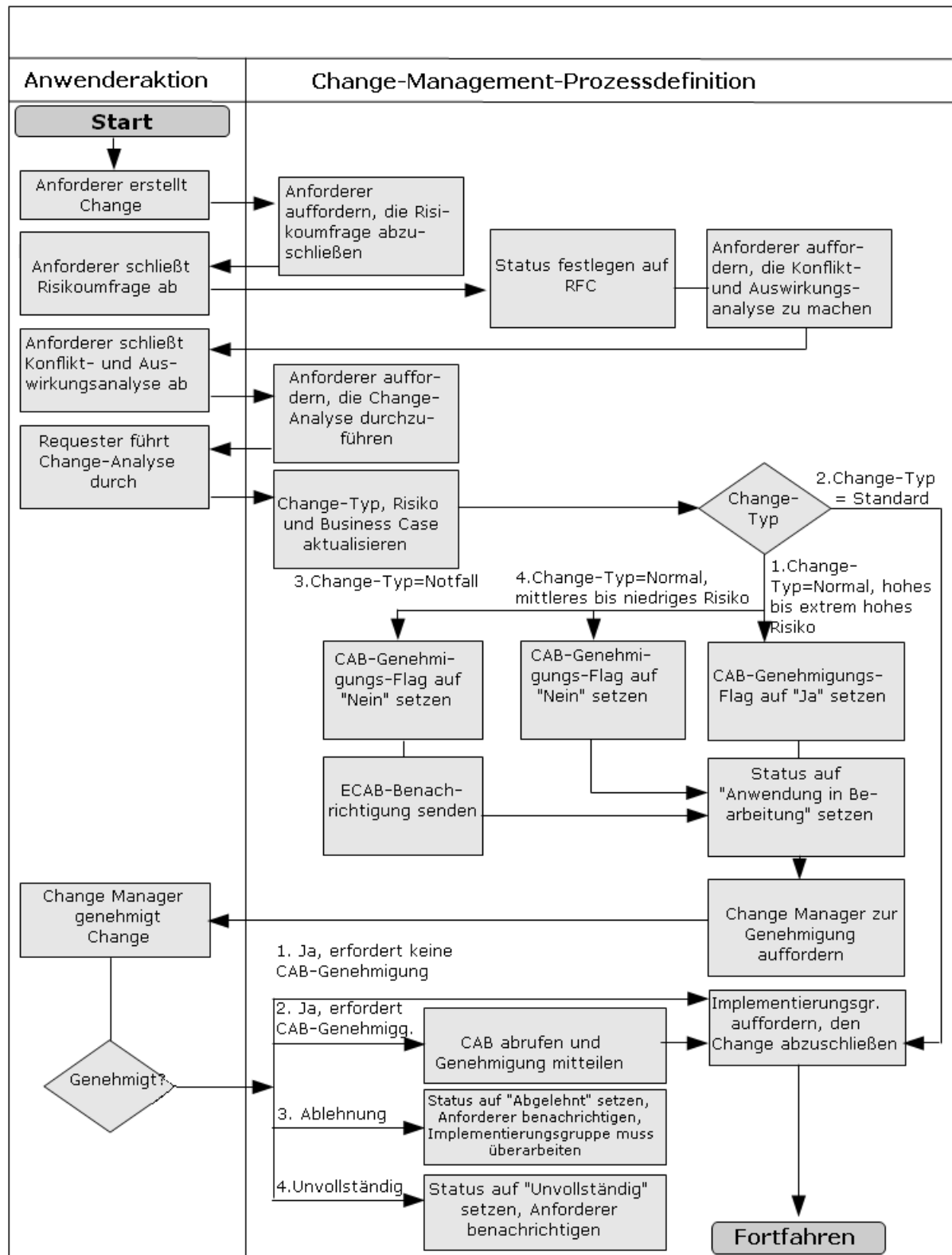
[Anzeigen von Standardrisikoumfragen](#) (siehe Seite 872)

[So implementieren Sie die Risikoumfrage:](#) (siehe Seite 872)

[Einrichten der Change Management-Vorgangsdefinition](#) (siehe Seite 843)

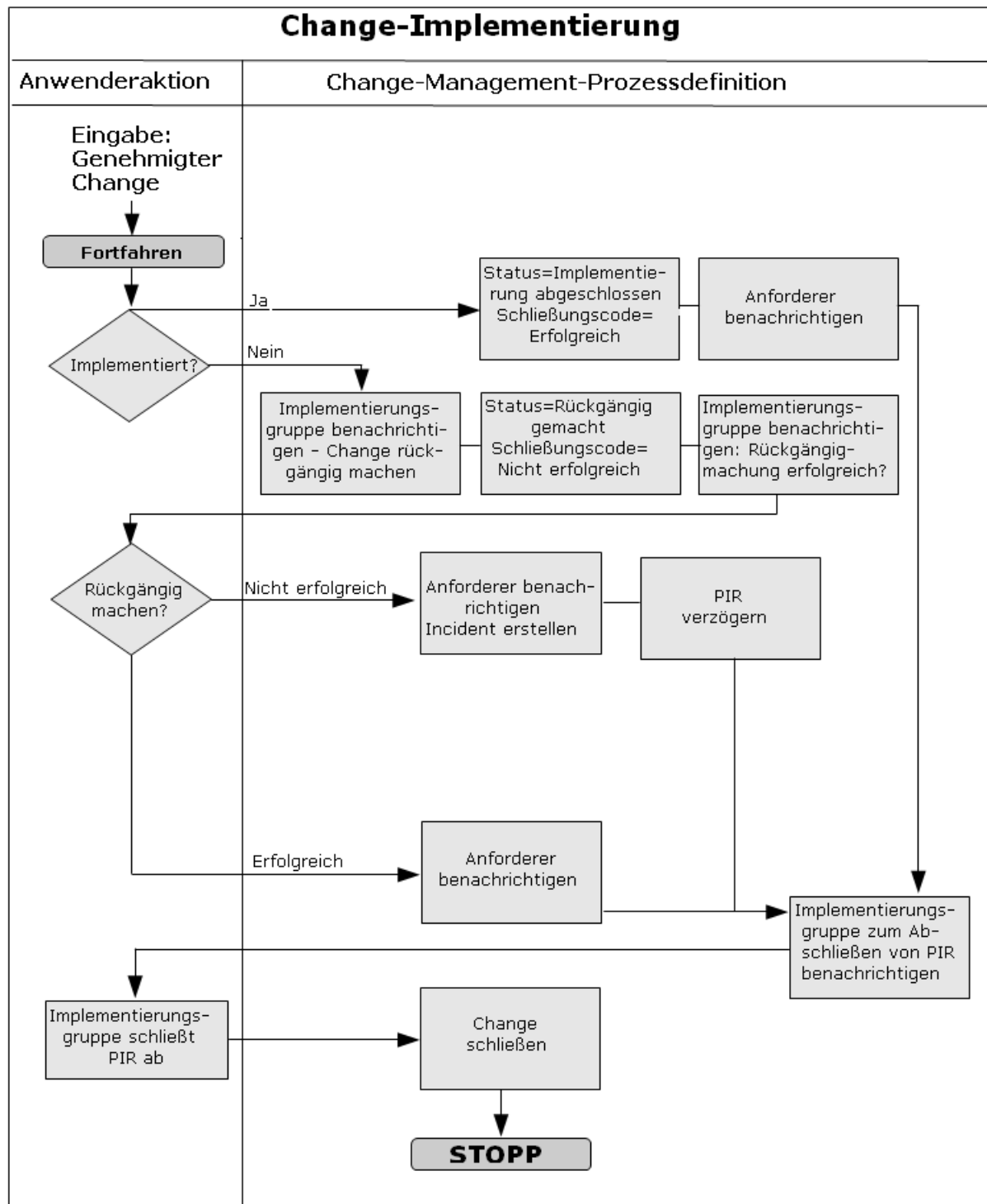
Verwalten von Change-Genehmigungen durch die CM-Vorgangsdefinition

Das folgende Diagramm zeigt, wie die [Change Management-Vorgangsdefinition](#) (siehe Seite 849) Genehmigungen für einen neuen Change verwaltet.



Verwalten von CO-Implementierungen durch die CM-Vorgangsdefinition

Das folgende Diagramm zeigt, wie die [Change Management-Vorgangsdefinition](#) (siehe Seite 849) die Change-Implementierung verwaltet.



Abschluss der Risikobewertungsumfrage

Wenn Sie einen Change erstellen, teilt Ihnen das System mit, die Risikobewertungsumfrage abzuschließen, die der Change-Kategorie zugeordnet ist. Als Anforderer identifizieren, bewerten und quantifizieren Sie die Risiken von Changes, die zu Change-Kategorien gehören, bevor ein System oder Service verändert wird.

So schließen Sie die Risikobewertungsumfrage ab:

1. Öffnen Sie den Change durch Klicken auf die Verknüpfung in der E-Mail-Benachrichtigung zur Risikobewertungsumfrage.
Das Fenster "Change - Detail" wird angezeigt.
2. Klicken Sie auf der Registerkarte "Workflow-Aufgaben" auf die Verknüpfung der Risikobewertungsumfrage des Anforderers und folgen Sie den Anweisungen zum Abschließen der Umfrage.
Es wird die CA Workflow-Worklist angezeigt.
3. Klicken Sie auf der Registerkarte "Aufgaben" auf die Verknüpfung "Durchführen".
Es wird die Seite zum Ausführen von Aufgaben angezeigt.
4. Notieren Sie sich die Anweisungen und klicken Sie auf die Verknüpfung.
Es wird die Risikoumfrage angezeigt.
5. Beantworten Sie gewissenhaft die Fragen aus der Umfrage, so dass der Workflow des Change Management-Prozesses den entsprechenden Risikopfad für den Change sorgfältig bewerten kann.
6. Klicken Sie auf "Absenden".
Es wird die Seite zum Ausführen von Aufgaben angezeigt.
7. Klicken Sie auf "Bestätigen".
Die Change-Detailseite zeigt "Status - RFC" an. Der Anforderer erhält eine E-Mail-Benachrichtigung zur Durchführung einer Konflikt- und Auswirkungsanalyse.

Weitere Informationen:

[Zugreifen auf eine Risikoumfrage direkt über eine URL](#) (siehe Seite 874)

Durchführen einer Konflikt- und Auswirkungsanalyse

Während der Konflikt- und Auswirkungsanalyse sucht der Anforderer nach Planungskonflikten und analysiert die Auswirkung des Change auf CIs.

So führen Sie eine Konflikt- und Auswirkungsanalyse durch:

1. Öffnen Sie den Change, indem Sie auf die Verknüpfung der E-Mail-Benachrichtigung klicken.

Das Fenster "Change - Detail" wird angezeigt.

2. Klicken Sie auf der Registerkarte "Workflow-Aufgaben" auf die Verknüpfung für die Auswirkungs- und Konfliktanalyse des Anforderers.

Es wird die Seite "Aufgaben" angezeigt.

3. Klicken Sie auf der Registerkarte "Aufgaben" auf die Verknüpfung "Durchführen".

Es wird die Seite zum Ausführen von Aufgaben angezeigt.

4. Notieren Sie sich die Anweisungen zur Auswirkungs- und Konfliktanalyse und klicken Sie auf die Verknüpfung.

Das Fenster "Change - Detail" wird angezeigt.

5. Klicken Sie auf der Registerkarte "Change-Konflikte" auf "Konfliktanalyse", um alle Planungs- und ausstehenden Konflikte zu lösen. Lösen Sie alle Konflikte, bevor Sie den Change implementieren.

Es wird die Konfliktliste angezeigt.

6. Klicken Sie auf der Registerkarte "Config. Items" auf "Auswirkungsanalyse", um die Details zu den CIs zu prüfen.

Die Seite Configuration Item-Liste wird angezeigt.

7. Klicken Sie auf der Registerkarte "Elemente" auf "Auswirkungs-Explorer", um Informationen zu jedem CI zu überprüfen.

Nun wird der Auswirkungs-Explorer geöffnet.

8. Klicken Sie auf Visualizer, um eine Grafik der CI-Beziehungen anzuzeigen.

Hinweis: Die Visualizer-Schaltfläche ist nur verfügbar, wenn CA CMDB installiert ist.

9. Kehren Sie zur Seite zum Durchführen der Aufgabe zurück und klicken Sie auf "Bestätigen".

Die Registerkarte "Workflow-Aufgaben" zeigt eine Verknüpfung für den Start der Change-Analyse. Der Anforderer erhält eine E-Mail-Benachrichtigung zum Durchführen einer Change-Analyse.

Weitere Informationen:

[Auswirkungs-Explorer](#) (siehe Seite 875)

[Starten von CMDB Visualizer im Auswirkungs-Explorer](#) (siehe Seite 878)

Durchführen der Change-Analyse

Während der Change-Analyse identifiziert und zeichnet der Anforderer folgende Informationen auf:

- Change-Typ
- Grund für den Change
- Geschäftsauswirkung
- Umfassende Auswirkung des Change

So führen Sie eine Change-Analyse durch:

1. Öffnen Sie den Change, indem Sie auf die Verknüpfung der E-Mail-Benachrichtigung klicken.

Das Fenster "Change - Detail" wird angezeigt.

2. Klicken Sie auf der Registerkarte "Workflow-Aufgaben" auf die Verknüpfung zum Change-Analyse-Formular des Anforderers.

Es wird die Seite "Aufgaben" angezeigt.

3. Klicken Sie auf der Registerkarte "Aufgaben" auf die Verknüpfung "Durchführen".

Nun wird die Seite "Change-Analyse" angezeigt.

4. Beantworten Sie auf der Registerkarte "Chg Analyse" die Fragen, um den Change zu bestätigen, und klicken Sie auf "Absenden". Fassen Sie zum Beispiel Ihre Analyse zusammen und erklären Sie den Zweck des Change. Geben Sie bei Bedarf an, ob der Change eine Wiederholung oder eine Überarbeitung ist. Fassen Sie die Geschäftsauswirkung und die Gesamtauswirkung des Change zusammen.

Basierend auf dem Change-Typ und dem Risiko führt das System folgende Aktionen durch:

- Wenn der Change-Typ "Normal" mit einem hohen bis extremen Risiko ist, zeigt die Change-Detailseite Folgendes an:
 - CAB-Genehmigung - Ja
 - Status - Genehmigung in Bearbeitung

Das System bittet den Change Manager, den Change zu genehmigen. Nach der Genehmigung durch den Change Manager wird die CAB-Gruppe mit einer Benachrichtigung um zusätzliche Genehmigung gebeten.

- Wenn der Change-Typ "Normal" mit einem mittleren bis niedrigen Risiko ist, zeigt die Change Detailseite Folgendes an:

- CAB-Genehmigung - Nein
- Status - Genehmigung in Bearbeitung

Das System bittet den Change Manager, den Change zu genehmigen.

- Wenn der Change-Typ "Standard" ist, fordert das System mit einer Benachrichtigung die Implementierungsgruppe auf, den Change zu implementieren.

- Wenn der Change-Typ "Dringend" ist, zeigt die Change-Detailseite die "CAB-Genehmigung - Nein" an.

Das System benachrichtigt das ECAB. Nachdem das ECAB den Change verarbeitet hat, zeigt die Change-Detailseite "Status - Genehmigung in Bearbeitung", und der Change Manager erhält eine Benachrichtigung mit der Bitte um Genehmigung des Change.

Genehmigen, Ablehnen oder Markieren eines Change als unvollständig

Der Change-Typ und die Risikoebene bestimmen den Genehmigungsvorgang für Changes, die die Change Management-Vorgangsdefinition verwenden. Die Change-Genehmiger werden von folgenden Change-Werten bestimmt:

- Ist der Typ auf "Normal" und das Risiko auf "Mittel" bis "Niedrig" gesetzt, erfordert der Change nur die Genehmigung des Change Managers.
- Ist der Typ auf "Normal" und das Risiko auf "Hoch" bis "Extrem" gesetzt, erfordert der Change die Genehmigung eines CAB-Mitglieds.
- Ist der Typ auf "Standard" gesetzt, sind keine Genehmigungen erforderlich. Das System benachrichtigt die Implementierungsgruppe, den Change zu bearbeiten.
- Ist der Typ auf "Notfall" gesetzt, benachrichtigt das System die ECAB-Gruppe. Der Change weist den Status "Genehmigung in Bearbeitung" auf. Wenn der Change genehmigungsbereit ist, benachrichtigt das System den Change Manager.

Als Genehmiger überprüfen Sie die Change-Analyseinformationen und entscheiden, ob der Change genehmigt, abgelehnt oder als unvollständig gekennzeichnet werden soll.

So können Sie einen Change genehmigen, ablehnen oder als unvollständig kennzeichnen

1. Öffnen Sie den Change, indem Sie auf die Verknüpfung für die E-Mail-Benachrichtigung klicken.

Das Fenster "Change - Detail" wird angezeigt.

2. Klicken Sie auf der Registerkarte "Workflow-Aufgaben" auf die Verknüpfung für das Change Manager-Genehmigungsformular.

Die Seite "Aufgaben" wird angezeigt.

3. Klicken Sie auf der Registerkarte "Aufgaben" auf die Verknüpfung "Perform" (Ausführen).

Die Seite "CAB-Genehmigung" oder "Change Manager Approval" (Change Manager-Genehmigung) wird angezeigt.

4. Überprüfen Sie die Registerkarte "Chg Analysis" (Change-Analyse) auf weitere Informationen zu dem Change.

5. Wählen Sie je nach erforderlicher Genehmigungsstufe eine der folgenden Genehmigungsregisterkarten aus, und beantworten Sie die Genehmigungsfragen:

Chg Mgr Approval (Change Manager-Genehmigung)

Beschreibt die Entscheidung des Change Managers für den Change.

CAB-Genehmigung

Beschreibt die Entscheidung des CAB-Genehmigers für den Change.

6. Wählen Sie eine der folgenden Genehmigungsstufen aus:

Genehmigen

Akzeptiert den Change.

Ablehnen

Lehnt den Change ab.

Unvollständig

Kennzeichnet den Change als unvollständig.

Die Seite "Result" (Ergebnis) wird angezeigt. Je nach Genehmigungsstufe können folgende Aktionen erfolgen:

- Wenn Sie den Change genehmigen und keine weitere CAB-Genehmigung erforderlich ist, zeigt die Seite "Changes – Detail" den Status "Genehmigt" an, und die Implementierungsgruppe erhält eine Benachrichtigung, mit der Arbeit zu beginnen.
- Wenn Sie den Change genehmigen und CAB-Genehmigung erforderlich ist, zeigt die Seite "Changes – Detail" den Status "Genehmigung in Bearbeitung" an. Die CAB-Gruppe erhält ebenfalls eine Benachrichtigung.
- Wenn Sie den Change ablehnen, zeigt die Seite "Changes – Detail" den Status "Abgelehnt" an, und sowohl der Anforderer als auch die Implementierungsgruppe erhalten eine Benachrichtigung.
- Wenn der Change unvollständig ist, zeigt die Seite "Changes – Detail" den Status "Unvollständig" an, und der Anforderer erhält eine Benachrichtigung.

Weitere Informationen:

[Funktionsweise der CAB-Prozessdefinitionen](#) (siehe Seite 810)

[CAB-Genehmigungen](#) (siehe Seite 868)

[CAB-Zuständigkeiten](#) (siehe Seite 810)

Implementieren eines Change

Die Implementierungsgruppe muss für den betreffenden Change mindestens ein Arbeitselement abschließen. Als Mitglied der Implementierungsgruppe geben Sie Informationen zu dem Change weiter.

Gehen Sie wie folgt vor:

1. Melden Sie sich als Mitglied der Implementierungsgruppe bei CA SDM an, und öffnen Sie den Change.
Die Seite "Change - Detail" wird geöffnet.
2. Klicken Sie unter Weitere Informationen auf der Registerkarte Workflow-Aufgaben auf die Verknüpfung Implement Change Order (Change implementieren).
Die Seite "Aufgabenliste" wird geöffnet.
3. Klicken Sie auf der Registerkarte "Aufgaben" auf die Verknüpfung "Perform" (Ausführen).
Die Seite "Perform Tasks" (Aufgaben ausführen) wird geöffnet.
4. Befolgen Sie die Anweisungen zur Überprüfung des Change, und klicken Sie auf "Bestätigen".
Die Seite "Changes – Detail" zeigt den Status "Implementierung in Bearbeitung" an.
5. Implementieren Sie die Änderung. Wenn der Change z. B. angewiesen hat, ein AntiVirus-Patch auf Exchange-Server 1 und Exchange-Server 2 zu installieren, schließen Sie den Change gemäß den Richtlinien und Standards Ihres Unternehmens ab.
6. Klicken Sie auf der Registerkarte "Workflow-Aufgaben" auf die Verknüpfung "Implement Complete Form" (Vollständiges Formular implementieren).
Die Seite "Aufgaben" wird geöffnet.

7. Klicken Sie auf der Registerkarte "Aufgaben" auf die Verknüpfung "Perform" (Ausführen).

Die Seite "Implementation Complete" (Implementierung vollständig) wird geöffnet.

8. Beantworten Sie die Fragen auf der Registerkarte "Implementation Complete" (Implementierung abgeschlossen), um zu beschreiben, wie Ihre Gruppe den Change implementiert hat, und klicken Sie auf eine der folgenden Optionen:

Abgeschlossen

Gibt an, dass alle Change-Aufgaben erfolgreich abgeschlossen wurden. Setzt den Change-Status auf "Implementation Complete" (Implementierung abgeschlossen) und den Schließungscode auf "Erfolgreich".

Unvollständig

Gibt an, dass ein oder mehrere Elemente des Change nicht abgeschlossen werden konnten.

Der Anforderer erhält eine oder mehrere Benachrichtigungen über den Abschluss empfängt einen oder mehr Benachrichtigungen über den Abschluss oder das Rückgängigmachen des Change. Das System reagiert außerdem in einer der folgenden Weisen:

- Wenn der Change abgeschlossen ist, zeigt die Seite "Change - Detail" Folgendes an:
 - Status: Implementation Complete (Implementierung abgeschlossen).
 - Schließungscode: Erfolgreich.

Das System benachrichtigt die Implementierungsgruppe, die Post-Implementierungsprüfung abzuschließen.

- Ist der Change unvollständig, zeigt die Seite "Changes – Detail" Folgendes an:
 - Status: Rückgängig gemacht
 - Schließungscode: Nicht erfolgreich

Außerdem benachrichtigt das System die Implementierungsgruppe, festzustellen, ob das Rückgängigmachen erfolgreich war.

Wenn das Rückgängigmachen erfolgreich ist, benachrichtigt das System die Implementierungsgruppe, die Post-Implementierungsprüfung abzuschließen. Ist das Rückgängigmachen nicht erfolgreich, erstellt das System einen Incident und benachrichtigt die Implementierungsgruppe, die Post-Implementierungsprüfung abzuschließen.

Abschließen der Prüfung nach der Implementierung

Nach Beenden der Arbeit schließt die Implementierungsgruppe die Prüfung nach der Implementierung (PIR) ab, die das Ergebnis des Change beschreibt. Als Mitglied der Implementierungsgruppe schließen Sie die PIR typischerweise drei bis sieben Tage nach der Implementierung des Change ab. Allerdings legt die Change Management-Prozessdefinition eine Standardverzögerung von zehn Sekunden für die Zuweisung dieser Aufgabe fest.

So schließen Sie die Prüfung nach der Implementierung ab:

1. Melden Sie sich bei CA SDM als Mitglied der Implementierungsgruppe an und öffnen Sie den Change.
Das Fenster "Change - Detail" wird angezeigt.
2. Klicken Sie auf der Registerkarte "Workflow-Aufgaben" auf die Verknüpfung zur Prüfung nach der Implementierung.
Nun wird die Aufgabenliste angezeigt.
3. Klicken Sie auf der Registerkarte "Aufgaben" auf die Verknüpfung "Durchführen".
Die Seite "PIR" wird angezeigt.
4. Beantworten Sie auf der Registerkarte "PIR" die Fragen, um die Behebung zu beschreiben, und klicken Sie auf "Absenden".
Die Change-Detailseite zeigt "Status - Geschlossen" an.

ActivityNode Actor not found: Update Object -Service Desk r12 ("ActivityNode"-Akteur nicht gefunden: Objekt -Service Desk r12 aktualisieren")

Symptom:

Das CA Workflow-Befehlsfenster zeigt den folgenden Fehler an:

ActivityNode Actor not found: Update Object -Service Desk r12 ("ActivityNode"-Akteur nicht gefunden: Objekt "-Service Desk r12" aktualisieren)

Lösung:

1. Melden Sie sich bei der CA Workflow-Anwendung an.
2. Klicken Sie auf die Registerkarte "Actors" (Akteure).
3. Wählen Sie den Ordner "Processes" (Vorgänge).

4. Wählen Sie "File" (Datei) > "New Actor" (Neuer Akteur).
5. Wählen Sie in der Drop-down-Liste die Option "Object -Service Desk r12" (Objekt "-Service Desk r12") aus.
6. Klicken Sie auf "OK".

Das System verwendet als Teil der Change Management-Vorgangsdefinition den neuen Akteur.

Change wird nicht geschlossen

Symptom:

Während des letzten Schritts im Workflow wird der Change nicht geschlossen. Die CA Workflow-Prozessinstanz zeigt den Status "Wird ausgeführt" an, und CA Workflow meldet einen Akteurfehler zurück.

Lösung:

Überprüfen Sie beim Schließen des Change, ob alle obligatorischen Felder wie beispielsweise die Ursache ausgefüllt wurden.

CAB-Konsole und Berichterstattung

Die CAB-Konsole ist ein Dashboard, das schnelle Online-Genehmigungen von Changes, die eine CAB-Genehmigung erfordern, ermöglicht. Der Change Manager und andere CAB-Mitglieder verwenden die Konsole, um Details über einen Change (und seine verknüpften Workflow-Aufgaben und Configuration Items) anzuzeigen, und genehmigen den Change oder lehnen ihn ab. Mit der CAB-Konsole können Teammitglieder einen Change überprüfen, genehmigen oder ablehnen, und dann mit dem nächsten Change fortfahren. Bei Change Requests kann das CAB die Requests bearbeiten, indem es sie direkt genehmigt oder an eine geeignete Gruppe eskaliert bzw. verweist.

Der Change Manager kann die Funktionalität von CA SDM zur Erstellung von zusammengefassten Berichten und Detailberichten verwenden, um folgende Aufgaben auszuführen:

- Berichte über genehmigte und abgelehnte Changes erstellen
- Berichte über Changes erstellen, die auf Genehmigung warten

Zum Drucken oder Anzeigen von zusammengefassten Berichten oder Detailberichten wählen Sie zuerst die Datensätze aus, die Sie in den Bericht einschließen möchten. Sie können bestimmte Datensätze für einen Bericht mit der Suchfunktion von Listenseiten auswählen.

Zum Beispiel können Sie aus der Change-Liste Suchkriterien eingeben, um eine Liste der Changes zu generieren, die auf die CAB-Genehmigung warten, und diese dann verwenden, um einen Bericht zu erstellen.

Hinweis: Weitere Informationen über das Generieren von zusammengefassten Berichten und Detailberichten in CA SDM finden Sie unter "Erzeugen von Berichten" in der *Online-Hilfe*.

Weitere Informationen:

[Verwalten von CAB-Gruppen](#) (siehe Seite 866)

[Zuweisen von CAB-Gruppen](#) (siehe Seite 868)

[CAB-Genehmigungen](#) (siehe Seite 868)

[Ändern der CAB-Konsoleneigenschaften](#) (siehe Seite 869)

[Change Management-Berichterstattung](#) (siehe Seite 870)

Verwalten von CAB-Gruppen

Sie können CAB-Gruppen mit Mitgliedern erstellen und gemäß den zu berücksichtigenden Changes verwalten. Das CAB kann je nach Bedarf Mitglieder des Anwendungsteams, Entwicklungsmanager, Komponenten-Eigentümer, QA, Support sowie beliebige andere Parteien enthalten.

Hinweis: Bevor Sie eine CAB-Gruppe implementieren, konfigurieren Sie die geeigneten Kontakte für Ihre Geschäftsstruktur.

So erstellen Sie eine CAB-Gruppe:

1. Wählen Sie auf der Registerkarte "Administration" die Option "Gruppen".
Die Seite "Gruppe - Suche" wird angezeigt.
2. Klicken Sie auf "Neu erstellen".
Die Seite "Neue Gruppe erstellen" wird angezeigt.

3. Füllen Sie die Felder nach Bedarf aus.
4. Klicken Sie auf "Speichern".

Die CAB-Gruppe wird auf der Seite "Gruppe - Liste" angezeigt.

So weisen Sie der CAB-Gruppe Mitglieder zu:

1. Wählen Sie auf der Seite "Gruppe - Detail" die Registerkarte "Mitglieder".
2. Klicken Sie auf "Mitglieder aktualisieren".

Die Seite "Kontakte - Suche" wird angezeigt.

3. Geben Sie die Suchkriterien ein, um die gewünschten Kontakte anzuzeigen, und klicken Sie auf "Suchen".

Die Seite "Mitglieder aktualisieren" wird angezeigt und führt die Kontakte auf, die den Suchkriterien entsprechen.

4. Wählen Sie aus der Liste auf der linken Seite die Kontakte aus, die Sie dieser Gruppe zuweisen möchten. Halten Sie die STRG-Taste gedrückt, während Sie mit der linken Maustaste klicken, um mehrere Elemente auszuwählen.

5. Wenn Sie alle gewünschten Kontakte ausgewählt haben, klicken Sie auf die Auswahl Schaltfläche (≥>).

Die ausgewählten Kontakte werden zur Mitgliederliste auf der rechten Seite verschoben.

6. Klicken Sie auf "OK".

Die Seite "Gruppe - Detail" wird angezeigt. Die ausgewählten Kontakte sind in der Registerkarte "Mitglieder" aufgeführt.

So fügen Sie die CAB-Gruppe einer Change-Kategorie hinzu:

Hinweis: Stellen Sie sicher, dass die Option "Category_Defaults" installiert ist, damit das Feld "CAB" auf Changes standardmäßig die CAB-Gruppe anzeigt.

1. Wählen Sie auf der Registerkarte "Administration" die Option "CA SDM" > "Changes" > "Kategorien".

Die Seite "Change-Kategorien - Liste" wird angezeigt.

2. Wählen Sie eine Kategorie aus der Liste.

Die Seite "Change-Kategorie aktualisieren" wird angezeigt.

3. Wählen Sie die passende CAB-Gruppe aus dem Feld "CAB".
4. Füllen Sie die anderen Felder nach Bedarf aus.

5. Klicken Sie auf "Speichern".

Auf der Seite "Change-Kategorie - Detail" wird eine Meldung angezeigt, dass der Speichervorgang erfolgreich war.

6. Klicken Sie auf "Fenster schließen".

Die CAB-Gruppe ist mit der Change-Kategorie und dem Change verknüpft.

Weitere Informationen:

[Area Defaults](#) (siehe Seite 517)

[Change- und Issue-Kategorien](#) (siehe Seite 430)

Zuweisen von CAB-Gruppen

Sie können einer Überprüfung eine CAB-Gruppe zuweisen, um einen Change zu überprüfen, bevor dieser implementiert wird.

So weisen Sie einem Change eine CAB-Gruppe zu:

1. Wählen Sie den gewünschten Change aus der Change-Liste aus.

Das Fenster "Change - Detail" wird angezeigt.

2. Klicken Sie auf "Bearbeiten".

3. Wählen Sie im Bereich "Details" "CAB" aus.

Die Seite "Liste der Gruppen" wird angezeigt.

4. Wählen Sie eine CAB-Gruppe aus.

5. Klicken Sie auf "Speichern" und "Fenster schließen".

Die CAB-Gruppe ist nun dem Change zugewiesen.

CAB-Genehmigungen

Der Change Advisory Board (CAB) muss einen Change genehmigen, bevor der Change implementiert werden kann, wenn das CAB-Feld "Genehmigung" auf "JA" gesetzt ist. Wenn die Change Manager während des Genehmigungsprozesses auf "Genehmigen" oder "Ablehnen" klicken, wird der Change-Status entsprechend zu "Genehmigt" oder "Abgelehnt" geändert.

Hinweis: Wenn Sie verschiedene Statuswerte verwenden möchten, können Sie mit Web Screen Painter den Code der Schaltfläche "Genehmigen" oder "Ablehnen" aktualisieren.

Weitere Informationen:

[Ändern der CAB-Konsoleneigenschaften](#) (siehe Seite 869)

Ändern der CAB-Konsoleneigenschaften

Mit Web Screen Painter können Sie die CAB-Konsoleneigenschaften ändern, die auf Webformularen in der CAB-Konsole angezeigt werden. Sie können beispielsweise folgende Vorgänge ausführen:

- Die Schaltflächen "Genehmigen" und "Ablehnen" umbenennen. Diese Schaltflächen sind Eigenschaften auf den Webformularen "orderwf_approval_console.html" (CA Workflow-Aufgaben) und "order_approval_console.html" (Changes).
- Die Statuswerte der Schaltflächen "Genehmigen" und "Ablehnen" an Ihre Anforderungen anpassen, indem Sie die Werte "REJ" oder "APR" ändern.
 - Die Schaltfläche "Aufgabe ablehnen" ruft die Funktion "approve_reject('REJ')" auf.
 - Die Schaltfläche "Approve Task" ruft die Funktion "approve_reject('APR')" auf.

Wichtig! Sie können nur einen aktiven Übergang mit einer Schaltfläche verknüpfen. Desaktivieren Sie keinen vordefinierten Statusübergang, der mit einer Schaltfläche verknüpft ist, da sonst der vordefinierte Statusübergang nicht mehr funktioniert.

So ändern Sie die CAB-Konsoleneigenschaften:

1. Öffnen Sie im Web Screen Painter das CAB-Konsolenformular, das Sie ändern möchten.

Web Screen Painter wird geöffnet, und das Formular wird angezeigt.

2. Klicken Sie mit der rechten Maustaste auf der Registerkarte "Design" auf die Schaltfläche, die Sie ändern möchten, und wählen Sie "Eigenschaften" aus.

Die Seite "Eigenschaften - *Steuerung*" wird angezeigt.

3. Ändern Sie die Eigenschaften nach Bedarf, indem Sie neue Werte eingeben.

Die Änderungen werden wirksam, sobald Sie außerhalb des Felds klicken und die Seite "Eigenschaften" schließen.

Web Screen Painter zeigt eine kurze Zusammenfassung der Bedeutung einer Eigenschaft in einem Hinweis an, der unten im Dialogfeld "Eigenschaften" angezeigt wird, wenn Sie eine Eigenschaft auswählen.

Hinweis: Weitere Informationen zum Web Screen Painter finden Sie im *Implementierungshandbuch*.

Beispiel: Anpassen der CAB-Konsole für Change-Workflow-Aufgaben

In diesem Beispiel wird gezeigt, wie Sie den Aufgabenstatus mit Web Screen Painter an Ihren Bedarf anpassen.

1. Öffnen Sie in Web Screen Painter das Webformular "orderwf_approval_console.html".

Web Screen Painter wird geöffnet, und das Formular wird angezeigt

2. Klicken Sie mit der rechten Maustaste auf der Registerkarte "Design" auf die Schaltfläche "Aufgabe ablehnen", und wählen Sie "Eigenschaften" aus.

Die Seite "Eigenschaften - Schaltfläche" wird geöffnet.

3. Suchen Sie die Funktion "approve_reject('REJ')".

"REJ" ist der Statuscode für den Aufgabenstatus "Ablehnen".

4. Geben Sie einen neuen Wert für "REJ" ein.

Die Änderungen werden wirksam, sobald Sie außerhalb des Felds klicken und die Seite "Eigenschaften" schließen.

Web Screen Painter zeigt eine kurze Zusammenfassung der Bedeutung einer Eigenschaft in einem Hinweis an, der unten im Dialogfeld "Eigenschaften" angezeigt wird, wenn Sie eine Eigenschaft auswählen.

Change Management-Berichterstattung

Ein Change Manager mit geeigneten Privilegien kann mit Hilfe von BusinessObjects Infoview die folgenden Aufgaben ausführen:

- Erstellen von Berichten über das Change-Volumen nach Betriebssystem, Change-Kategorie, Gruppe, Implementierer, Risiko, Status, Implementierungsdatum, betroffene Configuration Items (CIs) und Changes, die von Incident oder Problem-Tickets stammen
- Erstellen von Berichten über erfolgreich implementierte Änderungen gruppiert nach Change-Kategorie, Dringlichkeit, Priorität, Auswirkung, % erfolgreicher Änderungen vs. Gesamtzahl für den spezifizierten Zeitraum, und nach der Gruppe des Change-Anforderers.
- Erstellen von Berichten über fehlgeschlagene Änderungen gruppiert nach Kategorie, Dringlichkeit, Priorität, Auswirkung, Grund für das Rückgängigmachen, % fehlgeschlagener Änderungen vs. Gesamtzahl für den spezifizierten Zeitraum, und nach der Gruppe des Change-Anforderers.
- Erstellen von Berichten über die Gesamtanzahl der Change Requests gruppiert nach Change-Kategorie, Change-Koordinator, Risikoebene, Priorität und betroffenen CIs für einen bestimmten Zeitraum.

Im linken Bereich des Fensters "InfoView" können Sie zu den folgenden vordefinierten Berichten navigieren, um den Bericht anzuzeigen, zu planen, zu bearbeiten oder auszuführen, oder um den Verlauf und die Eigenschaften für einen Bericht anzuzeigen.

Hinweis: Weitere Informationen über die Verwendung von BusinessObjects Infoview finden Sie unter "CA Business Intelligence" in der *Online-Hilfe*.

Risikobewertung

Risikobewertungen lassen Sie die Risiken von Changes, die zu Change-Kategorien gehören, bestimmen, bewerten und beziffern, bevor Sie ein System oder einen Service in Ihrer Umgebung ändern. Sie erstellen Risikoumfragen, um Risiken zu evaluieren, und verknüpfen die Befragungen mit Change-Kategorien. Wenn ein Anwender einen Change erstellt und eine Change-Kategorie angibt, wird die Befragung, die mit dieser Kategorie verknüpft ist, bereitgestellt und kann abgeschlossen und abgesendet werden.

Die Risikoumfrage führt eine Reihe von einfachen und Multiple-Choice-Fragen auf. Jede Antwort besitzt einen Schweregradwert. Beim Erstellen eines Change, wählt der Anwender die geeigneten Antworten aus und sendet die Befragung ab. Die evaluierte Risikoebene basiert auf den Schweregraden der Antworten, die vom Anwender ausgewählt werden.

Weitere Informationen:

[Bereitstellen eines Risikoumfrage-Beispiels](#) (siehe Seite 873)

[Anzeigen von Standardrisikoumfragen](#) (siehe Seite 872)

So implementieren Sie die Risikoumfrage:

Implementieren Sie die Risikoumfrage folgendermaßen:

1. Richten Sie Risikoebenen für Ihre Organisation ein.
2. Erstellen Sie eine Risikoumfrage, oder wählen Sie eine Risikoumfrage aus der Standardliste aus.
3. Erstellen Sie Fragen und Antworten für die Risikoumfrage oder ändern bestehende Fragen und Antworten.
4. Ändern Sie Risikobereiche für die Risikoumfrage.
5. Verknüpfen Sie die Risikoumfrage mit einer Change-Kategorie.
6. Nachdem Sie eine Risikoumfrage mit einer Change-Kategorie verknüpft haben, wird die Schaltfläche "Risikoumfrage" für den Anfragenden angezeigt, wenn dieser einen Change mit dieser Change-Kategorie speichert.
7. Zeigen Sie das Risiko gemäß den Ergebnissen der Risikoumfrage an.
8. (Optional) Setzen Sie das bewertete Risiko über das Menü "Aktivitäten" außer Kraft.

Hinweis: Ausführliche Informationen zum Erstellen und Ändern von Risikoumfragen finden Sie in der *Online-Hilfe*.

Anzeigen von Standardrisikoumfragen

CA SDM enthält Standardrisikoumfragen, die Sie mit Change-Kategorien verknüpfen können.

So zeigen Sie die Standardrisikoumfragen an:

1. Navigieren Sie zu "Service Desk" > "Changes" > "Risikoumfrage".
2. Wählen Sie "Allgemein" aus der Spalte "Name der Risikoumfrage" aus.
Die Seite "Allgemeine Risikoumfrage - Details" wird angezeigt.
3. Klicken Sie auf "Befragung anzeigen".
Die Risikoumfrage wird angezeigt. Sie enthält Fragen, Antworten und Gewichtungen für jede Antwort. Diese Umfrage gilt für allgemeine Changes in Ihrer Organisation.
4. Schließen Sie die Umfrage.
5. Die Seite "Allgemeine Risikoumfrage - Details" wird angezeigt; schließen Sie sie.

Bereitstellen eines Risikoumfrage-Beispiels

In diesem Beispiel wird gezeigt, wie Sie mit Hilfe einer Standard-Change-Kategorie eine Standardrisikoumfrage auf Ihrem System bereitstellen.

1. Navigieren Sie zu "Service Desk", "Changes" und "Kategorien".
Die Seite "Change-Kategorien - Liste" wird angezeigt.
2. Wählen Sie "Add.IT.Other" aus der Spalte "Symbol" aus.
Die Seite "Add.IT.Other - Kategorie - Detail" wird angezeigt.
3. Klicken Sie auf "Bearbeiten".
Die Seite "Add.IT.Other - Change-Kategorie aktualisieren" wird angezeigt.
4. Klicken Sie auf "Risikoumfrage".
Das Fenster "Vorlagen für Risikoumfragen - Suche" wird angezeigt.
5. Suchen Sie nach der Risikoumfrage. Suchen Sie in diesem Beispiel nach "Allgemein", und wählen Sie die Risikoumfrage aus, um sie dem Detailformular hinzuzufügen.
Im Feld "Risikoumfrage" wird "Allgemein" angezeigt.
6. Speichern und schließen Sie das Fenster.

Wenn ein Benutzer einen Change mit der Kategorie "Add.IT.Other" erstellt, wird beim Speichern des Changes die Schaltfläche "Risikoumfrage" angezeigt.

Zugreifen auf eine Risikoumfrage direkt über eine URL

Sie können eine dynamische URL bereitstellen, um einem Anwender zu erlauben, auf eine Change-Risikoumfrage direkt über eine URL innerhalb einer Aufgabe in CA Workflow zuzugreifen. Sie können diese dynamische URL mit dem Parameter *KEEP.UsingURL=1* versehen, um zu zeigen, dass auf die Risikoumfrage direkt über eine URL zugegriffen wird.

So erstellen Sie die dynamische URL innerhalb von CA Workflow:

1. Öffnen Sie Ihre CA Workflow-Prozessdefinition und fügen Sie Aktivitätsknoten hinzu, damit ein Anwender die Risikoumfrage abschließt.
2. Fügen Sie innerhalb des Aktivitätsknotens eine dynamische URL mit der entsprechenden Syntax hinzu. Überprüfen Sie, ob der Parameter *KEEP.UsingURL=1* angehängt ist, so wie im folgenden Beispiel:

```
http://<hostname>:CA Portal/CAisd/pdmweb.exe?CNT_ID=<ID of contact>+CRID=<ID of Change Order>+OP=DO_RISK_SURVEY+KEEP.UsingURL=1
```

hostname

Gibt den Hostnamen des Anwendungsservers oder eine URL des Lastenausgleichs an, die zu einer Gruppe von Anwendungsservern führen kann.

port

Gibt den Port an, an dem CA SDM installiert ist.

ID des Kontaktes

Gibt die interne ID des Kontaktes an, der die Risikoumfrage ausführt.

ID des Changes

Gibt die interne ID des mit der Risikoumfrage verbundenden Changes an.

Das folgende Beispiel zeigt eine Beispiel-URL:

```
http://hostname:8080/CAisd/pdmweb.exe?CNT_ID=21A7CC606A3011DEA39AA8010000A800+CRID=400009+OP=DO_RISK_SURVEY+KEEP.UsingURL=1
```

Wichtig! Wenn Sie den Parameter *KEEP.UsingURL=1* nicht der dynamischen URL hinzufügen, erhält der Anwender nach dem Senden der Risikoumfrage eine Fehlermeldung und die Risikoebene wird nicht kalkuliert.

3. Speichern Sie die CA Workflow-Prozessdefinition.
4. Erstellen Sie eine Change-Kategorie und verbinden Sie eine Risikoumfrage und die CA Workflow-Prozessdefinition mit der Change-Kategorie.
Speichern der Änderungen.
5. Öffnen Sie einen Change mit dieser Change-Kategorie und speichern Sie ihn, um den CA Workflow-Prozess zu instanzieren.

6. Als ein Teil des CA Workflow-Prozesses wird ein Anwender einer Aufgabe zugewiesen, um die Risikoumfrage abzuschließen. Der Anwender klickt auf die URL, wie bereits beschrieben.
7. Der Anwender loggt sich über die URL in CA SDM ein und wird direkt zur Risikoumfrage für den Change geleitet.
8. Der Anwender sendet die Umfrage, und eine Meldung zeigt an, ob der Vorgang erfolgreich war oder nicht.

Wenn das Absenden erfolgreich war, wird die Risikoebene kalkuliert und im Change aktualisiert.

Auswirkungs-Explorer

Auswirkungs-Explorer ist ein erweitertes Tool zum Verwalten und Steuern von Changes in einer Organisation. Mit Auswirkungs-Explorer kann der Change Manager an einen Change angehängte CIs untersuchen und direkt mit angehängten CIs oder untergeordneten CIs arbeiten.

Auswirkungs-Explorer bietet die folgenden Vorteile:

- Anzeige aller CIs, die an einen Change angehängt wurden
- Anzeige aller Unterordnungs-/Überordnungs- und Peer-to-Peer-Beziehungen für angehängtes CIs
- Die Möglichkeit, beliebige verwandte CIs an den Change anzuhängen
- Anzeige einer Liste der nachfolgenden Elemente mit verwandten CIs für ein beliebiges angehängtes CI
- Bietet die Möglichkeit, CMDB-Visualizer für einen CI zu starten.

Weitere Informationen:

[Starten von Auswirkungs-Explorer](#) (siehe Seite 876)

[Untersuchen von angehängten CIs](#) (siehe Seite 876)

[Anzeigen von CIs in Auswirkungs-Explorer](#) (siehe Seite 877)

[Hinzufügen von verwandten CIs zu Changes](#) (siehe Seite 877)

[Anzeigen der Liste der nachfolgenden Elemente des CI](#) (siehe Seite 878)

[Starten von CMDB Visualizer im Auswirkungs-Explorer](#) (siehe Seite 878)

[Konfigurieren von Auswirkungs-Explorer](#) (siehe Seite 879)

Starten von Auswirkungs-Explorer

Sie können Auswirkungs-Explorer über die Registerkarte "Config. Items" jedes Changes öffnen.

So öffnen Sie Auswirkungs-Explorer:

1. Öffnen Sie eine Seite "Change-Detail".
2. Wählen Sie die Registerkarte "Config. Items" aus.
3. Klicken Sie auf "Auswirkungs-Explorer".

Die Seite "Auswirkungs-Explorer" wird angezeigt.

Hinweis: Wenn Sie die Seite "Change-Detail" schließen, wird auch die Seite "Auswirkungs-Explorer" geschlossen.

Hinweis: Wenn Auswirkungs-Explorer von mehreren Changes gestartet wird, werden mehrere Auswirkungs-Explorer-Seiten angezeigt.

Untersuchen von angehängten CIs

Die Auswirkungs-Explorer-Baumstruktur enthält einen Knoten für jeden CI, der an einen Change angehängt ist. Ein Plussymbol (+) zeigt an, dass ein CI mindestens über einen untergeordneten CI verfügt.

Hinweis: Wenn mehr als 100 CIs an einem Change angehängt sind, werden nur die ersten 100 angezeigt.

Um die Beziehungen für einen angehängten CI anzuzeigen, klicken Sie auf das Plussymbol (+) für den CI. Die verwandten CIs werden in der Baumstruktur angezeigt. Neben den verwandten CI-Namen werden in der Baumstruktur auch die Beziehungstypen in Klammern angezeigt.

Hinweis: Wenn der Change über mehr als 100 angehängte CIs verfügt, werden nur die ersten 100 angezeigt. Um die nächsten 100 CIs anzuzeigen, klicken Sie auf "Mehr...".

Anzeigen von CIs in Auswirkungs-Explorer

Die Auswirkungs-Explorer-Baumstruktur zeigt einen Knoten für jeden CI an, der mit einem Change verknüpft ist. Ein Plussymbol (+) zeigt an, dass ein CI mindestens über einen untergeordneten CI verfügt.

So zeigen Sie einen CI an:

1. Klicken Sie auf einen CI-Knoten im linken Bereich.

Die Seite "CI - Detail" wird im rechten Fensterausschnitt angezeigt.

Hinweis: Sie können die Seite "CI - Detail" auch im rechten Fensterausschnitt anzeigen, indem Sie mit der rechten Maustaste auf das CI klicken und im Kontextmenü "Ansicht" auswählen.

2. Klicken Sie auf den Change-Knoten oben im linken Bereich.

Das Fenster "Change - Detail" wird angezeigt.

Hinweis: Wenn der Change über mehr als 100 angehängte CIs verfügt, werden nur die ersten 100 angezeigt. Um die nächsten 100 CIs anzuzeigen, klicken Sie auf "Mehr..."

Hinzufügen von verwandten CIs zu Changes

Beim Untersuchen von CI-Beziehungen möchten Sie möglicherweise einen verwandten CI an einen Change anhängen.

So fügen Sie einem Change einen verwandten CI hinzu:

1. Klicken Sie auf die Registerkarte "Config. Items" eines Changes.

Die Seite "Configuration Items - Liste" wird angezeigt.

2. Klicken Sie auf "Auswirkungs-Explorer".

In der Auswirkungs-Explorer-Baumstruktur werden angehängte CIs angezeigt.

3. Klicken Sie auf das Plussymbol (+) für einen angehängten CI-Knoten.

Die mit diesem Knoten verwandten CIs werden angezeigt.

4. Klicken Sie mit der rechten Maustaste auf einen verwandten CI, und wählen Sie aus dem Kontextmenü "Hinzufügen" aus.

Der neu angehängte CI wird auf der Registerkarte "Config. Items" eines Changes angezeigt.

Anzeigen der Liste der nachfolgenden Elemente des CI

Sie können für jeden CI Verbindungen verwandter CIs anzeigen (benannte *Descendants*). Zusätzlich zu den grundlegenden Informationen zu jedem CI werden in der Liste der nachfolgenden Elemente des CI Verwandtschaftsebenen angezeigt, wobei der ursprüngliche CI der ersten Ebene entspricht. Untergeordnete CIs entsprechen der zweiten Ebene, CIs, die diesen untergeordnet sind, der dritten Ebene und so weiter. Wenn ein CI mehr als einmal in den verfolgten Beziehungen auftaucht, wird nur dessen nächste Beziehungsebene angezeigt.

Beispiel: Mehrere Descendant-Pfade für einen CI

Da mehrere Beziehungen bestehen, findet eine Descendant-Suche denselben verwandten CI auf der zweiten und der vierten Ebene. Der Descendant-CI wird nur auf der zweiten Ebene angezeigt.

So listen Sie nachfolgende Elemente für einen CI auf:

1. Wählen Sie auf der Seite "Change-Detail" die Registerkarte "Config. Items" aus.
2. Klicken Sie auf "Auswirkungs-Explorer", um angehängte CIs anzuzeigen.
3. Erweitern Sie bei Bedarf einen CI-Knoten.
4. Klicken Sie mit der rechten Maustaste auf einen CI, und wählen Sie "Nachfolgende Elemente auflisten" aus.

Die "Liste der nachfolgenden Elemente des CI" wird angezeigt.

Starten von CMDB Visualizer im Auswirkungs-Explorer

Mit Hilfe von Auswirkungs-Explorer können Sie CMDB Visualizer von einem angehängten oder verwandten CI aus starten.

So starten Sie CMDB Visualizer in Auswirkungs-Explorer:

1. Klicken Sie auf einer Seite "Change-Detail" auf "Auswirkungs-Explorer".
Die Seite "Auswirkungs-Explorer" wird angezeigt.
2. Klicken Sie mit der rechten Maustaste auf einen CI, und wählen Sie im Kontextmenü "Visualizer starten" aus.

CMDB Visualizer wird für das CI gestartet.

Konfigurieren von Auswirkungs-Explorer

Administratoren können Auswirkungs-Explorer folgendermaßen konfigurieren:

- Festlegen der Anzahl der untergeordneten CIs, die für einen angehängten CI angezeigt werden
- Festlegen der Anzahl von Beziehungsebenen, die in der Liste der nachfolgenden Elemente des CI angezeigt werden
- Unterdrücken der Anzeige von untergeordneten CIs

Die Anzahl der untergeordneten CIs, die angezeigt wird, lässt sich konfigurieren, indem die Einstellung "NX_IMPACT_EXPLORER_MAX_CHILD_NODES" der Konfigurationsdatei "NX.env" hinzugefügt wird. Der Standardwert ist 100.

Beispiel: Konfigurieren der Anzeige der untergeordneten CIs

Mit der folgenden Einstellung, zeigt Auswirkungs-Explorer nur zehn untergeordnete CIs auf einmal an:

```
@NX_IMPACT_EXPLORER_MAX_CHILD_NODES=10
```

Standardmäßig werden in der Liste der nachfolgenden Elemente des CI neun (9) Ebenen angezeigt. Die Anzahl der angezeigten Ebenen lässt sich konfigurieren, indem die Einstellung "NX_IMPACT_EXPLORER_MAX_LEVELS" der Konfigurationsdatei "NX.env" hinzugefügt wird.

Beispiel: Konfigurieren der Anzahl der Descendant-Ebenen

Mit der folgenden Einstellung zeigt die Liste der nachfolgenden Elemente des CI den ursprünglichen CI und nur die (verwandtschaftlich) angrenzenden untergeordneten CIs an:

```
@NX_IMPACT_EXPLORER_MAX_LEVELS=2
```

Verwenden Sie die folgende Optionsmanager-Option, um die Anzeige einer bestimmten Art von untergeordneten CIs zu unterdrücken:

```
IMPACT_EXPLORER_EXCLUDE_HIER=boolean
```

Wenn die Option "IMPACT_EXPLORER_EXCLUDE_HIER" installiert und auf "Ja" gesetzt ist, werden die untergeordneten CIs, die über die Registerkarte "CMDB-Beziehungen" einer Seite "CI - Detail" verknüpft sind, in der Auswirkungs-Explorer-Baumstruktur oder der Liste der nachfolgenden Elemente des CI nicht angezeigt.

Hinweis: Untergeordnete CIs, die über CA CMDB verknüpft sind, werden weiterhin angezeigt.

Kapitel 19: Verwalten von Berichten

Dieses Kapitel enthält folgende Themen:

[CA Business Intelligence-Berichte](#) (siehe Seite 883)

[Berichterstellungsszenarios](#) (siehe Seite 883)

[Berichtskomponenten](#) (siehe Seite 884)

[Berichtsdatenflussdiagramm](#) (siehe Seite 887)

[Anzeigen von webbasierten Berichten in InfoView](#) (siehe Seite 888)

[Sicherheit und Autorisierung](#) (siehe Seite 889)

[Verweisen eines vorhandenen CA Business Intelligence-Servers auf einen](#)

[CA SDM-Server](#) (siehe Seite 895)

[Einrichten der Datenaufteilungssicherheit für die Berichterstellung](#) (siehe Seite 897)

[Replizierte Datenbank für Offline-Berichterstellung](#) (siehe Seite 899)

[Rollenbasierte Berichte](#) (siehe Seite 900)

[Webbasierte Berichte](#) (siehe Seite 909)

[KPIs \(Kritische Prozess-Indikatoren\)](#) (siehe Seite 912)

[Ad-hoc-Berichte](#) (siehe Seite 924)

[Ad-hoc-Beispielberichte](#) (siehe Seite 926)

[Dashboard-Berichte](#) (siehe Seite 932)

[Schreiben von CA Business Intelligence-Berichten](#) (siehe Seite 933)

Kapitel 20: CA Business Intelligence-Berichte

CA Business Intelligence ist eine webbasierte Komponente, die die Business Objects-Technologie mit CA SDM und verschiedenen verbreiteten Datenquellen vereint, z. B. SQL Server, Oracle und Open Database Connectivity (ODBC).

CA Business Intelligence verwendet BusinessObjects Enterprise als Standardberichterstellungssystem. Vordefinierte Berichte werden für CA SDM, Knowledge Management und Support-Automatisierung bereitgestellt.

Mit CA Business Intelligence-Berichterstellung können Anwender folgende Aktionen durchführen:

- Anpassen vorhandener Berichte
- Anzeigen der Daten, die sich hinter den Diagrammen und zusammengefassten Gruppen verbergen, per Drilldown-Funktion in den Business Objects-Berichtsdaten
- Exportieren von Instanzen der Berichte in verschiedene Ausgabeformate
- Erstellen von Ad-hoc-Berichten
- Veröffentlichen neuer Berichte und Verteilen dieser Berichte an befugte Anwender
- Planen der Ausführung von Berichten zu bestimmten Zeiten
- Verwenden von Dashboard-Berichten zur Überwachung von täglichen Vorgängen für alle CA SDM-Ticket-Typen.

Hinweis: Der Zugriff auf die Berichterstellung ist durch die CA SDM-Datenpartitionssicherheit eingeschränkt.

Berichterstellungsszenarios

Mit BusinessObjects Enterprise integriertes CA Business Intelligence unterstützt die folgenden Szenarien für die Berichterstellung:

- **Rollenbasierte Berichterstellung** — Über die Registerkarte "Berichte" von CA SDM können autorisierte Anwender für ihre Rolle definierte Berichte anzeigen und dann auf die Schaltfläche "InfoView" klicken, um ihre persönlichen Berichte in BusinessObjects InfoView zu verwalten. CA SDM verwendet die InfoView-Schnittstelle zum Sammeln, Organisieren und Darstellen von Informationen in Berichtsformaten. In InfoView sind vordefinierte Berichte in öffentlichen Ordnern gruppiert.

- **Webbasierte Berichterstellung:** Webbasierte Berichte sind vordefinierte Berichte in CA SDM, Knowledge Management, CMDB und Support-Automatisierung. Sie werden entweder mit Web Intelligence oder Crystal Reports entwickelt. Der Zugriff auf die Berichte erfolgt über InfoView. Die Berichte können als Modelle zum Definieren standortspezifischer Berichte verwendet werden.
- **Ad-hoc-Berichterstellung** — Ad-hoc-Berichte werden mit Hilfe einer Plugin-basierten Web Intelligence-Schnittstelle in InfoView erstellt und verwaltet. Sie können Berichte in einem persönlichen Arbeitsbereich ("Eigene Ordner") speichern und verwalten. Ad-hoc-Berichterstellung ist gedacht für Anwender, die problemlos einfache Berichte erstellen möchten, ohne Abfragen zu schreiben.
- **Dashboard-Berichterstellung:** Über Dashboard-Berichte können Sie laufend den Status für CA SDM-Ticket-Typen (Request/Incident/Problem, Change oder Issue) in InfoView überwachen. Jeder Bericht enthält Analysedaten über Mitarbeiter, die bei der Arbeit mit aktiven Tickets beste Leistungen erbringen. So können Sie den Fortschritt überwachen. Sie können mit einzelnen vordefinierten Dashboard-Berichten arbeiten oder anhand von unternehmensweiten Dashboards alle täglichen Vorgänge von CA SDM in einer einzigen Ansicht anzeigen.

Berichtskomponenten

BusinessObjects Enterprise und die zugeordneten Tools sind, in Verbindung mit Crystal-Reports XI, der Backbone der CA BI-Architektur.

Obwohl Crystal-Reports der primäre Bestandteil von CA Business Intelligence ist, wird das Berichterstellungs- und Wartungstool Crystal-Reports XI nicht als Teil von CA Business Intelligence mitgeliefert. Crystal-Reports XI ist ein separat lizenziertes Produkt, das von BusinessObjects Enterprise gekauft und zusammen mit CA Business Intelligence verwendet werden kann.

Hinweis: Vordefinierte Berichte für Microsoft Access werden nicht mehr für CA SDM entwickelt oder bereitgestellt.

Sie können die folgenden Komponenten verwenden, um die CA Business Intelligence-Berichtsumgebung zu verwalten, zu überwachen und zu konfigurieren:

- **CA SDM Datenbank/Domsrvr/ODBC-Treiber:** Die Berichtsdaten werden in einer SQL Server- oder Oracle-CA SDM-Datenbank gespeichert. BusinessObjects-Berichtsanwendungen (Crystal Reports und Web Intelligence) greifen auf die Datenbank über einen ODBC-Treiber zu, der direkt mit der Objekt-Engine (domsrvr) von CA SDM verbunden ist. Alle CA SDM-Sicherheitsfunktionen, einschließlich Datenpartition und Mandantenbeschränkungen werden automatisch auf Berichte, aber nicht auf Ihre Berichtsumgebung angewandt. Sie können Ihre Berichtsumgebung so einrichten, dass sie mit vorhandenen Datenpartitionen in CA SDM arbeitet.

Hinweis: Weitere Informationen zur Absicherung von Datenpartitionen für Ihre Berichtsumgebung finden Sie unter [Absichern von Datenpartitionen bei der Berichterstellung](#) (siehe Seite 889).

- **Central Management Server (CMS):** Die zentrale Repository zur Speicherung aller Objekte, die in den einzelnen Berichterstellungsprozessen verwendet werden.
- **Central Management Console:** Eine administrative Komponente für den Zugriff auf alle Administratorfunktionen von BusinessObjects. Mithilfe der CMC können Sie Berichte bereitstellen und Anwenderzugriff sowie Ordnerberechtigungen für InfoView zuweisen. Anwender-Genehmigungen, Rollen und Authentifizierungsoptionen müssen mit der CMC eingerichtet werden.

Hinweis: Bevor Sie CA Business Intelligence verwenden, müssen Sie Anwenderberechtigungen, Rollen und Authentifizierungsoptionen einrichten. Weitere Informationen über Sicherheitseinstellungen finden Sie unter [Sicherheit und Authentifizierung](#) (siehe Seite 889).

- **BusinessObjects-Universum:** Bezeichnet die Klassen (Tabellen] und Objekte (Spalten), die in Berichten verwendet werden. CA SDM Universum wird während der Installation ebenfalls installiert und konfiguriert. Sobald die Installation abgeschlossen ist, wird die Universums-Verbindung verschiedenen Gruppen und Anwendern in CA SDM zugewiesen.
- **Designer:** Dies ist eine Komponente in BusinessObjects, mit der Sie das CA SDM-Universum ändern können, welches eine Metaebene zwischen CA SDM-Schema-Tools und BusinessObjects-Berichterstellungs-Tools bildet. Mit dem Import-/Exportassistenten können Sie Objekte in CMS einfügen oder daraus extrahieren.
- **Vordefinierte Standardberichte** - Vordefinierte Berichte sind webbasierte CA SDM- und Knowledge Management-Berichte, die entweder mit Web Intelligence oder mit Crystal Reports entwickelt wurden. Die Berichte können als Modelle zum Definieren standortspezifischer Berichte verwendet werden.
- **InfoView** - BusinessObjects InfoView ist eine Web-Schnittstelle, die es autorisierten CA SDM-Anwendern ermöglicht, durch Anzeige, Ausführung und Planung von Berichtstypen wie Web Intelligence und Crystal Reports (um nur zwei zu nennen) mit webbasierten vordefinierten Berichten zu interagieren. Berichte werden im öffentlichen Abschnitt von InfoView in Ordnern gespeichert.

- **Ad-Hoc-Berichte:** Mit Ad-hoc-Berichten können Sie Berichte über eine Plugin-basierte Web-Intelligence-Schnittstelle erstellen und verwalten. Dieses Tool dient Anwendern, die problemlos einfache Berichte erstellen möchten, ohne Abfragen zu schreiben.

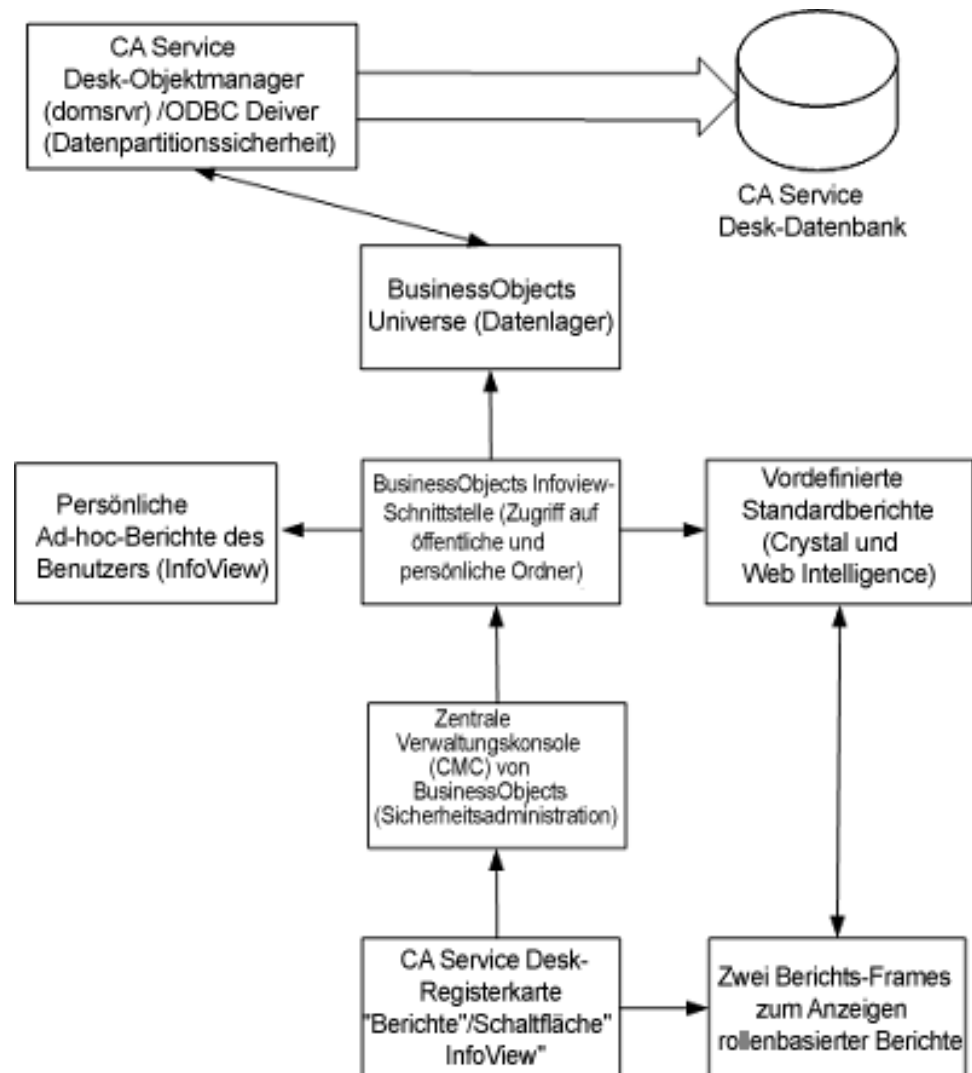
Hinweis: Beispiel für die Anwendung von Ad-hoc-Berichten finden Sie unter [Ad-Hoc-Berichte](#) (siehe Seite 924).

- **Dashboard-Berichte:** Über Dashboard-Berichte können Sie laufend den Status für CA SDM-Ticket-Typen (Request/Incident/Problem, Change oder Issue) in BusinessObjects InfoView überwachen. Jeder Bericht enthält Analysedaten über Mitarbeiter, die bei der Arbeit mit aktiven Tickets beste Leistungen erbringen. So können Sie den Fortschritt überwachen.
- **CA SDM-Registerkarte "Berichte":** Auf der Registerkarte "Berichte" können befugte Anwender ihre rollenbasierten Berichte in CA SDM anzeigen und dann auf dieser Registerkarte auf die Schaltfläche "InfoView" klicken, um ihre persönlichen Berichte in InfoView zu verwalten.

Hinweis: Weitere Informationen über das Verwalten von rollenbasierten Berichten und das Anzeigen von neuen Berichten auf der Registerkarte "Berichte" finden Sie unter [Webbasierte Berichte](#) (siehe Seite 909).

Berichtsdatenflussdiagramm

Das folgende Diagramm veranschaulicht für CA Business Intelligence in Integration mit BusinessObjects Enterprise den Datenfluss zwischen einzelnen Komponenten und deren Ausführung:



Anzeigen von webbasierten Berichte in InfoView

CA SDM verwendet die BusinessObjects InfoView-Schnittstelle zum Sammeln, Organisieren und Darstellen von Informationen in Berichtsformaten.

Wichtig! Sie *müssen* für alle Bericht die Datumsfelder aktualisieren, damit sie generiert werden können. Die restlichen Felder sind optional.

Gehen Sie wie folgt vor:

1. Klicken Sie auf der Registerkarte "Berichte" in CA SDM auf die Schaltfläche "InfoView".

Die Startseite von InfoView wird angezeigt.

2. Wählen Sie im Bereich "Kopfzeile" "Liste der Dokumente" aus.

Die Liste der Dokumente zeigt CA SDM-Berichte, administrative Tools, Beispiele usw. in öffentlichen Ordnern an. Wenn Sie einen Ordner auswählen, wird sein Inhalt im Detailbereich angezeigt. Die Ordner, auf die Sie über die Liste der Dokumente zugreifen können, hängen von den Rechten ab, die Ihnen von Ihrem Administrator erteilt wurden.

Um zum Beispiel die Berichte für CMDB anzuzeigen, navigieren Sie zu CA Service Desk/CMDB. Die Liste von Berichten wird im Detailbereich angezeigt.

3. Doppelklicken Sie auf einen Bericht.

Das Berichtsformular wird angezeigt. Das Formular enthält Felder für Werte, die von Ihnen eingegeben werden müssen, um den ausgewählten Bericht zu generieren.

4. Geben Sie die Information ein, die für die Generierung des ausgewählten Berichts relevant sind.

Beispiel: Wenn Sie den Bericht zu in einem bestimmten Zeitbereich hinzugefügten Cls öffnen, müssen Sie den Zeitbereich eingeben, für den Sie die hinzugefügten Cls, die Namen der CI-Mandanten-Namen usw. anzeigen möchten.

Wichtig! Wenn Sie die Oracle-Datenbank verwenden und Berichte zu allen Change-Auswirkungen, CI-Beziehungen und Ursachenanalyse generieren möchten, klicken Sie im CMDB-Ordner auf "Oracle" (diese Berichte funktionieren nur in Oracle), um auf die Berichte zuzugreifen. Wenn Sie diese Berichte im SQL Server-Ordner generieren, werden sie nicht erstellt, und es wird eine Fehlermeldung angezeigt. Wenn Sie die SQL-Datenbank verwenden und Berichte zu allen Change-Auswirkungen, CI-Beziehungen und Ursachenanalyse generieren möchten, klicken Sie im CMDB-Ordner auf "SQL Server" (diese Berichte funktionieren nur in SQL), um auf die Berichte zuzugreifen.

Hinweis: Es ist obligatorisch, alle Felder auszufüllen, um einen Bericht zu generieren.

5. Klicken Sie auf "OK".

Der Bericht wird angezeigt.

Hinweis: BusinessObjects InfoView umfasst ein Anwenderhandbuch mit Informationen zur Verwendung von BusinessObjects InfoView. Klicken Sie auf das Hilfesymbol in InfoView, um auf das Anwenderhandbuch zuzugreifen.

Sicherheit und Autorisierung

Die standardmäßige Sicherheitskonfiguration für BusinessObjects Enterprise wird über die CA Business Intelligence-Konfiguration ausgeführt. Die Konfiguration bestimmt die Sicherheitsrichtlinien der Ordner, Universes, Universumverbindungen und Tools. Hier finden Sie auch Methoden zum Hinzufügen von Anwendern und zum Zuordnen dieser Anwender zu Gruppen sowie zum Festlegen einiger Einstellungen.

Speziell bedeutet die Konfiguration der CA Business Intelligence-Berichterstellung folgendes:

- Einrichten der Sicherheit
- Bereitstellen von Berichten
- Bereitstellen von Universes
- Konfigurieren der Web Intelligence-Einstellungen

Zum Abschluss der Installation wird die Universumverbindung verschiedenen Gruppen und Anwendern in CA SDM zugewiesen.

Der Administrator kann sich bei der BusinessObjects-CMC anmelden und die Standardeinstellungen jederzeit ändern. Anwender bekommen Zugriff auf InfoView-Ordner und der Zugriff richtet sich danach, zu welcher CA Business Intelligence-Gruppe sie gehören.

Gruppen und Anwender

Die in der folgenden Tabelle aufgeführten Gruppen werden im Zuge der Konfiguration von CA Business Intelligence zum Central Management Server (CMS) hinzugefügt. Sie beziehen sich auf CA SDM-Rollen mit den gleichen Namen. Während der Konfigurationsphase von stand ein optionales Kontrollkästchen zur Verfügung, um anzugeben, ob zum CMS Beispielanwender hinzugefügt werden sollen. Wenn es ausgewählt wurde, schließt Ihre Standard-CMS-Konfiguration einen Beispielanwender für jede Gruppe ein. In CMC können Sie diese Beispielanwender als Modelle verwenden, wenn Sie Anwenderberechtigungen und Authentifizierungsoptionen für Ihre Berichtsumgebung festlegen.

Gruppenname	Anwendername
Change Manager	Change Manager-Anwender

Gruppenname	Anwendername
Kundenservicemanager	Kundenservicemanager-Anwender
Knowledge-Manager	Knowledge Manager-Anwender
Knowledge-Analyst	Knowledge-Analyst-Anwender
CA Service Desk-Manager	CA Service Desk-Manager-Anwender
Incident Manager	Incident Manager-Anwender
Problem Manager	Problem Manager-Anwender

CA SDM-Datenpartitionen in Infoview

Beachten Sie die folgenden Informationen zu den Beziehungen zwischen CA SDM Datenpartitionen und InfoView:

- Der Analyst stellt über die CA SDM-Registerkarte "Berichte" oder über InfoView (mit dem Zugriffstyp einer standardmäßigen Berichterstellungsrolle) eine Verbindung zu CA Business Intelligence her.
- Die CA SDM-Anmeldeinformationen *müssen* mit den InfoView-Anmeldeinformationen übereinstimmen. Der Administrator legt eine Authentifizierungsmethode wie secLDAP oder secEnterprise fest. CA SDM meldet sich bei CA Business Intelligence an, was sich wiederum über ODBC bei CA SDM anmeldet.
- Die CA Business Intelligence-Analystenmeldung wird der CA SDM-Anmeldung zugeordnet. CA Business Intelligence verwendet diese CA SDM-Anmeldung sowie die Berichterstellungsrolle, die dem Zugriffstyp der Anmeldung zugeordnet ist. Wenn der Analyst keine zugeordnete CA SDM-Anmeldung hat, verwendet CA Business Intelligence den Systemstandard. Der Systemstandard ist in den ODBC-Parametern im Universe Designer und in der Berichterstellungsrolle des Zugriffstyps definiert.
- Um zu vermeiden, dass ein Anwender einen Bericht anzeigt, kann der Administrator den Zugriff auf den Bericht oder auf den Ordner, der ihn enthält, deaktivieren.

Universum und Verbindungen mit einem Universum

Die Standardkonfiguration umfasst auch die Sicherheitsrichtlinien für den Zugriff auf das CA SDM-Universum und auf Verbindungen mit einem Universum. Um einen vollständigen Zugriff auf die Daten zu ermöglichen, haben alle Standardgruppen Vollzugriff.

Gruppenname	Zugriffsebene
Change Manager	Vollzugriff
Kundenservicemanager	Vollzugriff
Knowledge-Analyst	Vollzugriff
Knowledge-Manager	Vollzugriff
CA Service Desk-Manager	Vollzugriff
Incident Manager	Vollzugriff
Problem Manager	Vollzugriff

Berichtsordner

Die Standardkonfiguration umfasst eine Reihe von Ordnern mit vordefinierten Berichten für CA SDM und Knowledge Management. Jede CA SDM-Gruppe ist so konfiguriert, dass sie Zugriff auf eine Teilmenge dieser Ordner hat.

Ordnername	Gruppenname	Zugriffsebene
Aggregat	■ Change Manager	■ Ansicht
	■ Kundenservicemanager	■ Ansicht
	■ Knowledge-Manager	■ Kein Zugriff
	■ Knowledge-Analyst	■ Kein Zugriff
	■ CA Service Desk-Manager	■ Vollzugriff
	■ Incident Manager	■ Ansicht
	■ Problem Manager	■ Ansicht

Ordnername	Gruppenname	Zugriffsebene
Asset	■ Change Manager	■ Nach Bedarf ansehen
	■ Kundenservicemanager	■ Ansicht
	■ Knowledge-Manager	■ Kein Zugriff
	■ Knowledge-Analyst	■ Kein Zugriff
	■ CA Service Desk-Manager	■ Vollzugriff
	■ Incident Manager	■ Ansicht
	■ Problem Manager	■ Ansicht
Change (schließt alle Unterordner ein)	■ Change Manager	■ Vollzugriff
	■ Kundenservicemanager	■ Kein Zugriff
	■ Knowledge-Manager	■ Kein Zugriff
	■ Knowledge-Analyst	■ Kein Zugriff
	■ CA Service Desk-Manager	■ Ansicht
	■ Incident Manager	■ Ansicht
	■ Problem Manager	■ Ansicht
Issue (schließt alle Unterordner ein)	■ Change Manager	■ Kein Zugriff
	■ Kundenservicemanager	■ Vollzugriff
	■ Knowledge-Manager	■ Kein Zugriff
	■ Knowledge-Analyst	■ Kein Zugriff
	■ CA Service Desk-Manager	■ Kein Zugriff
	■ Incident Manager	■ Kein Zugriff
	■ Problem Manager	■ Kein Zugriff
Anfrage (schließt alle Unterordner ein)	■ Change Manager	■ Kein Zugriff
	■ Kundenservicemanager	■ Kein Zugriff
	■ Knowledge-Manager	■ Kein Zugriff
	■ Knowledge-Analyst	■ Kein Zugriff
	■ CA Service Desk-Manager	■ Vollzugriff
	■ Incident Manager	■ Ansicht
	■ Problem Manager	■ Kein Zugriff

Ordnername	Gruppenname	Zugriffsebene
Knowledge Management	■ Change Manager	■ Kein Zugriff
	■ Kundenservicemanager	■ Ansicht
	■ Knowledge-Manager	■ Vollzugriff
	■ Knowledge-Analyst	■ Ansicht
	■ CA Service Desk-Manager	■ Ablauf
	■ Incident Manager	■ Ansicht
	■ Problem Manager	■ Ansicht
Survey	■ Change Manager	■ Kein Zugriff
	■ Kundenservicemanager	■ Kein Zugriff
	■ Knowledge-Manager	■ Ansicht
	■ Knowledge-Analyst	■ Kein Zugriff
	■ CA Service Desk-Manager	■ Vollzugriff
	■ Incident Manager	■ Ansicht
	■ Problem Manager	■ Ansicht
Störungs- und Problemmanagement	■ Change Manager	■ Kein Zugriff
	■ Kundenservicemanager	■ Kein Zugriff
	■ Knowledge-Manager	■ Ansicht
	■ Knowledge-Analyst	■ Kein Zugriff
	■ CA Service Desk-Manager	■ Ablauf
	■ Incident Manager	■ Vollzugriff
	■ Problem Manager	■ Vollzugriff

Zugriffsebenen

Die Standardkonfiguration umfasst die folgenden Zugriffsebenen für Gruppen und Benutzer:

Kein Zugriff

Setzt alle Genehmigungen auf "Nicht angegeben".

Ansicht

Erlaubt dem Benutzer, den Ordner, den Bericht oder das Universum anzuzeigen. Wenn der Bericht Daten enthält, kann der Benutzer den Bericht öffnen und mit ihm interagieren. Wenn der Bericht keine Daten enthält, kann der Benutzer den Bericht nicht aktualisieren. Standardmäßig kann der Benutzer den Bericht bearbeiten und ihn in einem persönlichen Ordner abspeichern, um ihn dort aktualisieren. Sie können Benutzer daran hindern, Firmendokumente in persönlichen Ordnern zu speichern, indem Sie ein individuelles Zugriffsrecht einrichten, welches das Kopieren von Objekten in einen anderen Ordner nicht gestattet.

Ablauf

Erlaubt einem Benutzer, einen Bericht zu planen, jedoch nicht, diesen in Echtzeit zu aktualisieren.

Nach Bedarf ansehen

Erlaubt einem Benutzer, einen Bericht in Echtzeit zu aktualisieren. Wenn es sich bei dem Bericht um ein Web Intelligence-Dokument handelt, benötigt der Benutzer auch Zugriff auf das Universum und Verbindung mit einem Universum um die Aktualisierung auszuführen.

Vollzugriff

Erlaubt einem Benutzer, neue Berichte innerhalb eines Ordners zu erstellen, bestehende Berichte zu ändern oder Elemente zu löschen.

Erweitert

Wenn die vorhergehenden Zugriffsebenen nicht Ihren Anforderungen entsprechen, ermöglicht die Option "Erweitert" einen differenzierteren Zugriff.

Wenn die Zugriffsebene eines Benutzers oder einer Gruppe auf "Erweitert" gesetzt ist, dann ist eine differenziertere Steuerung der Berechtigungen verfügbar als bei den Rechten, die durch die Auswahl der Optionen "Anzeigen", "Ablaufplan", "View On Demand" oder "Vollzugriff" zugewiesen werden.

BusinessObjects-Ordner verwenden vererbte Sicherheitsfunktionen. Für untere und obere Ordnersebenen erhalten Sie erhalten die gleiche Autorisierung, die Ihnen oder Ihrer Gruppe zugewiesen wurden, es sei denn es gelten Einschränkungen für untere Ebenen, die gegen solch eine Autorisierung sprechen. Standardautorisierungen werden auf Ordner- und Gruppenebene eingerichtet. Benutzer erben die Rechte ihrer Gruppe für alle Objekte, die sich in einem Ordner und in untergeordneten Ordnern befinden.

CA Business Intelligence wird mit zwei Gruppen installiert: "Administratoren" und "Jeder". Der Gruppe "Jeder" wird die Zugriffsebene "Ablaufplan" zugewiesen, die das Planen und Anzeigen aller Berichtsobjekte ermöglicht.

Weitere Informationen:

[Berichtsordner](#) (siehe Seite 891)

Verweisen eines vorhandenen CA Business Intelligence-Servers auf einen CA SDM-Server

Wenn Sie über einen existierenden CA Business Intelligence-Server verfügen, können Sie mit ihm auf einen CA SDM-Server verweisen. Hierfür sind folgende Schritte erforderlich:

1. [Erstellen Sie eine neue ODBC-Datenquelle](#) (siehe Seite 895).
2. [Konfigurieren Sie das Universe](#) (siehe Seite 896).
3. [Exportieren Sie das Universe](#) (siehe Seite 897).
4. Starten Sie InfoView, um die Verbindung zu überprüfen.

Erstellen einer ODBC-Datenquelle

Sie können mithilfe des ODBC-Datenquellenadministrators eine ODBC-Datenquelle auf einem CA Business Intelligence-Server erstellen.

So erstellen Sie eine ODBC-Datenquelle:

1. Navigieren Sie zu "Start" > "Alle Programme" > "Verwaltung" > "Datenquellen (ODBC)".

Der ODBC-Datenquellenadministrator wird geöffnet.

2. Klicken Sie auf die Registerkarte "System-DSN" und dann auf "Hinzufügen".

Die Seite "Neue Datenquelle erstellen" wird geöffnet.

3. Wählen Sie "DataDirect OpenAccess", und klicken Sie auf "Fertig stellen".

Die Setup-Seite für "DataDirect OpenAccess ODBC" wird angezeigt.

4. Geben Sie "casd_Servername" in das Feld "ODBC Name" ein.

5. Klicken Sie auf "Erweitert".

Die Seite "Erweitert" wird angezeigt.

6. Klicken Sie auf "Hinzufügen".

Die Seite "Open Access Database Setup" wird geöffnet.

7. Füllen Sie die folgenden Felder aus:

- **Name.** Geben Sie "casd_Servername" ein.
- **IP-Adresse.** Geben Sie den *Servernamen* oder die IP-Adresse ein.

Hinweis: Senden Sie ein Ping-Signal an *Servername*, um die IP-Adresse zu ermitteln und dann die IP-Adresse statt *Servername* zu verwenden.

- **Port.** Geben Sie den Wert 1706 ein.
- **Typ.** (Optional) Geben Sie die Datenbank an, die auf dem Server verwendet wird. Dieses Feld dient lediglich als Referenzinformation.

8. Klicken Sie auf "OK".
9. Wählen Sie *casd_servername* in der Dropdown-Liste "Datenbank" aus.
10. Klicken Sie auf "OK".

Ihre ODBC-Datenquelle wurde erstellt.

Konfigurieren des Universums

Nachdem Sie ODBC-Datenquelle erstellt haben, müssen Sie das Universum konfigurieren, indem sie eine Verbindung zwischen CA SDM und CA Business Intelligence einrichten.

So konfigurieren Sie das Universum:

1. Starten Sie den Designer und melden Sie sich als Administrator an.
2. Klicken Sie auf "Datei" > "Importieren".
Die Seite "Import Universe" (Universum importieren) wird angezeigt.
3. Navigieren Sie, wählen Sie Ihr CA SDM-Universum aus, und klicken Sie auf "OK".
Die Meldung "Universe successfully imported" (Das Universum wurde erfolgreich importiert) wird angezeigt.
4. Klicken Sie auf "Datei" > "Parameter".
Die Seite mit den Universumsparametern wird angezeigt.
5. Klicken Sie auf "Bearbeiten".
Die Seite "Edit CA SDM connection" (CA SDM-Verbindung bearbeiten) wird angezeigt.
6. Geben Sie Benutzernamen und Kennwort des berechtigten CA SDM-Benutzers ein, z. B. Service Desk.
7. Wählen Sie "*casd_servername*" als Bezeichnung der Datenquelle, und klicken Sie auf "Weiter".
8. Klicken Sie auf "Test Connection" (Verbindung testen) um zu überprüfen, dass das CA SDM-Universum mit CA Business Intelligence kommuniziert.
9. Klicken Sie auf "Weiter" > "Weiter" > "Fertig stellen".
Das Universum wird konfiguriert.

Exportieren des Universums

Nachdem Sie das Universum konfiguriert haben, müssen Sie es vom Designer exportieren.

So exportieren Sie das benutzerdefinierte Universum:

1. Klicken Sie auf "Datei" > "Exportieren".

Das Dialogfeld "Universe exportieren" wird angezeigt.

2. Klicken Sie auf "Fortsetzen".

3. Klicken Sie auf "OK".

Das Universum wird exportiert.

Einrichten der Datenaufteilungssicherheit für die Berichterstellung

Der Zugriff auf die CA Business Intelligence-Berichterstellung ist durch die CA SDM-Datenpartitionssicherheit eingeschränkt. Alle CA SDM-Sicherheitseinstellungen, einschließlich derjenigen zu Datenpartition und Einschränkungen der Mandantenfähigkeit, werden automatisch auf Berichte angewendet.

Die Datenaufteilungssicherheit für Ihre spezielle Berichterstellungsumgebung wird während der Konfigurationphase nicht angewendet. Sie können Ihre Berichterstellungsumgebung so einrichten, dass sie mit vorhandenen Datenpartitionen in CA SDM arbeitet.

Verwenden Sie dazu die folgenden Tools:

- **BusinessObjects Central Management Console (CMC):** Ermöglicht die Verwaltung von Authentifizierungen und Genehmigungen für Anwender von BusinessObjects Enterprise.
- **BusinessObjects Designer:** Ermöglicht die Änderung des Universums von CA SDM, Knowledge Management, CMDB und Support-Automatisierung, welches eine Metaebene zwischen CA SDM-Schema und Reporting-Tools darstellt.
- **CA SDM Sicherheit und Rollenverwaltung:** Zum Einrichten der Datenaufteilungssicherheit, mit der Sie die Daten bestimmen, auf die die Anwender zugreifen können.

Hinzufügen des privilegierten CA SDM-Anwenders zu CMC

Die Verbindung mit dem Universum wird standardmäßig so konfiguriert, dass beim Datenzugriff der berechnigte Anwender und das Kennwort von Service Desk verwendet werden. Dieser Anwender sollte dem CMC als ein neuer CA Business Intelligence-Anwender hinzugefügt werden. Es gibt zwei Gründe für das Hinzufügen dieses Anwenders. Erstens: Sie benötigen diesen Benutzer, wenn Sie die Einrichtung der Datenpartitionssicherheit planen. Zweitens: So können Sie diesen Benutzer verwenden, wenn Sie anfänglich Berichte über die CA SDM-Registerkarte "Berichte" testen. Für die Registerkarte "Berichte" muss der Anwender sowohl in CA SDM als auch in CA Business Intelligence definiert sein.

Verwenden Sie die Anleitungen im *Implementierungshandbuch*, um Ihre CA SDM-Anwender dem CMC hinzuzufügen und das CA SDM-Konto für berechnigte Anwender zu konfigurieren.

Definieren der Universe-Datenbank-Anmeldeinformationen

Das Universum muss die Datenbank-Anmeldeinformationen verwenden, die mit dem BusinessObjects-Anwenderkonto verknüpft sind.

Hinweis: Vergewissern Sie sich, dass Sie beim Anmelden bei BusinessObjects Designer das Konto des berechtigten Benutzers verwenden, und nicht das Benutzerkonto des Administrators.

So definieren Sie die Datenbank-Anmeldeinformationen für das Universum:

1. Gehen Sie aus dem Startmenü zu "BusinessObjects XI" > "BusinessObjects Enterprise", "Designer".
2. Melden Sie sich beim Designer an.
Das Fenster "Designer" wird angezeigt.
3. Wählen Sie "Datei" > "Importieren" aus.
Das Dialogfeld "Import Universe" (Universum importieren) wird angezeigt.
4. Wählen Sie aus der Dropdown-Liste den Universenordner CA SDM, Knowledge Management, CMDB oder Support-Automatisierung aus.
Hinweis: Wenn Sie den Designer das erste Mal verwenden, wählen Sie "Durchsuchen" > "CA Universes" aus.
5. Überprüfen Sie den Dateipfad für den Importordner im Feld "Import Folder".
6. Klicken Sie auf "OK".
Das Universe-Fenster wird angezeigt.
7. Wählen Sie "Datei" > "Parameter" aus.
Das Dialogfeld "Universe-Parameter" wird angezeigt.

8. Klicken Sie auf der Registerkarte "Definition" auf "Bearbeiten".
Das Dialogfeld "Anmeldeparameter" wird angezeigt.
9. Aktivieren Sie das Kontrollkästchen "Use database credentials associated with Business Objects user account".
10. Klicken Sie auf "Weiter" > "Verbindungstest", und gehen Sie durch die angezeigten Dialogfelder "Universe-Verbindung".
11. Klicken Sie auf "OK", um den Vorgang zu beenden.
12. Wählen Sie "Datei" > "Exportieren" aus.
Das Dialogfeld "Export Universe" wird angezeigt.
13. Wählen Sie in der Drop-down-Liste "Domäne" das Universum aus, das Sie verwenden möchten.
14. Wählen Sie in der Liste der Gruppen die Option "Jeder".
15. Klicken Sie auf "OK", um die Universe-Änderungen zu exportieren.

Einrichten von Datenaufteilungen

Erstellen Sie in der Sicherheit und Rollenverwaltung eine Datenpartitionseinschränkung, die den Datenbank-Datensatzzugriff für alle Berichtsbenutzer einschränkt, die der Datenpartition zugewiesen sind.

Hinweis: Weitere Informationen zum Einrichten von Datenpartitionseinschränkungen finden Sie unter [Einrichten von Datenpartitionen](#) (siehe Seite 317).

Replizierte Datenbank für Offline-Berichterstellung

Um potenziellen Leistungsproblemen vorzubeugen, die sich auf die mit CA SDM installierten Berichtskomponenten auswirken könnten, können Sie eine replizierte Datenbank für Offline-Berichterstellungszwecke erstellen.

Hinweis: Weitere Informationen zum Erstellen einer replizierten Datenbank für Offline-Berichterstellung finden Sie in der Beispieldokumentation und den Skripts im Verzeichnis "NX_ROOT\samples\reporting".

Rollenbasierte Berichte

CA SDM präsentiert rollenbasierte Berichte in zwei Berichterstellungsrahmen auf der Registerkarte "Berichte". Jeder Rahmen bietet grafische Ansichten, mit denen die Anwender per Drilldown präzisere Berichtsdaten anzeigen können, die sich hinter den Diagrammen und zusammengefassten Gruppen verbergen. Auf der Registerkarte "Berichte" können Sie rollenbasierte Berichte verwalten und neue BusinessObjects-Berichte anzeigen.

Die Seite "Bericht – Liste" enthält Details der Berichte, die zur Verfügung stehen. Sie klicken auf das Symbol "Bericht - Liste", das im ausgewählten Rahmen angezeigt wird, um diese Seite zu öffnen.

Definieren rollenbasierter Berichte für die Rolle

Sie können die Berichts-Webformulare verwalten, die auf der Seite "Bericht - Liste" angezeigt werden, wenn ein dieser Rolle zugewiesener Anwender beim System angemeldet ist.

So definieren Sie einen rollenbasierten Bericht für die Rolle

1. Navigieren Sie auf der Registerkarte 'Verwaltung' zu 'Sicherheit und Rollenverwaltung', 'Rollenverwaltung', 'Rollenliste'.

Die Seite "Rollenliste" wird angezeigt. Die folgenden Standardrollen sind für die Berichterstellung verfügbar:

- Change Manager
- Kundenservicemanager
- Knowledge-Manager
- Knowledge-Analyst
- CA Service Desk-Manager
- Incident Manager
- Problem Manager

2. Wählen Sie *eine* der Berichterstellungsrollen aus der Liste.

Die Formularseite 'Rolle - Detail' wird angezeigt. Diese Seite enthält die folgenden Registerkarten:

Autorisierung

Hier können Sie die der Rolle zugewiesene Autorisierungsebene definieren.

Funktionszugriff

Definiert den Rollenzugriff für die einzelnen CA SDM-Funktionsbereiche.

Web-Schnittstelle

Passt die Web-Schnittstelle für die Rolle durch Definieren der Webseiten und der Inhalte der Online-Hilfe an, auf die die Anwender zugreifen können.

Knowledge Management

Gibt die Knowledge Management-Berechtigungen für die Rolle an.

KT-Dokumentsichtbarkeit

Gibt an, welchen Dokumentstatus die Rolle ansehen darf (z. B. "Entwurf", "Deaktiviert" und "Veröffentlicht").

Registerkarten

Definiert die Registerkarten, die angezeigt werden, wenn ein dieser Rolle zugewiesener Anwender bei CA SDM angemeldet ist.

Berichts-Webformulare

Definiert die Berichts-Webformulare, die für diese Rolle verfügbar sind.

'Los'-Ressourcen

Gibt an, welche Datensatztypen in der Drop-down-Liste "Los" für die Rolle angezeigt werden. Wählen Sie auf der Seite 'Rolle -Details' die Registerkarte 'Berichts-Webformulare' aus.

3. Klicken Sie die Registerkarte 'Berichts-Webformulare'.
Die Seite für die Berichts-Webformularliste wird angezeigt. Diese Seite enthält Details zu den verfügbaren Berichten.
4. Klicken Sie auf "Berichts-Webformulare aktualisieren".
Die Seite "Webformulare - Suche" wird angezeigt.
5. Geben Sie die Suchkriterien ein, um die Webformulare anzuzeigen, und klicken Sie auf "Suchen".
Die Seite "Zugewiesene Webformulare aktualisieren" wird angezeigt und enthält eine Liste der Formulare, die den Suchkriterien entsprechen.
6. Wählen Sie in der Liste links die Webformulare aus, die Sie für diese Rolle anzeigen möchten. Halten Sie die STRG-Taste gedrückt, während Sie mit der linken Maustaste klicken, um mehrere Elemente auszuwählen.
7. Nachdem Sie die gewünschten Formulare ausgewählt haben, klicken Sie auf die Schaltfläche 'Auswählen'.
Die ausgewählten Formulare werden in die Liste "Zugewiesene Berichts-Webformulare" rechts auf der Seite verschoben.
8. Klicken Sie auf "OK".
Die Seite "Rolle - Detail" wird angezeigt, und die ausgewählten Webformulare werden auf der Registerkarte "Berichts-Webformulare" aufgeführt.

Anzeigen neuer Berichte auf der Registerkarte 'Berichte'

Wenn ein Bericht für die Verwendung in CA SDM genehmigt wurde, wird er in den öffentlichen Abschnitt in InfoView verschoben und steht befugten Anwendern damit zur Verfügung. Um den Bericht zu CA SDM hinzuzufügen, muss der Administrator einige zusätzliche Schritte ausführen.

Sie können neue, in CA Business Intelligence erstellte Berichte auf der CA SDM-Registerkarte "Berichte" anzeigen. Verwenden Sie dazu die folgenden Tools:

- Web Screen Painter
- Rollenmanagement

Führen Sie zuvor Folgendes aus:

- Installieren und konfigurieren Sie CA Business Intelligence für die Zusammenarbeit mit CA SDM.

Hinweis: Weitere Informationen zur Installation finden Sie im *Implementierungshandbuch* und im *CA Business Intelligence-Installationshandbuch*.

- Die Anwenderberechtigungen, die Rollen und die [Authentifizierungsoptionen](#) (siehe Seite 889) für Ihre Berichterstellungsumgebung sind eingerichtet.

Schritt 1: Erstellen von zwei Webformular-Datensätzen zum Aufrufen von neuen Berichten

Standardmäßig enthält die Registerkarte "Berichte" zwei Berichterstellungs-Frames, mit deren Hilfe berechnete Anwender neue Berichte anzeigen können. In diesem Schritt erstellen Sie zwei Webformular-Datensätze und definieren die URLs, die auf die neuen Berichte verweisen.

So erstellen Sie zwei Webformular-Datensätze zum Aufrufen von Berichten:

1. Von der Registerkarte "Administration" navigieren Sie zu "Sicherheit und Rollenverwaltung", "Rollenverwaltung", "Webformulare".

Die Seite "Webformulare - Liste" wird angezeigt.

2. Klicken Sie auf "Neu erstellen".

Die Seite "Neues Webformular erstellen" wird angezeigt.

3. Geben Sie Daten in die folgenden Felder ein:

Name des Webformulars

Gibt den Namen für das Webformular an. Dieses Feld erfordert eine Eingabe.

Beispiel: Bericht zur Asset-Liste

Datensatzstatus

Geben Sie "Aktiv" an.

Code

Geben Sie einen eindeutigen Code an, der das Webformular im System identifiziert. Nachdem der Code definiert wurde, kann er nicht mehr geändert werden.

Beispiel: asset_list

Hinweis: Notieren Sie den Wert, den Sie in das Feld für den Code eingeben.

Typ

Wählen Sie einen Bericht aus.

Beschreibung

(Optional) Geben Sie eine kurze Beschreibung des Webformulars ein.

Ressource

Geben Sie den URL an, der den neuen Bericht aufruft.

Beispiel: Öffnen Sie in "Rollenmanagement" das Webformular für die Asset-Liste, und geben Sie den URL an, der in diesem Formular angezeigt wird.

`$B0ServerURL?sPath=[Home],[Public+Folders],[CA+Reports],[CA+Service+Desk],[Asset]&sDocName=Asset+List&sViewer=html`

4. Klicken Sie auf "Speichern".

Die Webformulardefinition wird gespeichert und die Seite "Webformular - Detail" angezeigt.

5. Wiederholen Sie die Schritte 1 bis 3, um einen zweiten Webformular-Datensatz zu erstellen, der den zweiten Berichts-URL aufrufen soll. Notieren Sie den Wert, den Sie in das Feld für den Code eingeben haben.

Schritt 2: Erstellen einer Multiframe-Seite und Zuweisen der neuen Berichte

Erstellen Sie in Web Screen Painter eine Multiframe-Webseite mit zwei vertikalen Frames. Dies wird als "Frameset" bezeichnet. Weisen Sie dann die Webformular-Datensätze, die Sie in Schritt 1 erstellt haben, diesem Frameset zu.

Hinweis: Sie können diese Seite mit beliebig vielen Frames erstellen. Denken Sie daran, dass zusätzliche Frames die Sichtbarkeit auf der Registerkarte "Berichte" begrenzen.

So erstellen Sie eine Multiframe-Seite und weisen Berichte zu:

1. Wählen Sie in Web Screen Painter die Option "Datei" > "Neu" aus.
Das Dialogfeld "Neues Formular" wird angezeigt.
2. Füllen Sie die Felder der Schnittstelle und der Formulargruppe mit den entsprechenden Daten aus.
3. Wählen Sie aus Liste der Dateinamen "multiframe.template" aus.

4. Klicken Sie auf "Neu".

Das Fenster "multiframe.html" wird angezeigt.

5. Wählen Sie "Steuerelemente" > "Frameset einfügen".

Das Dialogfeld "Frameset einfügen" wird angezeigt.

6. Verändern Sie die Standardeinstellungen nicht, und klicken Sie auf "OK".

Zwei vertikale Frames werden im Frameset angezeigt.

7. Klicken Sie mit der rechten Maustaste auf den linken vertikalen Frame, und wählen Sie im Kontextmenü die Option "Eigenschaften" aus.

Das Dialogfeld "Eigenschaften - Frameset" wird angezeigt.

8. Wählen Sie das leere Feld neben dem Attribut "web_form_name", und klicken Sie dann auf die Schaltfläche "(...)".

Das Dialogfeld "Name des Webformulars eingeben" wird angezeigt.

9. Geben Sie den Codewert des ersten Berichts an.

Beispiel: asset_list

10. Wenn der Name des Berichtswbformulars gefunden wurde, klicken Sie auf "Validieren".

11. Klicken Sie mit der rechten Maustaste auf den rechten vertikalen Frame, geben Sie den Codewert vom zweiten Bericht ein, und validieren Sie dann den Bericht.

12. Speichern Sie die Seite "multiframe.html". Notieren Sie diesen Dateinamen.

Beispiel: report_mframe.html

13. Wählen Sie "Datei" > "Veröffentlichen".

Indem Sie das Formular veröffentlichen, machen Sie es für alle CA SDM-Anwender verfügbar. Für die Analystenrolle ist die Datei in dem folgenden Verzeichnis verfügbar: Program Files/CA/Service Desk/Site/mods/www/html/web/analyst/report_mframe.html.

Hinweis: Wenn Sie nach Multiframe-Webformularen in CA SDM suchen, navigieren Sie auf der Registerkarte "Administration" zu "Sicherheit und Rollenmanagement" > "Rollenmanagement" > "Webformularen". Auf der Registerkarte "Eigenschaften" gibt diese Spalte die Bezeichnung von "web_form_name" für ein Multiframe-Formular in Web Screen Painter an.

Schritt 3: Erstellen Sie eine Startseite für die Registerkarte "Berichte".

Erstellen Sie in "Rollenmanagement" eine Startseite, um die in Schritt 2 erstellte Multiframe-Webseite aufzurufen.

So erstellen Sie eine Startseite für die Registerkarte "Berichte":

1. Von der Registerkarte "Administration" navigieren Sie zu "Sicherheit und Rollenverwaltung", "Rollenverwaltung", "Webformulare".

Die Seite "Webformulare - Liste" wird angezeigt.

2. Klicken Sie auf "Neu erstellen".

Die Seite "Neues Webformular erstellen" wird angezeigt.

3. Füllen Sie die folgenden Felder aus:

Name des Webformulars

Gibt den Namen für das Webformular an. Dieses Feld erfordert eine Eingabe.

Beispiel: Startseite

Datensatzstatus

Gibt den Status "Aktiv" oder "Inaktiv" an.

Code

Gibt den eindeutigen Code an, der das Webformular im System identifiziert. Nachdem der Code definiert wurde, kann er nicht mehr geändert werden.

Beispiel: start_page

Typ

Gibt HTML an.

Beschreibung

(Optional) Liefert eine kurze Beschreibung des Webformulars.

Ressource

Gibt den URL an, der den neuen Bericht aufruft.

Beispiel: Wählen Sie auf der Seite "Webformular - Liste" den Datensatz "Administratorberichte - Multiframe" aus. Geben Sie die URL für dieses Formular an. Geben sie am Ende dieses Pfades die neue Multiframe-Seite an (report_mframe.html).

`$cgi?SID=$SESSION.SID+FID=123+OP=DISPLAY_FORM+HTML=report_mframe.html`

Klicken Sie auf "Speichern".

Der neue Startseiten-Datensatz wird auf der Seite "Webformular - Liste" angezeigt.

Schritt 4: Erstellen Sie einen Datensatz für die Registerkarte "Berichte" und weisen Sie die Startseite zu.

Erstellen Sie in "Rollenmanagement" eine neue Registerkarte "Berichte" und geben Sie die in Schritt 3 erstellte Startseite an.

So erstellen Sie eine Registerkarte und weisen die Startseite zum Aufrufen der Berichte zu:

1. Wählen Sie auf der Registerkarte "Administration" "Sicherheit und Rollenverwaltung", "Rollenverwaltung", "Registerkarten" aus.

Die Seite "Registerkarten - Liste" wird angezeigt.

2. Klicken Sie auf "Neu erstellen".

Die Seite "Neue Registerkarte erstellen" wird angezeigt.

3. Füllen Sie die folgenden Felder aus:

Registerkartenname

Gibt den Namen an, der die Registerkarte innerhalb der Verwaltungsschnittstelle kennzeichnet. Der Registerkartenname wird beispielsweise auf der Seite "Registerkarten - Liste" angezeigt.

Beispiel: Registerkarte "Berichte"

Code

Gibt den Code an, der diese Registerkarte im System identifiziert. Nachdem der Code definiert wurde, kann er nicht mehr geändert werden.

Beispiel: reports_tab

Datensatzstatus

Geben Sie "Aktiv" an.

Anzeigename

Gibt den Namen an, der in der grafischen Darstellung der Registerkarte in der Benutzerschnittstelle angezeigt wird.

Beispiel: Registerkarte "Berichte"

Startseite

Gibt das Webformular an, das im Hauptfenster angezeigt wird, wenn ein Anwender diese Registerkarte auswählt.

Beispiel: Startseite

4. Klicken Sie auf "Speichern".

Das Formular wird auf der Seite "Webformular - Liste" angezeigt.

Schritt 5: Weisen Sie den Datensatz der Registerkarte einem Rollendatensatz zu.

Weisen Sie der gewünschten Rolle in der Rollenverwaltung die Registerkarte "Berichte" zu, die auf der Seite "Rolle - Detail" aufgeführt wird. Wenn ein dieser Rolle zugewiesener Anwender sich im System anmeldet, wird ihm in der Web-Schnittstelle die neue Registerkarte "Berichte" angezeigt.

So weisen Sie den Datensatz der Registerkarte einem Rollendatensatz zu:

1. Wählen Sie auf der Registerkarte "Administration" "Sicherheit und Rollenverwaltung", "Rollenverwaltung", "Rollenliste" aus.
Die Seite "Rollenliste" wird angezeigt.
2. Wählen Sie die gewünschte Rolle aus der Rollenliste aus.
Die Seite "Rolle - Detail" wird angezeigt.
3. Wählen Sie unten auf der Seite "Registerkarten" > "Registerkarten aktualisieren" aus.
Die neue Registerkarte wird in der Liste der Registerkarten angezeigt.

Erstellen einer Startseite für die Schaltfläche "InfoView"

Sie haben die Möglichkeit, die Schaltfläche "InfoView", die BusinessObjects-InfoView öffnet, einem neuen Fenster auf der Registerkarte "Berichte" hinzuzufügen. Diese Option ist auf der Registerkarte "Berichte" über "Startseite" zugänglich.

So erstellen Sie eine Startseite für die Schaltfläche "InfoView":

1. Von der Registerkarte "Administration" navigieren Sie zu "Sicherheit und Rollenverwaltung", "Rollenverwaltung", "Webformulare".
Die Seite "Webformulare - Liste" wird angezeigt.
2. Klicken Sie auf "Neu erstellen".
Die Seite "Neues Webformular erstellen" wird angezeigt.
3. Füllen Sie die folgenden Felder aus:

Name des Webformulars

(Erforderlich) Gibt den Namen für das Webformular an.

Beispiel: InfoView-Seite

Datensatzstatus

Gibt den Status "Aktiv" oder "Inaktiv" an.

Code

Gibt den Code an, der das Webformular im System identifiziert.

Beispiel: info_view_page

Typ

Gibt HTML an.

Beschreibung

(Optional) Beschreibt das Webformular.

Ressource

Gibt den URL an, der die Berichterstellungs-Frames aufruft.

Beispiel: Wählen Sie auf der Seite "Webformular - Liste" den Datensatz "Administrator - InfoView" aus. Geben Sie die URL für dieses Formular an. Geben Sie den URL an, der in dem Formular angezeigt wird.

```
$cgi?SID=$SESSION.SID+FID=123+OP=DISPLAY_FORM+HTML=show_report_frames.html+KEEP.report_form=start_page
```

Klicken Sie auf "Speichern".

Die InfoView-Startseite wird auf der Seite "Webformular - Liste" angezeigt.

Schritt 7: Weisen Sie die Startseite der Schaltfläche "InfoView" dem Datensatz der Registerkarte "Berichte" zu.

Weisen Sie in "Rollenmanagement" die Startseite der Schaltfläche "InfoView", die sie in Schritt 6 erstellt haben, dem Datensatz der Registerkarte "Berichte" zu.

So weisen Sie die Startseite der Schaltfläche "InfoView" dem Datensatz der Registerkarte "Berichte" zu:

1. Wählen Sie in "Rollenmanagement" auf der Seite "Registerkarten - Liste" den neuen Webformulardatensatz der Registerkarte "Berichte" aus.

Die Detailseite wird angezeigt.

2. Wählen Sie "Bearbeiten".

Die Seite "Registerkarte aktualisieren" wird angezeigt.

3. Legen Sie die neue Startseite für die Schaltfläche "InfoView" im Feld "Startseite" fest.

4. Klicken Sie auf "Speichern".

Wenn Sie die Registerkarte "Berichte" öffnen, wird die Schaltfläche "InfoView" in der rechten oberen Ecke des Formulars angezeigt.

Webbasierte Berichte

CA Business Intelligence installiert eine Reihe von webbasierten, vordefinierten Berichten für CA SDM und Knowledge Management. Sie werden entweder mit BusinessObjects Enterprise Web Intelligence oder Crystal Reports entwickelt. Die Berichte können als Modelle zum Definieren standortspezifischer Berichte verwendet werden.

Diese Berichte befinden sich in Ordnern, die nach der Installation automatisch auf dem CA Business Intelligence-Berichtserver bereitgestellt werden.

Sicherheitseinstellungen können auf Ordner und Dokumente angewendet werden, um anzugeben, ob der Zugriff darauf global, für bestimmte Rollen oder Personen möglich ist.

Hinweis: BusinessObjects InfoView umfasst ein Anwenderhandbuch mit Informationen zur Verwendung von BusinessObjects InfoView. Klicken Sie auf das Hilfesymbol in InfoView, um auf das Anwenderhandbuch zuzugreifen. Allgemeine Informationen zur Verwendung von vordefinierten Berichten finden Sie in der *Online-Hilfe*.

Weitere Informationen:

[Business Objects InfoView-Schnittstelle](#) (siehe Seite 909)

[Navigieren zu Berichten](#) (siehe Seite 910)

[InfoView-Voreinstellungen](#) (siehe Seite 910)

[Planen von Berichten](#) (siehe Seite 910)

[Einrichten der Datenanalyse](#) (siehe Seite 911)

[Veröffentlichen und Verteilen von Berichten](#) (siehe Seite 912)

Business Objects InfoView-Schnittstelle

Über die Registerkarte "CA SDM-Berichte" können Analysten und Manager mit Berichten arbeiten, die für ihre Rolle definiert sind, oder ihre persönlichen Berichte verwalten, indem sie auf die InfoView-Schaltfläche klicken. Über InfoView können Sie auf Crystal Reports- und Web Intelligence-Dokumente sowie andere Objekte zugreifen und diese Ihren Anforderungen entsprechend organisieren.

Die in InfoView verfügbaren Funktionen variieren nach Inhaltstyp. Im Allgemeinen können Sie jedoch Informationen in Ihrem Webbrowser anzeigen, sie in andere Geschäftsanwendungen (z. B. Microsoft Excel) exportieren und an einem angegebenen Ort speichern.

Hinweis: Die Ordner und Objekte, die Sie in InfoView sehen können, sind von der entsprechenden Gruppen- und Rollenzuweisung abhängig.

Navigieren zu Berichten

Im linken Bereich des Fensters "InfoView" können Sie zu den folgenden vordefinierten Berichten navigieren, um den Bericht anzuzeigen, zu planen, zu bearbeiten oder auszuführen oder um den Verlauf und die Eigenschaften für einen Bericht anzuzeigen.

So zeigen Sie einen Bericht an:

1. Verwenden Sie *eine* der folgenden Methoden, um InfoView zu öffnen:
 - Klicken Sie auf der Registerkarte "Berichte" in CA SDM auf die Schaltfläche "InfoView".
 - Navigieren Sie über das Startmenü zu "Programme", "BusinessObjects XI", "BusinessObjects Enterprise", "BusinessObjects Enterprise Java InfoView".Die Startseite von InfoView wird angezeigt.
2. Navigieren Sie im linken Fenster zur Ordnerstruktur "Öffentliche Ordner/CA-Berichte/CA SDM".
3. Klicken Sie auf den Ordner, der dem Berichtstyp entspricht, den Sie anzeigen möchten.
4. Klicken Sie auf den Berichtsnamen für den Informationstyp, den Sie sehen möchten.
Der Bericht wird in BusinessObjects InfoView angezeigt.

InfoView-Voreinstellungen

Anwender können allgemeine Voreinstellungen festlegen und damit angeben, dass InfoView mit einer ihrer persönlichen Dashboard-Seiten gestartet werden soll, die sie mit dem Tool "Eigene InfoView" in Web Intelligence entworfen haben. Sie können auch ihre persönlichen Voreinstellungen für die Anzeige von Web Intelligence- und Crystal Reports-Berichten festlegen.

Planen von Berichten

InfoView unterstützt das Planen von Berichten. Für Ad-hoc-Berichte werden geplante Berichte im Abschnitt "Eigene Ordner" gespeichert. Wenn ein Bericht so festgelegt wurde, dass er beim Öffnen aktualisiert wird, greift das System auf die Datenbank zu, um dem Endbenutzer bei jeder Anzeige des Berichts die aktuellen Informationen anzuzeigen. Benutzer können Berichte so planen, dass sie zu bestimmten Zeiten ausgeführt werden.

Administratoren können Kalender definieren, um die entsprechenden Ausführungszeiten anzugeben. Zum Beispiel kann ein Benutzer über die Option "Wenn" (für Zeitplanung und Häufigkeit) einen Kalender auswählen, in dem die verfügbaren Geschäftstage angezeigt und die Nicht-Geschäftstage ignoriert werden.

Hinweis: Weitere Informationen zum Planen von Berichten finden Sie in der BusinessObjects-Dokumentation.

Beim Planen können Benutzer folgendermaßen vorgehen:

- Geben Sie den Zeitpunkt und das Intervall für den Ablaufplan an (z. B. jetzt, stündlich, täglich und wöchentlich).
- Geben Sie den Bestimmungsort an, z. B. ein Postfach, einen Dateispeicherort oder einen E-Mail-Empfänger.
- Geben Sie an, an welche Postfächer der Bericht gesendet werden soll.
- Geben Sie das Ausgabeformat an, z. B. Web Intelligence, Crystal Report, Microsoft Excel und Adobe Acrobat.
- Geben Sie die Optionen für die Zwischenspeicherung an. Standardmäßig werden die Dokumentergebnisse auf dem Ausgabedatei-Repository-Server gespeichert. Benutzer können den Bericht über den Web Intelligence Report Server vom System zwischenspeichern lassen, indem sie ein Zwischenspeicherformat und ein Gebietsschema auswählen.
- Wählen Sie eine Servergruppe aus, um die Anfrage zu bearbeiten. Wenn ein definiertes Ereignis ausgewählt wird, wird das Objekt nur ausgeführt, wenn die Nebenbedingung oder das Nebenereignis auftritt.

Hinweis: Wenn Dateneinschränkungen im Abschnitt der öffentlichen Ordner in InfoView mit Hilfe von CA SDM-Datenpartitionen verwaltet werden, dann müssen geplante Berichte in öffentlichen Ordnern für jeden Benutzer definiert werden.

Einrichten der Datenanalyse

Ein interaktiver Viewer bietet umfassende Tools, mit denen Sie die Anzeige der Berichtsdaten anpassen können. Sie können per Drilldown verschiedene Detailstufen abrufen, z. B. von der Gruppe über den Zuständigen bis hin zu den eigentlichen Requests.

Mit dem interaktiven Viewer können Sie folgende Aufgaben ausführen:

- Das Erscheinungsbild des Berichts ändern, indem Sie die Daten in einem anderen "Block"-Format darstellen, z. B. als Kreisdiagramm. Wenn Sie beispielsweise mit der rechten Maustaste in den Bericht klicken und die Option "Tabelle umwandeln in" wählen, werden Berichtsdarstellungsfunktionen angezeigt.
- Durchführen verschiedener Aufgaben, z. B. Sortieren, Erstellen von Berichtsaufteilungen, Berechnen, Filtern, Einstufen des Berichts.
- Informationen mit anderen Anwendern und Gruppen teilen.

Veröffentlichen und Verteilen von Berichten

InfoView-Anwender können Berichtsdaten im Excel-, PDF- oder CSV-Format speichern und dann an einen Dateispeicherort, einen Posteingang, eine E-Mail-Adresse oder eine FTP-Site verteilen.

Wenn ein Bericht für die Verwendung in CA SDM genehmigt wurde, wird er in den öffentlichen Abschnitt verschoben und steht autorisierten Anwendern damit zur Verfügung. Sicherheitseinstellungen können auf Ordner und Dokumente angewendet werden, um anzugeben, ob der Zugriff darauf global, für bestimmte Rollen oder Personen möglich ist. Sicherheit wird in der BusinessObjects Central Management Console (Zentrale Verwaltungskonsole, CMC) verwaltet.

KPIs (Kritische Prozess-Indikatoren)

Kritische Prozess-Indikatoren (KPIs) sind Metriken, mit deren Hilfe Sie Bereiche Ihrer Service-Management-Umgebung identifizieren können, die möglicherweise administrative Schritte oder eine Feinabstimmung der Konfiguration erfordern.

Ihre KPI-Definitionen konfigurieren Sie in der CA SDM-Web-Schnittstelle. Die erstellten Daten werden in der CA SDM-Datenbank gespeichert und sind zum Erstellen [webbasierter Berichte](#) (siehe Seite 909) verfügbar.

Hinweis: Neben der Definition von KPI-Abfragen können Sie den KPI-Daemon so konfigurieren, dass CA SDM-Ticketdaten abgerufen werden, sobald ein Ticket geöffnet oder geschlossen wird oder bestimmte Felder geändert werden.

Durch Definieren und Überwachen einer sorgfältig zusammengestellten Gruppe von KPIs können Sie die Leistungsfortschritte Ihrer Organisation messen und wertvolle Daten als Grundlage für strategische Entscheidungen zur IT-Umgebung erfassen.

Hinweis: Weitere Informationen zu den KPI-Datenbanktabellen finden Sie im *technischen Referenzhandbuch*.

KPI-Typen

CA SDM unterstützt drei KPI-Typen:

- **System-KPIs:** werden gemeinsam mit dem Produkt installiert. Sie können die KPIs gemäß Ihren Anforderungen ändern, Sie können jedoch keine neuen System-KPIs erstellen.
- **KPIs "Gespeicherte Abfrage":** rufen eine gespeicherte Abfrage auf, um Indikatoren aus der Datenbank zu erhalten. Sie können benutzerdefinierte KPIs vom Typ "Gespeicherte Abfrage" erstellen oder die vordefinierten, mit dem Produkt installierten, Beispiele ändern.

- **SQL KPIs:** ermöglichen Ihnen, eine vollständige SQL-Abfrage direkt in den KPI zu integrieren. Sie können benutzerdefinierte KPIs vom Typ "Gespeicherte Abfrage" erstellen oder die vordefinierten, mit dem Produkt installierten, Beispiele ändern.

Hinweise:

- Weitere Informationen über die Konfiguration aller drei KPI-Typen finden Sie in der *Online-Hilfe*.
- KPIs können nicht gelöscht werden, egal ob sie vordefiniert oder benutzerdefiniert sind. Wenn ein KPI nicht mehr benötigt wird, können Sie den Datensatzstatus auf "Inaktiv" setzen, um so den KPI zu löschen.

Vordefinierte KPIs

Von jedem Typ werden einige KPIs zusammen mit CA SDM installiert. Die einzelnen KPI-Typen können Sie in diesem Handbuch nachschlagen.

Sie können die vordefinierten KPIs vom Typ "Gespeicherte Abfrage" und "SQL" mit ihren ursprünglichen Definitionen verwenden. Sie können sie aber auch als Ausgangspunkt für Ihre eigenen, benutzerdefinierten KPIs verwenden.

Sie können die vordefinierten System KPIs mit ihren ursprünglichen Definitionen benutzen oder einige der Felder anpassen, um Ihren Bedürfnissen zu entsprechen.

Hinweis: Die meisten der vordefinierten KPIs sind standardmäßig inaktiv. Filtern Sie die KPI-Listenseite, um inaktive KPIs in der Web-Schnittstelle anzuzeigen.

KPI-Daemon

Der KPI-Daemon dient zur Wiederherstellung, Organisation und Speicherung von KPI-spezifischen Indikatoren. Der Daemon wird kontinuierlich ausgeführt und führt zu festgelegten Intervallen Daten aus verschiedenen Systemressourcen zusammen.

Wenn die Aktualisierungszeit eines KPI erreicht wird, interagiert der KPI-Daemon mit anderen Systemkomponenten folgendermaßen:

- **System KPI:** Sendet eine Anfrage an einen Ziel-Daemon (Web-Engine, "domsrvr", "bpvrtddb" oder "db_agents"), um Daten über Anzahl oder Dauer zu erhalten.
- **KPI "Gespeicherte Abfrage":** Sendet eine Anfrage an "domsrvr", um Daten über die Anzahl zu erhalten.

- **SQL KPI:** Sendet eine Anfrage an "domsrvr", um Daten über Anzahl, Summe, Maximum oder Dauer zu erhalten.

Wenn der KPI-Daemon die angefragten Daten erhält, speichert er den entsprechenden Indikator in der Datenbank.

Hinweis: Die berechnete Dauer basiert auf einer Änderung von Werten in einem Ticket in Echtzeit, nicht während der Geschäftszeit.

System-KPIs

System-KPIs ermöglichen ihnen, Indikatoren über CA SDM-Prozesse zusammenzustellen.

Die folgenden Prozesstypen werden unterstützt:

- **domsrvr:** CA SDM-Objektmanager (Serverprozess) Der Objektmanager sorgt auch für das Zwischenspeichern verschiedener Datensätze und Tabellen für Clients.
- **bpvrtddb:** Der BOP Virtuelle Datenbankserver ermöglicht die Verwendung mehrerer Objektmanager in der CA SDM-Umgebung. Die Objektmanager stellen eine Verbindung zur virtuellen Datenbank her, die wiederum den Zugriff auf die Datenbank-Agenten vermittelt. Zum Beispiel stellt die virtuelle Datenbank beim Abruf eines neuen Bereichs von Ticket-Referenznummern sicher, dass nur ein Objektmanager gleichzeitig auf die Tabelle mit den Referenznummern zugreift.

Abhängig von Ihrer CA SDM-Konfiguration stellen die Objektmanager eine Verbindung mit der virtuellen Datenbank der folgenden Server her:

- Konventionell: Alle Objektmanager, die auf dem Primärserver oder Sekundärserver ausgeführt werden, stellen eine Verbindung mit der virtuellen Datenbank des Primärservers her.
- Erweiterte Verfügbarkeit: Alle Objektmanager stellen eine Verbindung zur virtuellen Datenbank des gleichen Servers her, auf dem sie ausgeführt wird. Zum Beispiel stellen Objektmanager, die auf dem Anwendungsserver ausgeführt werden, nur eine Verbindung zur virtuellen Datenbank des Anwendungsservers her.

Die virtuelle Datenbank ist auch ein Zwischenspeicher von Datenbankinformationen für Objektmanager.

- **db_agents:** Datenbank-Agenten führen SQL-Abfragen aus und steuern die Interaktion zwischen CA SDM und dem Datenbankmanagementsystem (DBMS). Datenbank-Agenten halten am CA SDM-Datenbankschema fest und übersetzen den SQL-Code in das vom DBMS benötigte Formular (zum Beispiel, Oracle).

- **Web-Engine:** CA SDM-Komponente, die einen Webbrowser mit einem Objektmanager verbindet. Die Verbindung erfolgt mit Hilfe eines pdmweb-CGI, das auf Microsoft IIS oder Apache Tomcat ausgeführt wird.

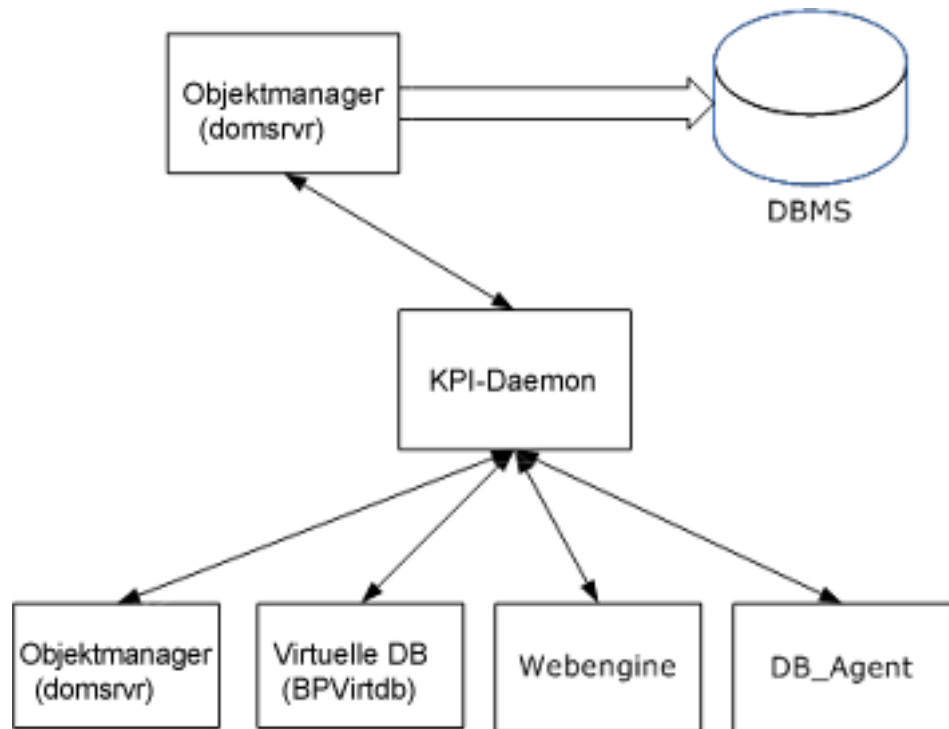
Abhängig von Ihrer CA SDM-Konfiguration muss eine Web-Engine für WSP auf folgenden Servern vorhanden sein, damit WSP-Schemadesigner Schemadateien schreiben können:

- Konventionell: Primärserver
- Erweiterte Verfügbarkeit: Hintergrundserver

Web-Engines sind der eigentliche Client des Objektmanagers für den Webbrowser eines Anwender-Clients. Web-Engines bewirken das Zwischenspeichern von .html-Webformularen für verbundene Anwender. Sie können den Cache-Speicher mit dem Hilfsprogramm "pdm_webcache" bearbeiten. Mit dem Hilfsprogramm "pdm_webstat" können Sie Verbindungsstatistiken für den Client anzeigen.

Hinweis: Weitere Informationen zu diesen Prozessen finden Sie im *Implementierungshandbuch*.

Das folgende Diagramm veranschaulicht den Datenfluss für System-KPIs.



Alle System-KPIs geben einen der folgenden Indikatoren aus:

- Anzahl
- Dauer

Beispiel für System-KPIs

- Dieses Beispiel generiert eine Zählung der an die BOP Virtuelle Datenbank geschickten Aktualisierungsanfragen:
`updateCt`
- Dieses Beispiel berichtet, wie lange die Fertigstellung von Aktualisierungen, Einfügungen und Löschungen in die BOP Virtuelle Datenbank gedauert haben:
`virtddbUpdateResponseDt`

Gespeicherte Abfrage-KPI

Mit gespeicherten Abfrage-KPI können Sie Berichte erstellen, die auf einer von der CA SDM-Datenbank abgerufenen Zählungsmetrik basiert.

CA SDM sorgt für einen Satz von vordefinierten gespeicherten Abfragen. Viele von ihnen sind nützlich, so wie sie sind. Sie können sie auch für spezielle Anforderungen anpassen oder sie als Modelle für das Schreiben Ihrer eigenen Abfragen verwenden.

Alle gespeicherten KPI verfügen über den Metriktyp "Anzahl".

Hinweis: Sie können mit gespeicherten Abfragen Zählerfelder für Ihr Web-Schnittstellen-Scoreboard oder Ihre KPI-Metriken oder beides erstellen. Um eine gespeicherte Abfrage in einer KPI-Definition zu verwenden, muss die Abfrage für die KPI-Verwendung ermöglicht werden. Weitere Informationen finden Sie unter [Einrichten gespeicherter Abfragen](#) (siehe Seite 490).

Beispiele für gespeicherte Abfrage-KPI

- In diesem Beispiel werden die ausstehenden Änderungsaufträge am Standort des Zuständigen gezählt:
`@cnt.location.name-Changes`
- In diesem Beispiel werden die Workflow-Aufgaben gezählt, die vor Mitternacht des aktuellen Tages eine SLA verletzen werden:
Workflow-Aufgaben für Issues, die heute eine SLA verletzen

SQL KPIs

SQL-KPI sorgen für mehr Flexibilität als gespeicherte Abfrage-KPI. Mit SQL-KPI können Sie Ihre eigenen Abfragen in die CA SDM-Datenbank schreiben, um die folgenden Arten von Metriken zu erstellen:

- Summe
- Anzahl

- Max.
- Dauer

Hinweis: Ihr SQL-Code muss mit der SQL92-Syntax kompatibel sein.

Die folgenden Erwägungen gelten für SQL-KPIs:

- Um den SQL-Code für diese Beispielabfragen anzuzeigen, öffnen Sie die Abfragedefinitionen auf der KPI-Listenseite.

Hinweis: Weitere Anweisungen finden Sie in der *Online-Hilfe*.

- Das @-Symbol wird in SQL-KPI nicht unterstützt. Verwenden Sie stattdessen die Syntax gemäß dem folgenden Beispiel zusammen mit einem Attributalias:

```
SELECT * FROM cr WHERE assignee_last_name = "Schmied"
```

Für dieses Beispiel könnten Sie einen vordefinierten Attribut-Aliasnamen benutzen. Die Seite "Attribut-Aliasname - Detail" wird wie folgt angezeigt:

```
"   Objektname      = cr
"   Aliasname        = assignee_last_name
"   Status           = Aktiv
"   Aliaswert        = assignee.last_name
```

Beispiele: SQL-Abfrage-KPI

- Bei diesem vordefinierten Beispiel wird die Summe der geschätzten Kosten aller ausstehenden Änderungsauftrags-Workflow-Aufgaben ermittelt:
Summe der geschätzten Kosten ausstehender Änderungsauftrags-Workflow-Aufgaben
- Bei diesem vordefinierten Beispiel wird die Anzahl der aktiven Änderungsaufträge ermittelt, die geschlossen und erneut geöffnet wurden:
Anzahl der erneut geöffneten Änderungsaufträge

KPI - Felder

In der folgenden Tabelle werden die KPI-Felder beschrieben. Die Spalten "Sys.", "S.Q." und "SQL" zeigen die KPI-Typen, zu denen jedes Feld gehört ("System", "Gespeicherte Abfrage" oder "SQL").

Hinweis: Alle Felder sind erforderlich, falls sie nicht ausdrücklich als optional angegeben sind.

Feld	Sys.	S.Q.	SQL	Beschreibung
KPI Name	X	X	X	Legt den Anzeigenamen für den KPI-Datensatz fest. Nicht editierbar
Typ	X	X	X	Definiert den Datensatz als ein System, eine gespeicherte Abfrage oder einen SQL-KPI. Nicht editierbar
Vorhandene Version beibehalten	X	X	X	Gibt an, dass die aktuelle Version des KPI-Datensatzes beibehalten wird, wenn der Datensatz aktualisiert wird. Kann bearbeitet werden, wenn die Einstellung "@NX_ALWAYS_KEEP_KPI_VERSIONS" in "NX.env" auf "Nein" festgelegt ist.
Version	X	X	X	Zeigt die Versionsnummer des KPI-Datensatzes an. Die Versionsnummer wird bei jeder Datensatzaktualisierung inkrementiert. Nicht editierbar
Datensatzstatus	X	X	X	Gibt an, ob der KPI aktiv ist (Daten sammelt) oder inaktiv ist (keine Daten sammelt). Kann nur bearbeitet werden, wenn die Funktion "In Liste bearbeiten" auf der KPI-Listenseite verwendet wird.
Metriktyp	X	X	X	Gibt die Art der Berechnung an, die der KPI durchführt. ■ Bei gespeicherten Abfrage-KPI handelt es sich immer um den Typ "Anzahl". ■ Bei System-KPI kann es sich um den Typ "Anzahl" oder "Dauer" handeln. ■ Bei SQL-KPI kann es sich um den Typ "Anzahl", "Summe", "Max" oder "Dauer" handeln. Kann nur für KPI vom Typ SQL bearbeitet werden.
AktualisierenUhrzeit	X	X	X	Gibt das Zeitintervall für das Abrufen von KPI-Metriken aus der Datenbank an. Der Wert kann bearbeitet werden. Die Aktualisierungszeit wird im HH:MM:SS-Format angegeben.

Feld	Sys.	S.Q.	SQL	Beschreibung
Prozess Typ	X			System-KPI (siehe Seite 914)-Metriken können von den folgenden CA SDM-Prozessen abgeleitet werden: ■ domsrvr – Objektmanager ■ bpvirtddb – BOP Virtual-Datenbankserver ■ db_agents – Datenbank-Agenten ■ webengine – Der CA SDM-Web-Client
System Name	X			Der interne Name des System-KPIs. Nicht editierbar
Anwender Kontext		X	X	(Optional) Gibt die Anwender-ID eines CA SDM-Kontakts an. Anhand der Rolle des Kontakts und der Mandantenzuweisungen wird die Datenpartition für die Metriken bestimmt, die vom KPI erstellt werden. Der Wert kann bearbeitet werden.
Gespeicherte Abfrage		X		Der Name der gespeicherten Abfrage, die von diesem KPI aufgerufen wird. Der Wert kann bearbeitet werden.
SQL-Abfrage			X	Der SQL-Code für die Abfrage. Der Wert kann bearbeitet werden.
Beschreibung	X	X	X	(Optional) Bietet eine ausführliche Beschreibung des KPI. Der Wert kann bearbeitet werden.

Abrufen von Ticket-Daten

Um Berichte über die Zeitdauer zu ermöglichen, über die die Tickets in den verschiedenen Verarbeitungsphasen (Verarbeitungsstatus) verbleiben, können Sie den KPI-Daemon so konfigurieren, dass CA SDM-Ticketdaten abgerufen werden, sobald ein Ticket geöffnet oder geschlossen wird oder einer der folgenden Feldwerte geändert wird:

- Aktiv
- Verantwortlicher
- Bereich oder Kategorie
- Gruppe
- Impact
- Organisation
- Priorität
- Ursache
- Status

■ Diensttyp

Um die Ticketwiedergewinnung zu aktivieren, installieren Sie die Option "KPI-Ticket-Datentabelle", die im Ordner "Optionsmanager-KPI" verfügbar ist.

Die Auflistung der Daten von neuen und aktualisierten Tickets ist aktiviert. Die Ticket-Daten werden in die Datenbanktabelle "usp_kpi_ticket_data" geschrieben und stehen zum Erstellen von webbasierten Berichten zur Verfügung.

Hinweis: Weitere Anweisungen finden Sie in der *Online-Hilfe*.

Die folgenden Erwägungen gelten für die Ticketwiedergewinnung:

- Es kann bis zu 30 Minuten dauern, bis KPI-Daemon die Datentabelle usp_kpi_ticket_data mit den Ticket-Informationen auffüllt.
- Das Feld "support_lev" ermöglicht die Verfolgung der Servicetyp-Verarbeitung, wenn die Option "classic_sla_processing" installiert ist. Die Option classic_sla_processing ermöglicht den Prozess "Servicetyp" ab CA SDM-Version 6.0 und früher.
- Hinweis: Das Aktivieren dieser Funktion kann dazu führen, dass die CA SDM-Leistung sinkt.

Weitere Informationen:

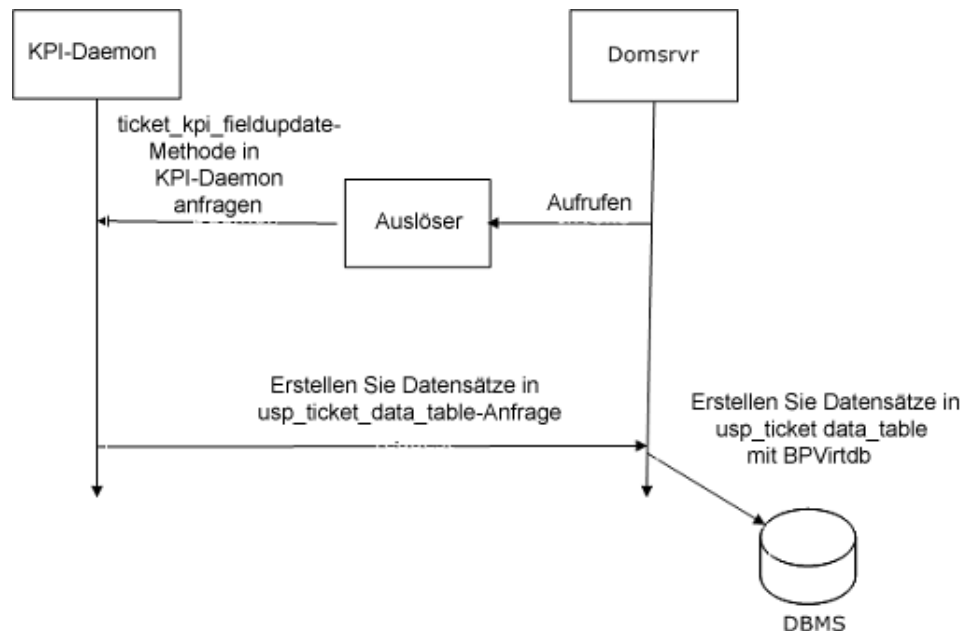
[Datei "NX.env"](#) (siehe Seite 923)

KPI-Ticket-Datenfluss

Die Funktion "KPI Ticket-Datentabelle" arbeitet an einem Triggermechanismus. Wenn die Option `kpi_ticket_data_table` installiert wird, beginnt der KPI-Daemon, CA SDM-Ticket-Objekte zu überwachen, um die folgenden Ereignisse zu verfolgen:

- Öffnen eines neuen Tickets
- Überprüfen von Änderungen zu einem oder mehr überwachten Feldern
- Schließen des Tickets

Wenn eines dieser Ereignisse auftritt, wird ein `POST_CI`-Trigger ausgelöst. Der Trigger sendet eine `BPMMessage` mit einer Triggerattributliste an den KPI-Daemon und fügt die zurückgegebenen Daten der Liste `"usp_kpi_ticket_data"` hinzu, wie im folgenden Datenflussdiagramm angezeigt.



Datensatztypen in KPI-Ticket-Datentabellen

Es gibt fünf Vorgangstypen in der Tabelle `usp_kpi_ticket_data`:

- INIT (0)
- NO_INIT_REC (1)
- REOPEN (2)
- UPDATE (3)
- CLOSE (4)

Der Typwert (in Klammern angezeigter Ganzzahlenwert) wird im Vorgangsfeld gespeichert. Der Wert von "end_time" des vorherigen Datensatzes wird im Feld "prev_time" gespeichert. Das Feld "ktd_duration" speichert die Dauer, die als "end_time" abzüglich "prev_time" berechnet wird. Der bisherige Datensatz wird in den folgenden Regeln definiert:

1. Der INIT-Datensatz zeigt, dass ein Ticket erstellt wurde.
2. Bei jeder Aktualisierung eines Tickets wird ein UPDATE-Datensatz erstellt. Er ruft die prev_time von einem älteren UPDATE-Datensatz für das gleiche Ticket ab, falls ein älterer UPDATE-Datensatz vorhanden ist. Falls nicht, wird prev_time vom Datensatz INIT, NO_INIT_REC oder REOPEN abgerufen, je nachdem, welcher Datensatz einen end_time-Wert mit dem zeitlich kürzesten Abstand zum UPDATE-Datensatz aufweist.
3. Der Datensatz CLOSE ist derselbe wie UPDATE.
4. Wird ein Ticket erneut geöffnet, wird ein REOPEN-Datensatz erstellt, um den Wert für das Feld "Aktiv" anzuzeigen. Der Datensatz REOPEN ruft die "prev_time" von einem älteren CLOSE-Datensatz für dasselbe Feld "Aktiv" ab.
5. Falls ein Ticket vor dem Aktivieren der Option "Optionsmanager" erstellt wurde, enthält es gegebenenfalls Datensätze für Aktualisierungen, jedoch ohne einen INIT-Datensatz. Das Programm erstellt in diesem Fall einen NO_INIT_REC-Datensatz und ruft die prev_time vom ersten Nicht-INIT-Datensatz ab, den es ermittelt.

Hinweis: Vollständige Erläuterungen zu den Tabellenfeldern finden Sie im *Technischen Referenzhandbuch*.

Fehlerbehebung

Sie können Probleme analysieren, die bei der KPI-Nutzung auftreten können.

Überprüfen Sie, ob der KPI-Daemon läuft.

Vergewissern Sie sich, dass der KPI-Daemon läuft, indem Sie das pdm_status-Befehlszeilen-Hilfsprogramm folgendermaßen ausführen:

```
pdm_status
```

Prüfen Sie die Ausgabe auf Folgendes:

```
KPI Daemon myserver Running myserver 3568 Wed Feb 06 07:23:53
```

Datei "NX.env"

Prüfen Sie die Datei \$NX_ROOT/NX.env, um sicherzustellen, dass die grundlegende KPI-Konfiguration richtig ist.

Wenn Sie die Option KPI-Ticket-Datentabelle installiert haben, hat die Datei "NX.env" folgenden Inhalt:

```
#####
# NX_KPI_TICKET_DATA_TABLE
# Enable the collection of changed fields from ticket objects (Aktivieren Sie das
# Sammeln geänderter Felder aus Ticket-Objekten)
# (like Requests, Issues and Change Orders) to write record entries (um
# Datensatzeinträge, wie z. B. Anfragen, Issues und Changes,)
# into the usp_kpi_ticket_data table. (in die Tabelle "sp_kpi_ticket_data" zu
# schreiben.)
#####
@NX_KPI_TICKET_DATA_TABLE=Yes
```

```
#####
# NX_KPI_FUZZ_TIME
# Specifies a tolerable delay for each KPI within which kpi_daemon (Gibt eine zulässige
# Verzögerung für jeden KPI an, wobei "kpi_daemon")
# sends a request to retrieve KPI data when this KPI's refresh time (eine Anfrage für
# das Abrufen von KPI-Daten sendet, wenn die Aktualisierungszeit dieses KPIs)
# is timeout (abgelaufen ist.)
#####
@NX_KPI_FUZZ_TIME=20
```

Hinweis: Der Standardwert von @NX_KPI_FUZZ_TIME ist 20 Sekunden. Sie können diesen Wert im Bereich von 0 und 40 Sekunden verändern. Wenn Sie den Wert höher als 40 setzen, werden 40 Sekunden verwendet.

```
#####
# NX_ALWAYS_KEEP_KPI_VERSIONS
# The keep_version attribute in Kpi table is displayed on the KPI (Das Attribut
# "keep_version" in der KPI-Tabelle wird für das Formular)
# Detail Edit form as a checkbox. ("Bearbeiten von KPI-Details" als Kontrollkästchen
# angezeigt.) The NX_ALWAYS_KEEP_KPI_VERSIONS (Die Option
# NX_ALWAYS_KEEP_KPI_VERSIONS)
# option specifies that checkbox is read-only and is always checked. (gibt an, dass
# dieses Kontrollkästchen schreibgeschützt ist, und diese Option ist stets aktiviert.)
#####
@NX_ALWAYS_KEEP_KPI_VERSIONS=Yes
```

Einschalten des KPI-Daemon-Tracing

Mit dem Dienstprogramm "pdm_logstat" können Sie die Tracing-Protokollierung einschalten, um die Verwendung von KPI innerhalb von CA SDM zu überwachen.

Führen Sie zur Aktivierung des KPI-Daemon-Tracing den folgenden Befehl aus:

```
pdm_logstat -f cache_table_mgr.c VERBOSE
```

Führen Sie zur Deaktivierung des KPI-Daemon-Tracing den folgenden Befehl aus:

```
pdm_logstat -f cache_table_mgr.c
```

Überprüfen Sie die Datei "stdlog.0" auf Einträge in Bezug auf KPI-Daemon-Aktivität.

Das folgende Beispiel zeigt normale KPI-Daemon-Verbindungen mit dem Hauptrechner und dem domsrvr:

```
02/06 05:42:14.58 garbo-2k3-bb kpi_daemon 2432 SIGNIFICANT kpi_daemon.c 117 KPIDaemon betriebsbereit!  
02/06 05:42:14.80 garbo-2k3-bb domsrvr 792 SIGNIFICANT connmgr.c 2314 Verbindungs-Client  
kpi_daemon:garbo-2k3-bb  
02/06 05:42:14.81 garbo-2k3-bb kpi_daemon 2432 SIGNIFICANT main.c 220 KPI-Daemon verbunden mit domsrvr
```

Das folgende Beispiel zeigt einen Fehler in einem webSessionCT genannten KPI an:

```
01/16 13:24:46.74 jed web:local 2152 ERROR sys_kpi.c 96 Ungültiger KPI-Metriktyp: 1382180215  
(KPI-Name:webSessionCT)
```

Die folgenden Beispiele zeigen KPI-Daemon-Aktivität:

```
02/06 07:23:50.47 garbo-2k3-bb kpi_daemon 3568 TRACE cache_table_mgr.c 427 Cache-Tabellenmanager  
erstellte Kpi_Obj (KPI dob record_id:9003) (KPI-Typ:2)  
02/06 07:23:50.53 garbo-2k3-bb kpi_daemon 3568 TRACE cache_table_mgr.c 427 Cache-Tabellenmanager  
erstellte Kpi_Obj (KPI dob record_id:9103) (KPI-Typ:1)
```

Hinweis: Information über KPI-Typen finden Sie unter [Datensatztypen in KPI-Ticket-Datentabellen](#) (siehe Seite 921).

Ad-hoc-Berichte

Ad-hoc-Berichte werden in InfoView mit Hilfe von Web Intelligence entwickelt. Sie können Ad-hoc-Berichte erstellen.

Hinweis: Weitere Informationen zur Ad-hoc-Berichterstellung finden Sie in der Dokumentation zu BusinessObjects Enterprise. Klicken Sie auf das Hilfesymbol in InfoView, um auf die Dokumentation zuzugreifen.

Web Intelligence-Schnittstelle

In InfoView bietet Web Intelligence ein Tool zur Ad-hoc-Berichterstellung, das für Benutzer gedacht ist, die problemlos einfache Berichte erstellen möchten, ohne Abfragen zu schreiben. Web Intelligence verwendet vordefinierte Berichtsmodelle und -vorlagen zur Verwaltung von Datenverbindungen, Abfragen und Datenbeziehungen. Zum Erstellen von tabellarischen oder Matrixberichten reicht es aus, Datenfelder per Drag-and-Drop auf eine Vorlage zu ziehen. Sie können alle InfoView-Funktionen verwenden, die im *InfoView-Anwenderhandbuch* beschrieben werden.

Ein Web Intelligence-Dokument verweist zum Erstellen von Berichten auf ein BusinessObjects-Objekt namens Universe. Neue Berichte werden in BusinessObjects Universes erstellt. CA Business Intelligence stellt das CA SDMUniverse mit dem Produkt zur Verfügung.

Funktionsweise der Ad-hoc-Berichterstellung

Die Ad-hoc-Berichterstellung funktioniert folgendermaßen:

1. Sie beginnen den Ad-hoc-Bericht, indem Sie zunächst in InfoView das CA SDM-Universum auswählen.
2. Das Universe ist der CA SDM-Datenbank zugeordnet, die Unternehmensinformationen enthält. Wenn Sie eine Verbindung zu einem Universe herstellen, startet Web Intelligence automatisch den Dokumenteditor, der auf der Seite "Web Intelligence-Dokument - Voreinstellungen" in InfoView ausgewählt wird.

Hinweis: Weitere Informationen zum Definieren von Voreinstellungen finden Sie im *Benutzerhandbuch zu BusinessObjects InfoView*.

3. Bei der Verwendung des Universums erstellen Sie Abfragen, um Daten zur Verwendung in einem Bericht abzurufen. Diese Daten werden aus Objekten erfasst, die in Ordner mit der Bezeichnung "Klasse" gruppiert sind. Jede Klasse kann eine oder mehrere Unterklassen enthalten. Unterklassen enthalten Objekte, die eine weitere Unterkategorie der Objekte in der oberen Ebene der Klasse darstellen. Klassen und Objekte werden in einer Baumstruktur (Hierarchie) auf der Registerkarte "Daten" angezeigt.

Hinweis: Weitere Anweisungen zum Erstellen von Abfragen für Web Intelligence-Dokumente finden Sie in der Dokumentation zu BusinessObjects Enterprise.

4. Erstellen Sie eine Abfrage, indem Sie dem Fenster "Result Objects" (Ergebnisobjekte) die erforderlichen Objekte hinzufügen, und definieren Sie die Eigenschaften des Abfragefilters. Anschließend können Sie die Abfrage ausführen. Beim Ausführen einer Abfrage weist das Universum die Datenbank an, die Daten abzurufen, die den Anfragen der einzelnen Objekte in der Abfrage entsprechen. Sie führen eine Abfrage aus, indem Sie in der Symbolleiste auf "Run Query" (Abfrage ausführen) klicken.

Wichtig! Wenn Sie Objekte für Ihre Abfrage auswählen, verwenden Sie immer nur Objekte, Messwerte und Filter aus einer einzigen Universe-Basisklasse und den zugehörigen Unterklassen. Wenn Sie Objekte, Messungen und Filter aus mehreren Universumsbasisklassen in eine Abfrage aufnehmen, sind möglicherweise unerwartete Ergebnisse und eine unzureichende Ausführungsleistung die Folge.

Ad-hoc-Beispielberichte

Nutzen Sie Web Intelligence und die Beispielabfragen, um Ad-hoc-Berichte mit dem CA SDM-Standard-Universum zu erstellen. Wenn Sie einen Bericht erstellen, achten Sie darauf, in regelmäßigen Abständen zu speichern. Wenn eine Zeitüberschreitung der Web Intelligence-Verbindungssitzung eintritt, verlieren Sie sämtliche Änderungen am Bericht seit dem letzten Speichern.

Hinweis: Informationen zum Ändern des Sitzungszeitlimitwerts finden Sie im *Implementierungshandbuch*.

Beispiel: Anzeigen aller offenen Requests mit Priorität 1 und 2 für alle Anwender

In diesem Beispiel legen Sie Eingabewerte fest, die vor der Erstellung des Berichts zusätzliche Daten erfassen.

Beispiel: Anzeigen aller offenen Requests mit Priorität 1 und 2 für alle Anwender

1. Klicken Sie in der Menüleiste auf "Neu", "Web Intelligence-Dokument".
Die Seite "Neues Web Intelligence-Dokument" wird angezeigt.
2. Wählen Sie in der Spalte "Universe" das CA SDM Universe aus.
Das Web Intelligence-Dokument wird zusammen mit den Universe-Informationen im linken Bereich angezeigt.
Hinweis: Schließen Sie den Ordner "Angehängter Servicetyp" im linken Fensterbereich, um einfacher navigieren zu können.
3. Erweitern Sie den Ordner "Request", "Request - Detail" im linken Bereich. Benutzen Sie die Bildlaufleiste, um Ordner zu lokalisieren.

4. Wählen Sie jedes der folgenden Objekte aus, und übertragen Sie diese mit Drag-and-Drop aus dem linken in den rechten Fensterbereich unter "Ergebnisobjekte".
 - Übersicht
 - Prioritätssymbol
 - Customer Combo Name (Kunden-Kombinationsname)
5. Wählen Sie jedes der folgenden Objekte aus, und übertragen Sie diese mit Drag-and-Drop in den rechten unteren Fensterbereich unter "Abfragefilter". Schließen Sie die Seite "Request - Detail", wenn Sie fertig sind.
 - Statussymbol
 - Prioritätssymbol
6. Erweitern Sie den Ordner "Request-Filter", und übertragen Sie dann den Filter "Aktiv" mit Drag-and-Drop in den rechten unteren Fensterbereich unter "Abfragefilter".
7. Klicken Sie im Fenster "Abfragefilter" auf den Listenpfeil im Statussymbol-Filter. Wählen Sie dann den Operator "Not Equal to" (Ist nicht gleich) aus.
8. Wählen Sie aus der Liste im Operandentypmenü die Option "Value(s)" (Wert(e)) aus.

Das Dialogfeld mit der Liste von Werten wird angezeigt.
9. Wählen Sie in der Statussymbol-Liste die Option "Offen" aus, klicken Sie dann auf den grünen Pfeil.

Der ausgewählte Wert wird im Feld "Value(s) Selected" (Ausgewählte Werte) angezeigt.
10. Klicken Sie auf "OK".
11. Klicken Sie im Fenster "Abfragefilter" im Prioritätssymbol auf das Dropdownmenü der Liste, und wählen Sie den Operator "In List" (In Liste) aus.
12. Wählen Sie in der Prioritätssymbolliste gleichzeitig "1" und "2" aus. Klicken Sie dann auf den grünen Pfeil.

Die Werte "1" und "2" werden in dem Feld "Value(s) Selected" (Ausgewählte Werte) angezeigt.
13. Klicken Sie auf "OK".
14. Klicken Sie auf "Abfrage ausführen" in der Symbolleiste, um den Bericht zu generieren.

Hinweis: Da der Kunden-Kombinations-Name mit Anwender-ID-Schnellfilter die Funktion "Aufforderung" verwendet, wird das Dialogfeld "Prompts" (Aufforderungen) angezeigt. Dieses Dialogfeld ermöglicht Ihnen, zusätzliche Daten zu erfassen, bevor der Bericht generiert wird.

15. Wählen Sie im Fenster "Prompts" (Aufforderungen) die erste Option, "ALL" (Alle).
Klicken Sie dann auf die grüne Pfeilschaltfläche.

Alle Anwendernamen werden in der Liste "Select Customer" (Kunden auswählen) angezeigt.
16. Klicken Sie auf "Abfrage ausführen", um den Bericht zu generieren.

Der Bericht wird in einem neuen Fenster angezeigt.
17. Doppelklicken Sie auf den Berichtstitel und geben Sie "Offene Requests mit Priorität 1 & 2" für alle Anwender in das Textfeld ein. Die Schriftgröße können Sie in 16 oder andere Größen ändern.
18. Um andere Aspekte des Berichts zu ändern, klicken Sie auf die Registerkarte "Eigenschaften".
19. Zum zusätzlichen Anordnen der Daten nach dem Nachnamen des Kunden klicken Sie mit der rechten Maustaste in der Spalte "Nachname des Kunden" auf eine beliebige Datenzelle, und wählen Sie "Set as Section" (Als Abschnitt festlegen) aus.
20. Klicken Sie auf "Speichern", und geben Sie mit der Option "Speichern unter" einen Speicherort an.

Beispiel: Anzeigen aller offenen Requests, deren Status nicht "In Bearbeitung" ist.

In diesem Beispiel stellen Sie die Berichterstellungsfunktion "Count" (Zähler) so ein, dass sie die Gesamtanzahl der offenen Anfragen ausgibt.

Beispiel: Anzeigen aller offenen Requests, deren Bearbeitungsstatus nicht "In Bearbeitung" ist.

1. Klicken Sie in der Menüleiste auf "Neu", "Web Intelligence-Dokument".

Die Seite "Neues Web Intelligence-Dokument" wird angezeigt.
2. Wählen Sie in der Spalte "Universe" das CA SDM Universe aus.

Das Web Intelligence-Dokument wird zusammen mit den Universe-Informationen im linken Bereich angezeigt.

Hinweis: Schließen Sie den Ordner "Angehängter Servicetyp" im linken Fensterbereich, um einfacher navigieren zu können.
3. Erweitern Sie den Ordner "Request", "Request - Detail" im linken Bereich.
(Benutzen Sie die Bildlaufleiste, um Ordner zu durchsuchen.)

4. Wählen Sie jedes der folgenden Objekte aus, und übertragen Sie diese mit Drag-and-Drop aus dem linken in den rechten Fensterbereich unter "Ergebnisobjekte".
 - Statussymbol
 - Ref.-Nr.
 - Übersicht
5. Wählen Sie das Statussymbol-Objekt aus, und übertragen Sie es mit Drag-and-Drop in den rechten unteren Fensterbereich unter "Abfragefilter". Schließen Sie den Ordner "Request - Detail".
6. Erweitern Sie den Ordner "Request-Filter", und übertragen Sie dann den Filter "Aktiv" mit Drag-and-Drop in den rechten unteren Fensterbereich unter "Abfragefilter".
7. Klicken Sie im Fenster "Abfragefilter" auf den Listenpfeil im Statussymbol-Objekt. Wählen Sie dann den Operator "Not Equal to" (Ist nicht gleich) aus.
8. Wählen Sie im Operandentypmenü den Status "In Bearbeitung" aus.
9. Klicken Sie in der Hauptsymbolleiste auf "Edit Report" (Bericht bearbeiten).
Der Bericht-Viewer wird angezeigt.
10. Wählen Sie im Bericht die Spalte "Ref.-Nr." aus. Dadurch wird in der Berichterstellungs-Symbolleiste der Befehl "Insert Sum" (Summe einfügen) aktiviert.
11. Klicken Sie auf den Befehl "Insert Sum" (Summe einfügen), und wählen Sie dann aus dem Menü die Option "Count" (Zähler).
12. Klicken Sie im Bericht mit der rechten Maustaste auf die Zelle "=[Status Symbol]", und wählen Sie dann im Kontextmenü die Option "Set as Section" aus.
13. Klicken Sie in der Hauptsymbolleiste auf "Refresh Data" (Daten aktualisieren), um den Bericht auszuführen.
14. Klicken Sie auf "Speichern".
Der Bericht zeigt die Gesamtzahl der Requests an, deren Status *nicht* "In Bearbeitung" ist.

Beispiel: Anzeigen aller in den letzten 30 Tagen geschlossenen Requests für Anwender, deren Nachname mit "C" beginnt.

In diesem Beispiel geben Sie die Eingabewerte für das Schließungsdatum und den Nachnamen des Kunden an. Basierend auf diesen Werten werden alle geschlossenen Requests zurückgegeben.

Beispiel: Anzeigen aller in den letzten 30 Tagen geschlossenen Requests für Anwender, deren Nachname mit "C" beginnt.

1. Klicken Sie in der Menüleiste auf "Neu", "Web Intelligence-Dokument".
Die Seite "Neues Web Intelligence-Dokument" wird angezeigt.
2. Wählen Sie in der Spalte "Universe" das CA SDM Universe aus.
Das Web Intelligence-Dokument wird zusammen mit den Universe-Informationen im linken Bereich angezeigt.
Hinweis: Schließen Sie den Ordner "Angehängter Servicetyp" im linken Fensterbereich, um einfacher navigieren zu können.
3. Suchen und erweitern Sie den Ordner "Request", "Request - Detail" im linken Bereich. Benutzen Sie die Bildlaufleiste, um Ordner zu durchsuchen.
4. Wählen Sie jedes der folgenden Objekte aus, und übertragen Sie diese mit Drag-and-Drop aus dem linken in den rechten Fensterbereich unter "Ergebnisobjekte".
 - Ref.-Nr.
 - Schließdatum
 - Nachname des Kunden
 - Übersicht
5. Wählen Sie jedes der folgenden Objekte aus und übertragen Sie diese mit Drag-and-Drop in den rechten unteren Fensterbereich unter "Abfragefilter".
 - Statussymbol
 - Schließdatum
 - Nachname des Kunden
6. Klicken Sie im Statussymbolfilter auf den Listenpfeil und wählen Sie "Value(s)" (Wert(e)) aus dem Operandentypmenü aus.
Das Dialogfeld mit der Liste von Werten wird angezeigt.
7. Wählen Sie die folgenden Werte in der Statussymbol-Liste aus:
 - Geschlossen
 - Geschlossen – Ungelöst

- Schließung angefordert
- Problem geschlossen
- Problem behoben
- Gelöst

8. Klicken Sie auf den grünen Pfeil.

Die Werte werden im Feld "Value(s) Selected" (Ausgewählte Werte) angezeigt.

9. Klicken Sie auf "OK".

10. Klicken Sie im Fenster "Abfragefilter" auf den Listenpfeil im Objekt "Schließdatum", und wählen Sie den Operator "Between" (Zwischen).

11. Klicken Sie auf den Listenpfeil, und wählen Sie aus dem ersten und zweiten Operandentypmenü die Option "Aufforderung".

12. Klicken Sie im Objekt "Nachname des Kunden" auf den Listenpfeil, und wählen Sie den Operator "Matches pattern" (Stimmt mit Muster überein) aus.

13. Klicken Sie auf den Listenpfeil und wählen Sie im Operandentypmenü die Option "Aufforderung".

14. Klicken Sie auf das Symbol zur Anforderung der Eigenschaften, das neben dem Listenpfeil angezeigt wird.

Das Dialogfeld "Aufforderung" wird angezeigt.

15. Geben Sie im Textfeld ein Muster für den Nachnamen des Kunden ein.

16. Klicken Sie auf "OK".

17. Klicken Sie auf "Abfrage ausführen" in der Symbolleiste, um den Bericht zu generieren.

Hinweis: Aktivieren Sie von den Objekten "Schließdatum" und "Nachname des Kunden" aus die Aufforderungsfunktion. Daraufhin wird das Dialogfeld "Aufforderung" angezeigt. Dieses Dialogfeld ermöglicht Ihnen, zusätzliche Daten zu erfassen, bevor der Bericht generiert wird.

18. Wählen Sie im Aufforderungsfenster die Eingabewerte für die einzelnen Aufforderungen wie folgt aus:

- Enter Close Date (Start) (Schließdatum eingeben, Start): Geben Sie ein Datum ein, das 30 Tage vor dem aktuellen Datum liegt.
- Enter Close Date (End) (Schließdatum eingeben, Ende): Geben Sie das aktuelle Datum ein.
- Enter a pattern for Customer Last Name (Geben Sie ein Muster für den Nachnamen des Kunden ein): C%.

19. Klicken Sie auf "Abfrage ausführen", um den Bericht zu generieren.

Der Bericht wird in einem neuen Fenster angezeigt.

20. Doppelklicken Sie auf den Berichtstitel und geben Sie "Anzeigen aller in den letzten 30 Tagen geschlossenen Requests für Anwender, deren Nachname mit "C" beginnt" in das Textfeld ein. Die Schriftgröße können Sie in 16 oder andere Größen ändern.
21. Um andere Aspekte des Berichts zu ändern, klicken Sie auf die Registerkarte "Eigenschaften".
22. Klicken Sie auf "Speichern", und geben Sie mit der Option "Speichern unter" einen Speicherort an.

Dashboard-Berichte

Sie können Dashboard-Berichte verwenden, um tägliche Vorgänge für alle CA SDM-Tickets (Request/Incident/Problem, Change oder Issue), Knowledge Management, Support-Automatisierung und CMDB im BusinessObjects InfoView zu überwachen. Jeder Bericht enthält Analysedaten über Mitarbeiter, die bei der Arbeit mit aktiven Tickets beste Leistungen erbringen. So können Sie den Fortschritt überwachen.

Mit den Dashboard-Berichten können Sie folgendes tun:

- Zusammenfassungen und Detailinformationen über aktive Tickets nach Priorität, Analyst, Kategorie oder Gruppe anzeigen lassen.
- Stellen Sie fest, wie viele Tickets innerhalb eines bestimmten Zeitrahmens gelöst wurden und vieles mehr.
- Sie können Berichte in anderen Formaten wie .xls und .pdf bearbeiten, nachverfolgen und speichern.

Sie können mit einzelnen vordefinierten Dashboard-Berichten arbeiten oder anhand von unternehmensweiten Dashboards alle täglichen Vorgänge von CA SDM in einer einzigen Ansicht anzeigen. Über das Unternehmens-Dashboard gibt Ihnen wichtige Informationen über tägliche Vorgänge für alle Ticket-Typen (Request/Incident/Problem, Change oder Request) nach Priorität, Analyst, Kategorie oder Gruppe.

Hinweis: Wenn Sie mit Dashboard-Berichten arbeiten, können Sie die InfoView-Funktionen verwenden, die im Abschnitt "Working with Dashboard and Analytics" im *BusinessObjects InfoView-Anwenderhandbuch* beschrieben sind. Klicken Sie auf das Hilfesymbol in InfoView, um auf das Anwenderhandbuch zuzugreifen.

Anzeigen von Dashboards und Berichten in InfoView

Das Administratorkonto kann sich bei BusinessObjects InfoView anmelden und die Berichte anzeigen. Welche Ordner und Berichte Anwender in InfoView sehen, hängt von dem Konto ab, über das sie sich anmelden, und von den Rechten, die ihnen vom Administrator gewährt wurden.

So überprüfen Sie Dashboard-Berichte in InfoView

1. Melden Sie sich bei CA SDM an.
2. Klicken Sie auf der Registerkarte "Berichte" auf die Schaltfläche "InfoView".
InfoView wird in Ihrem Webbrowser angezeigt.
3. Wählen Sie auf der InfoView-Symbolleiste "Liste der Dokumente" aus.
Im Navigationsbereich werden Ordner und Objekte angezeigt.
4. Wählen Sie "Öffentliche Ordner", CA-Berichte, CA SDM-Dashboards" aus.
Die folgenden Ordner werden angezeigt: Change, Incident, Issue, Problem, Request, Konfiguration und Knowledge.
5. Wählen Sie den entsprechenden Bericht aus.
Der Bericht wird im rechten Fensterbereich angezeigt.
6. Doppelklicken Sie auf den Titel, um einen Bericht anzuzeigen.
Der Bericht kann nun angesehen werden.

Schreiben von CA Business Intelligence-Berichten

Sie können CA Business Intelligence-Berichte für CA SDM schreiben.

Weitere Informationen:

[CA SDM-ODBC-Treiber](#) (siehe Seite 933)

[Schreiben von SQL für BusinessObjects-Berichte](#) (siehe Seite 934)

[PDM-Funktionen](#) (siehe Seite 935)

[Attributaliasnamen](#) (siehe Seite 938)

[pdm isql - interaktives SQL](#) (siehe Seite 938)

CA SDM-ODBC-Treiber

Business Objects-Berichtsanwendungen (Crystal Reports und Web Intelligence) greifen über einen ODBC-Treiber auf Daten zu. Dieser ist direkt mit der Objekt-Engine (domsrvr) von CA SDM verbunden.

Dies bietet verschiedene Vorteile:

- SELECT-Anweisungen, die von BusinessObjects-Berichten verwendet werden, referenzieren Objekte und Attribute mit Hilfe ihrer CA SDM-Namen (oder ihrer Majic-Namen). Eine SELECT-Anweisung für einen Bericht zu Kontakten könnte z. B. so geschrieben werden:
`SELECT combo_name FROM cnt WHERE last_name LIKE 'smith%'`
- Der CA SDM-ODBC-Treiber ordnet Attribute wie "combo_name" und Objekte wie "cnt" ihren entsprechenden DBMS-Namen zu.
- Alle CA SDM-Sicherheitseinstellungen, einschließlich derjenigen zu Datenpartition und Einschränkungen der Mandantenfähigkeit, werden automatisch auf Berichte angewendet. Alle Verbindungen zwischen BusinessObjects und CA SDM sind einem CA SDM-Kontakt zugeordnet und ODBC ändert eingegebene SELECT-Anweisungen so, dass die zur Endbenutzerberichtsrolle gehörenden Sicherheitseinschränkungen erzwungen werden. BusinessObjects stellt keine direkte Verbindung zur Datenbank her.
- Die Funktion des CA SDM-Attributalias "vereinfacht" die CA SDM-Datenbank. Attribut-Aliasnamen sind zusätzliche Attribute in CA SDM-Objekten. Damit kann eine Abfrage Attribute in verknüpften Tabellen ohne explizite Verknüpfung referenzieren, so dass die Basistabelle wie eine Berichtsansicht verwendet werden kann.
- Der CA SDM-ODBC-Treiber unterstützt Datumsliteralen in Abfragen und überträgt automatisch Werte im internen CA SDM-Datumsformat in ein standardmäßiges DBMS-Datum.

Wichtig! Der CA SDM-ODBC-Treiber wird nur für BusinessObjects-Berichte unterstützt (Crystal und Web Intelligence). CA SDM bietet keinen eigenständigen ODBC-Client. Die Verwendung des ODBC-Treibers mit Anwendungen außer BusinessObjects wird nicht empfohlen.

Schreiben von SQL für BusinessObjects-Berichte

Alle von BusinessObjects-Berichten verwendeten SQL-Anweisungen werden vom CA SDM-ODBC-Treiber verarbeitet. Der ODBC-Treiber unterstützt SELECT-Anweisungen des Standards SQL 92 mit den folgenden Änderungen und Erweiterungen:

- Anstelle von DBMS-Tabellennamen werden CA SDM-Objektnamen und anstelle von DBMS-Spaltennamen werden CA SDM-Attributnamen verwendet.
- Ein CA SDM-Attributaliasname kann an einer beliebigen Stelle in der Abfrage verwendet werden, an der ein Spaltenname gültig ist. Der ODBC-Treiber ersetzt die Attributaliasreferenz durch eine oder mehrere Verknüpfungen.

Hinweis: Weitere Informationen dazu finden Sie unter [Attributaliasnamen](#) (siehe Seite 938).

- DERIVED-Attribute von CA SDM (z. B. "combo_name") können nur in der Auswahlliste verwendet werden. Sie werden in keinem anderen Teil der Abfrage unterstützt, einschließlich der WHERE-Klausel.

Hinweis: Viele "Combo Name With Userid"-Objekte wurden im Universum bereitgestellt, z. B. das Objekt "Customer Combo Name With Userid", das als Filter im Ad-hoc-Beispielbericht im *Administrationshandbuch* verwendet wurde. Diese Objekte ermöglichen es, dass "Combo Name" als Filteranforderung in Ad-hoc-Abfragen mit Web Intelligence verwendet werden kann, um die Einschränkung der Einbeziehung von "Combo Name" in die WHERE-Klausel zu überwinden. Sie zeigen "Combo Name" und "Userid" in der Filteranforderung an, verwenden in der sich ergebenden SQL-Abfrage jedoch nur die ausgewählten "Userids".

- Abfragen können Datumsliteralen in einem der folgenden Formate enthalten:
d'yyyy-mm-dd hh:mm:ss xm' (wobei xm entweder am oder pm ist)
ts'yyyy-mm-dd hh:mm:ss'

Diese Literalen können an einer beliebigen Stelle in der Abfrage verwendet werden. Der ODBC-Treiber konvertiert sie automatisch in das CA SDM-interne Datumsformat (Anzahl der Sekunden ab 1. Januar 1970, Mitternacht).

PDM-Funktionen

Zur Erleichterung der Arbeit mit speziellen CA SDM-Funktionen und -Datentypen erweitert der ODBC-Treiber die SQL-Unterstützung auf eine Reihe zusätzlicher Abfragefunktionen. Alle vom Treiber unterstützten Funktionen beginnen mit der Zeichenfolge "Pdm" und werden als PDM-Funktionen bezeichnet. Eine Beschreibung finden Sie in der folgenden Tabelle:

PDM-Funktionen	Beschreibung
PdmAddDays([date,] count)	Bei Verwendung mit einem Argument wird die Anzahl der Tage im Argument zum heutigen Datum addiert, und das Ergebnis wird zurückgegeben. Bei Verwendung mit zwei Argumenten wird die Anzahl der Tage im zweiten Argument zum Wert der Datumspalte addiert, die im ersten Argument angegeben wurde. Das Ergebnis wird zurückgegeben. Diese Funktion kann an einer beliebigen Stelle in der Abfrage verwendet werden.
PdmAddMonths([date,] count)	Bei Verwendung mit einem Argument wird die Anzahl der Monate im Argument zum heutigen Datum addiert, und das Ergebnis wird zurückgegeben. Bei Verwendung mit zwei Argumenten wird die Anzahl der Monate im zweiten Argument zum Wert der Datumspalte addiert, die im ersten Argument angegeben wurde. Das Ergebnis wird zurückgegeben. Das Format mit einem Argument kann an einer beliebigen Stelle in der Abfrage verwendet werden. Das Format mit zwei Argumenten kann nur in der Auswahlliste verwendet werden.

PDM-Funktionen	Beschreibung
PdmDay([date])	Bei Verwendung ohne Argumente wird der aktuelle Tag als Ganzzahl zurückgegeben. Bei Verwendung mit einem Argument wird der Tag zurückgegeben, der mit dem Wert der Datumspalte verknüpft ist, die im Argument angegeben wurde. Das Format ohne Argumente kann an einer beliebigen Stelle in der Abfrage verwendet werden. Das Format mit einem Argument kann nur in der Auswahlliste verwendet werden.
PdmDownTime(slaName, workshift, startDate, endDate)	Berechnet die Ausfallzeiten zwischen zwei Daten unter dem angegebenen SLA und der Schicht. Diese Funktion kann nur in der Auswahlliste verwendet werden.
PdmMonth([date])	Bei Verwendung ohne Argumente wird der aktuelle Monat als Ganzzahl zwischen 1 und 12 zurückgegeben. Bei Verwendung mit einem Argument wird der Monat zurückgegeben, der mit dem Wert der Datumspalte verknüpft ist, die im Argument angegeben wurde. Das Format ohne Argumente kann an einer beliebigen Stelle in der Abfrage verwendet werden. Das Format mit einem Argument kann nur in der Auswahlliste verwendet werden.
PdmMonthName([date])	Bei Verwendung ohne Argument wird der lokalisierte Name des aktuellen Monats zurückgegeben ("Januar", "Februar", usw.). Bei Verwendung mit einem Argument wird der lokalisierte Name des Werts der Datumspalte zurückgegeben, die im Argument angegeben wurde. Das Format ohne Argumente kann an einer beliebigen Stelle in der Abfrage verwendet werden. Das Format mit einem Argument kann nur in der Auswahlliste verwendet werden.
PdmDay([date])	Bei Verwendung ohne Argumente wird der aktuelle Tag als Ganzzahl zurückgegeben. Bei Verwendung mit einem Argument wird der Tag zurückgegeben, der mit dem Wert der Datumspalte verknüpft ist, die im Argument angegeben wurde. Das Format ohne Argumente kann an einer beliebigen Stelle in der Abfrage verwendet werden. Das Format mit einem Argument kann nur in der Auswahlliste verwendet werden.
PdmSeconds(date)	Gibt den Wert der im Argument angegebenen Datumspalte im Rohformat als die Anzahl der Sekunden ab 1. Januar 1970, Mitternacht, zurück. Diese Funktion kann nur in der Auswahlliste verwendet werden. Das Argument ist erforderlich.
PdmString(column)	Gibt das Zeichenfolgenäquivalent des Werts der Spalte zurück, die im Argument angegeben wurde. Diese Funktion kann mit UUID-, Datums- oder Zeichenfolge-Spalten verwendet werden. Sie kann nur in der Auswahlliste verwendet werden.

PDM-Funktionen	Beschreibung
PdmToday()	PdmToday() [timeAdj [, day [, month [, year]]]]) Evaluiert zum heutigen Datum (in Sekunden vom 1.1.1970), eingestellt mit den folgenden Argumenten: timeAdj -1: Zeit auf Beginn des Tages (0:00:00) einstellen +1: Zeit auf Ende des Tages einstellen (23:59:59) Tag: negativ: Datum auf Anzahl der angegebenen Tage einstellen positiv: Tag auf den absoluten angegebenen Wert setzen (oder auf den letzten Tag des Monats, je nachdem welcher Wert niedriger ist) Monat: negativ: Datum auf Anzahl der angegebenen Monate einstellen positiv: Monat auf angegebenen Absolutwert einstellen (oder auf "Dezember (12)", je nachdem, welcher Wert niedriger ist) Jahr: negativ: Datum auf Anzahl der angegebenen Jahre einstellen positiv: Jahr auf den Absolutwert einstellen Anpassungen erfolgen in der Reihenfolge Jahr, Monat, Tag. Eine Null oder ausgelassene Argumente werden ignoriert.
PdmYear([date])	Bei Verwendung ohne Argumente wird das aktuelle Jahr als vierstellige Ganzzahl zurückgegeben. Bei Verwendung mit einem Argument wird das Jahr zurückgegeben, das mit dem Wert der Datumspalte verknüpft ist, die im Argument angegeben wurde. Das Format ohne Argumente kann an einer beliebigen Stelle in der Abfrage verwendet werden. Das Format mit einem Argument kann nur in der Auswahlliste verwendet werden.

Attributaliasnamen

Attributaliasnamen sind zusätzliche Attribute in CA SDM-Objekten, die Daten aus verknüpften Tabellen mit Hilfe von Majic-Syntax mit Punktverknüpfung referenzieren (wobei die Syntax "srelname.attrname" eine Referenz auf das Attribut "attrname" in der Tabelle ist, die vom Fremdschlüssel "srelname" referenziert wird). Mit CA SDM Version 12.9 wurden zahlreiche vordefinierte Attributaliasse bereitgestellt, deren Namen in der Regel identisch sind mit der entsprechenden Majic-Verknüpfung, wobei Unterstriche die Punkte ersetzen, die die Verknüpfung anzeigen. So könnte z. B. die folgende SELECT-Anweisung für einen Bericht verwendet werden, der Informationen zu den Zuständigen für die Anfrage aufführt:

```
SELECT ref_num, assignee_combo_name, assignee_organization_name  
FROM cr WHERE customer_last_name LIKE 'smith%'
```

Der CA SDM-ODBC-Treiber erstellt automatisch Verknüpfungen nach Bedarf für den Zugriff auf die Tabellen, die von Attributaliasnamen referenziert werden. Ein Benutzer in der CA SDM-Administratorrolle kann problemlos neue Attributaliasnamen online hinzufügen. Dies bietet die Möglichkeit, die einem Objekt entsprechende Ansicht spaltenweise zu erweitern.

Um auf die Tabelle "Attributalias" zuzugreifen, wählen Sie die Registerkarte "Administration" aus, und navigieren Sie zu "CA SDM" > "Codes" > "Attribut-Aliasnamen".

pdm_isql - interaktives SQL

Zusammen mit CA SDM wird das Befehlszeilendienstprogramm "pdm_isql" bereitgestellt, das die interaktive Eingabe von SQL SELECT-Anweisungen ermöglicht. In "pdm_isql" eingegebene SELECT-Anweisungen werden an den CA SDM-ODBC-Treiber gesendet, was es Ihnen ermöglicht, SQL SELECT-Anweisungen außerhalb von BusinessObjects zu testen.

So verwenden Sie "pdm_isql"

1. Stellen Sie sicher, dass "\$NX_ROOT/bin" im Pfad ist.
2. Geben Sie folgenden Befehl ein:

pdm_isql

3. Geben Sie an der `pdm_isql`-Aufforderung folgenden Befehl ein:

`connect username*password@casd_hostname`

(Wobei *username* und *password* für gültige CA SDM-Anmeldeinformationen stehen und der Hostname der Hostname eines CA SDM-Servers mit einer Web-Engine ist.)

4. Geben Sie SQL SELECT-Anweisungen ein, gefolgt von einem Semikolon.

Kapitel 21: Generieren von Berichten in USDK

Dieses Kapitel enthält folgende Themen:

- [Berichte erzeugen](#) (siehe Seite 941)
- [Datenbankansichten](#) (siehe Seite 941)
- [Einrichten von Berichtsmethoden](#) (siehe Seite 945)
- [Berichtsformatierung](#) (siehe Seite 945)
- [Ändern der Sortierreihenfolge der Spalten](#) (siehe Seite 946)
- [Zusammengefasste Berichte und Detailberichte](#) (siehe Seite 946)
- [Analyseberichte](#) (siehe Seite 947)

Berichte erzeugen

CA SDM bietet verschiedene integrierte Berichtsfunktionen und -optionen, darunter:

- Druckformulare für Assets und einzelne Changes, Issues, Incidents, Probleme und vieles mehr.
- Generieren von Übersichts- oder Detailberichten für Listen von Changes, Issues, Incidents, Problemen, Anfragen, Configuration Items.
- Generieren von Analyseberichten.

Hinweis: Weitere Informationen zur Verwendung von CA SDM-Berichten finden Sie in der *Online-Hilfe* unter "Erzeugen von Berichten". Neben der Verwendung der in CA SDM integrierten Berichtsfunktionen können Sie benutzerdefinierte Berichte auf der Basis der Tabellen und Ansichten in Ihrer CA SDM-Datenbank generieren. Weitere Informationen zu benutzerdefinierten Berichten finden Sie im *Implementierungshandbuch*.

Datenbankansichten

Die CA SDM-Datenbank ist ein Repository für die Daten, die Sie für den Betrieb Ihres Service Desks eingeben und nutzen. CA SDM bietet mehrere Datenbankansichten und ermöglicht Ihnen die Erstellung benutzerdefinierter Berichte der Datenbank.

Diese Ansichten unterteilen sich in zwei Arten:

- Standard
- Erweitert

Weitere Informationen:

[Beschreibungen der Felder in Ansichten](#) (siehe Seite 1213)

Grundlegende Ansichten

Die grundlegenden Ansichten basieren auf den Tabellen von CA SDM. Diese Ansichten enthalten Daten, wenn die Implementierung Anforderungen, Incidents, Probleme, Changes, Issues, Anlagen oder Kontakte/Gruppen nutzt.

Mithilfe der grundlegenden Ansichten können Sie zahlreiche Berichte entwerfen und erstellen, darunter:

- Detaillierte und zusammengefasste Listen offener Anfragen der Priorität 1, nach Anfragebereich sortiert
- Detaillierte und zusammengefasste Listen von Änderungsaufträgen der Ebene 1, die mehr als 24 Stunden offen sind, sortiert nach Priorität
- Anzahl der Issues, die länger als eine bestimmte Anzahl von Tagen offen sind, sortiert nach Priorität oder zugewiesene Gruppe oder Priorität und zugewiesene Gruppe

Die folgenden Hauptansichten sind verfügbar:

Name anzeigen	Beschreibung
View_Contact_Full	alle Kontakte, einschließlich Kontakttyp, Lokation, Organisationen und Servicetypen
View_Contact_to_Environment	alle Kontakte und ihre Umgebung (Assets)
View_Group	alle in der Datenbank definierte Gruppen
View_Group_To_Contact	alle Kontakte (einschließlich Managern) innerhalb ihrer Gruppenzuweisungen
View_Request	alle Anfragen, einschließlich Servicetypen, Schweregrad, Dringlichkeit, Kategorien, Assets, Auswirkungscode, Zuständige mit Namen, Kunden mit Namen, Gruppen, Status und Prioritäten
View_Act_Log	Informationen des Anfrageaktivitätsprotokolls, einschließlich Aktivitätstyp und Analystenname
View_Request_to_Act_Log	alle Anfragen mit ihren Aktivitätsprotokollen (diese Ansicht ist eine Verbindung von "View_Request" und "View_Act_Log")

Name anzeigen	Beschreibung
View_Request_to_Properties	Anfragen und ihre Eigenschaften (dies muss nicht alle Anforderungen einschließen, insbesondere, wenn ihnen keine Eigenschaften zugewiesen sind)
View_Change	alle Changes, einschließlich Status, Prioritäten, Kategorien, Organisationen, betroffene Endbenutzer mit Namen, Anforderer mit Namen, Zuständige mit Namen, Gruppen, Servicetypen und Auswirkungscodes
View_Change_Act_Log	Informationen des Aktivitätsprotokolls von Changes
View_Change_to_Change_Act_Log	alle Changes mit ihren Aktivitätsprotokollen (diese Ansicht ist eine Verbindung von "View_Change" und "View_Change_Act_Log")
View_Change_to_Properties	Changes und ihre Eigenschaften (dies muss nicht alle Changes einschließen, insbesondere, wenn ihnen keine Eigenschaften zugewiesen sind)
View_Change_to_Change_WF	Changes und ihre Workflow-Aufgaben (dies muss nicht alle Changes einschließen, insbesondere, wenn ihnen keine Workflow-Aufgaben zugewiesen sind)
View_Change_to_Assets	Changes und ihre Assets (dies muss nicht alle Changes einschließen, insbesondere, wenn ihnen keine Assets zugewiesen sind)
View_Change_to_Requests	Changes mit grundlegenden Informationen über zugewiesene Anfragen (diese Ansicht ist eine Verbindung der Tabellen "View_Change" und "Call_Request"; muss nicht alle Changes einschließen, insbesondere, wenn ihnen keine Anfragen zugewiesen sind)
View_Issue	Alle Issues, einschließlich Status, Prioritäten, Kategorien, Organisationen, betroffene Endbenutzer mit Namen, Zuständige mit Namen, Gruppen, Servicetypen usw.
View_Issue_Act_Log	Informationen des Aktivitätsprotokolls von Issues
View_Issue_to_Issue_Act_Log	alle Issues mit ihren Aktivitätsprotokollen (diese Ansicht ist eine Verbindung von "View_Issue" und "View_Issue_Act_Log")
View_Issue_to_Properties	Issues und ihre Eigenschaften (dies muss nicht alle Issues einschließen, insbesondere, wenn ihnen keine Eigenschaften zugewiesen sind)
View_Issue_to_Issue_WF	Issues und ihre Workflow-Aufgaben (dies muss nicht alle Issues einschließen, insbesondere, wenn ihnen keine Workflow-Aufgaben zugewiesen sind)

Name anzeigen	Beschreibung
View_Issue_to_Assets	Issues und ihre Assets (dies muss nicht alle Issues einschließen, insbesondere, wenn ihnen keine Assets zugewiesen sind)

Erweiterte Ansichten

Die erweiterten Ansichten basieren auf der Tabelle „audit_log“ von CA SDM.

Hinweis: Vor Verwendung dieser Ansichten müssen Sie die Optionen "audit_ins" und /oder "audit_upd" im Optionsmanager installieren und das System neu starten.

Mit Hilfe der erweiterten Ansichten können Sie Berichte über die Dauer eines Tickets (d.h. Anfrage, Change oder Issue) in einem bestimmten Status erstellen. So können Sie zum Beispiel Berichte zu folgenden Themen erstellen:

- die Dauer zwischen Öffnung und Zuweisung zu Ebene 2 anzeigen; für ab 1. Januar 2002 geöffnete Anfragen.
- die Dauer anzeigen, für die Problemanfragen in Priorität 3 verblieben sind, bevor eine Eskalation zu Priorität 2 erfolgte; für ab 1. Januar 2002 geöffnete Problemanfragen.

Die folgenden erweiterten Ansichten sind verfügbar. Diese sind Ansichten der Tabelle "audit_log" in der CA SDM-Datenbank, die speziell die Attribute für Status, Priorität, Gruppe oder Zuständigen abfragt.

Name anzeigen	Beschreibung
View_Audit_Status	alle Tickets, sortiert nach Dauer in jedem Status (schließt keine Tickets ein, die keinen Status haben)
View_Audit_Priority	alle Tickets, sortiert nach Dauer in jeder Priorität
View_Audit_Group	alle Tickets, sortiert nach Dauer in jeder Gruppe (schließt Tickets nicht ein, die keine Gruppe haben)
View_Audit_Assignee	alle Tickets, sortiert nach Dauer in jeder einzelnen Zuweisung (schließt Tickets nicht ein, die keinen Zuständigen haben)

Wichtig! Zur Anzeige von Daten in den erweiterten Ansichten müssen Sie Audit-Protokolloptionen mit Hilfe des Optionsmanagers installieren. Weitere Informationen hierzu finden Sie in den Beschreibungen zu den Optionen "audit_ins" und "audit_upd" in der Online-Hilfe.

Weitere Informationen:

[Verwendung des Optionsmanagers](#) (siehe Seite 497)

Einrichten von Berichtsmethoden

Mit Berichtsmethoden können Sie angeben, wohin Berichtsergebnisse gesendet werden sollen, wenn Sie einen Bericht auswählen. Beispiele sind die im Menü „Berichte“ verfügbaren zusammengefassten Berichte und Detailberichte und die im Menü „Analyse“ verfügbaren Berichte. Es werden mehrere vordefinierte Berichtsmethoden zur Verfügung gestellt, die Sie auch ändern können.

Hinweis: Weitere Informationen zum Definieren von Berichtsmethoden finden Sie in der *Online-Hilfe*.

Berichtsformatierung

Mit der Datei "dataent.fmt" im Verzeichnis "\$NX_ROOT/fig/cfg" (UNIX) oder im Verzeichnis "installation_directory\fig\cfg" (Windows) können Sie die verschiedenen Datenformate in den Berichten, die Sie drucken, anpassen. Sie können die Datei mit einem beliebigen Text-Editor anzeigen und bearbeiten (Windows-Benutzer sollten zum Bearbeiten der Datei WordPad verwenden).

Die folgenden Zeilen in der Datei steuern einige der Einstellungen für das Datums- und Zeitformat:

```
default_date = "long_date"
short_date = "M/D/YY// Enter a date as MM/DD/YY"
long_date = "MM/DD/YYYY// Enter a date as MM/DD/YY"
default_tod = "hour_12"
hour_12 = "h:mm:ss a(am,pm)// Enter a time of day as hh:mm:ss am/pm"
hour_24 = "HH:mm:ss// Enter a time of day as 00:00:00 - 23:59:59"
hms_12 = "h:mm:ss a(am,pm)// Enter a time of day as hh:mm:ss am/pm"
hms_24 = "HH:mm:ss// Enter a time of day as 00:00:00 - 23:59:59"
default_date_time = "date_time12"
date_time12 = "M/DD/YYYY h:mm:ss a(am,pm)// Enter a date and time as MM/DD/YY hh:mm:ss am/pm"
date_time24 = "M/DD/YYYY HH:mm:ss// Enter a date and time as MM/DD/YY 00:00:00-23:59:59"
```

Sie können diese Zeilen beispielsweise wie folgt ändern, um das europäische Datums- und Zeitformat zu unterstützen:

```
default_date = "long_date"
short_date = "D/M/YY// Enter a date as DD/MM/YY"
long_date = "DD/MM/YYYY// Enter a date as DD/MM/YYYY"
default_tod = "hour_24"
hour_12 = "h:mm:ss a(am,pm)// Enter a time of day as hh:mm:ss am/pm"
hour_24 = "HH:mm:ss// Enter a time of day as 00:00:00 - 23:59:59"
hms_12 = "h:mm:ss a(am,pm)// Enter a time of day as hh:mm:ss am/pm"
hms_24 = "HH:mm:ss// Enter a time of day as 00:00:00 - 23:59:59"
default_date_time = "date_time24"
date_time12 = "M/DD/YYYY h:mm:ss a(am,pm)// Enter a date and time as MM/DD/YY hh:mm:ss am/pm"
date_time24 = "M/DD/YYYY HH:mm:ss// Enter a date and time as MM/DD/YY 00:00:00-23:59:59"
```

Hinweis: Wenn Sie mit "pdm_extract" Daten aus der CA SDM-Datenbank in ein anderes System exportieren und das in der Datei "dataent.fmt" angegebene Datumsformat für die Daten verwenden möchten, verwenden Sie beim Aufrufen von "pdm_extract" das Flag-"d".

Ändern der Sortierreihenfolge der Spalten

Administratoren können mit Web-Screen Painter die Reihenfolge der Spalten ändern, die in Berichten angezeigt werden.

Benutzer können Daten in den folgenden Reihenfolgen sortieren:

- Aufsteigend (A bis Z, 0 bis 9 oder frühestes bis spätestes Datum)
- (Z bis A, 9 bis 0 oder aktuelles bis frühestes Datum)

Hinweis: Weitere Informationen finden Sie in der *Online-Hilfe zu Web Screen Painter*.

Zusammengefasste Berichte und Detailberichte

In CA SDM sind Optionen für die Erzeugung von zusammengefassten Berichten und Detailberichten integriert. Sie können bestimmte Datensätze für einen Bericht mit der Suchfunktion von Listenfenstern auswählen. Zum Beispiel können Sie im Fenster "Anfrageliste" Suchkriterien eingeben, um eine Liste der Anfragen zu generieren, die Sie dann zum Generieren eines Berichts verwenden können.

Zum Drucken oder Anzeigen von zusammengefassten Berichten oder Detailberichten müssen Sie zuerst die Datensätze auswählen, die Sie in den Bericht einschließen möchten. Wählen Sie hierzu in einer Detailseite im Menü "Datei" die Option "Formular drucken". Um einen Bericht für einen neu erstellten Datensatz zu drucken, müssen Sie den Datensatz zuerst speichern.

Hinweis: Weitere Informationen zur Verwendung von Berichten finden Sie in der *Online-Hilfe*.

Analyseberichte

Die Registerkarte „Administration“ von CA SDM bietet die folgenden integrierten Analyseberichte für eine globale und detaillierte Perspektive des Service Desk-Prozesses:

- Berichte zu Anfragen und Issues
- Berichte zu Anfragebereichen und Issue-Kategorien
- Berichte zur Priorität von Anfragebereichen und zur Priorität von Issue-Kategorien

Sie können Analyseberichte für das aktuelle Datum, für die vergangenen dreißig Tage und für Jahr bis dato anzeigen.

Weitere Informationen:

[Generieren von Berichten zu Requests und Issues](#) (siehe Seite 947)

[Generieren von Berichten zu Request-Bereichen und Issue-Kategorien](#) (siehe Seite 948)

[Erstellen von Berichten zur Priorität von Anforderungsbereichen und zur Priorität von Issue-Kategorien](#) (siehe Seite 948)

Generieren von Berichten zu Requests und Issues

Berichte zu Anfragen oder Issues liefern Statistiken für einen bestimmten Zeitraum, wie zum Beispiel die Anzahl der geöffneten Anfragen oder Issues, die Anzahl der geschlossenen Anfragen oder Issues, die durchschnittliche Zeit, die Anfragen oder Issues offen sind, und die durchschnittliche Zeit bis zu ihrer Schließung. Diese Berichte sind nach aufsteigendem Datum sortiert.

So generieren Sie Berichte zu Requests oder Issues über die Web-Schnittstelle:

1. Klicken Sie auf die Registerkarte "Administration".
2. Erweitern Sie die Service Desk- und Analyseknotten.

3. Wählen Sie "Anfrage" oder "Issue" aus.
4. Wählen Sie den entsprechenden Bericht basierend auf dem gewünschten Zeitrahmen aus.

Generieren von Berichten zu Request-Bereichen und Issue-Kategorien

Berichte zu Anfragebereichen oder Issue-Kategorien liefern Ihnen die Anzahl der im angegebenen Zeitraum geöffneten Anfragen oder Issues für jeden Anfragebereich bzw. jede Issue-Kategorie. Diese Berichte sind alphabetisch nach Request-Bereich oder Issue-Kategorie sortiert.

So generieren Sie Berichte zu Request-Bereichen oder Issue-Kategorien über die Web-Schnittstelle:

1. Klicken Sie auf die Registerkarte "Administration".
2. Erweitern Sie die Service Desk- und Analyseknotten.
3. Wählen Sie "Anfrage" oder "Issue" aus.
4. Wählen Sie den entsprechenden Bericht basierend auf dem gewünschten Zeitrahmen aus.

Erstellen von Berichten zur Priorität von Anforderungsbereichen und zur Priorität von Issue-Kategorien

Berichte zur Priorität von Anforderungsbereichen oder zur Priorität von Issue-Kategorien liefern Ihnen die Anzahl der Anfragen oder Issues, die im angegebenen Zeitraum für die einzelnen Anfragebereiche bzw. Issue-Kategorien nach Priorität geöffnet wurden. Diese Berichte sind nach Priorität (von der höchsten bis zur niedrigsten) und dann alphabetisch nach Request-Bereich oder Issue-Kategorie sortiert.

So generieren Sie Berichte zur Priorität von Request-Bereichen oder zur Priorität von Issue-Kategorien über die Web-Schnittstelle:

1. Klicken Sie auf die Registerkarte "Administration".
2. Erweitern Sie die Service Desk- und Analyseknotten.
3. Wählen Sie "Anfrage" oder "Issue" aus.
4. Wählen Sie den entsprechenden Bericht basierend auf dem gewünschten Zeitrahmen aus.

Kapitel 22: Verwalten von Knowledge

Dieses Kapitel enthält folgende Themen:

[Knowledge Management](#) (siehe Seite 949)

[Suchen von Prozeduren für das Knowledge Management](#) (siehe Seite 950)

[Knowledge und Mandantenfähigkeit](#) (siehe Seite 950)

[So richten Sie eine Knowledge Base ein:](#) (siehe Seite 951)

[So verwenden Sie Dokumente in der Knowledge Base:](#) (siehe Seite 954)

[Knowledge-Suche](#) (siehe Seite 960)

[So rufen Sie das CAFedSearch-Servlet über einen REST-Webservice auf](#) (siehe Seite 961)

[Foren](#) (siehe Seite 962)

[Knowledge-Baumstrukturdokumente](#) (siehe Seite 962)

[Knowledge-Dokument-Ablaufplan](#) (siehe Seite 963)

[Zugreifen auf Export/Import](#) (siehe Seite 973)

[Webservices](#) (siehe Seite 990)

Knowledge Management

Knowledge Management bezeichnet das Finden, Organisieren und Veröffentlichen von Knowledge. Knowledge Management erfasst Informationen schnell und effizient und stellt dann diese Informationen einem Benutzer oder einer Gruppe zur Verfügung. Die erfassten und zur Verfügung gestellten Informationen werden als Knowledge Base bezeichnet.

Benutzer greifen auf eine Knowledge Base über eine Suchmaschine zu. Mit Knowledge Management können Sie Inhalt in einer Knowledge Base erstellen und verwalten. Sie können Kategorie- und Dokumentberechtigungen einrichten um dann Gruppen und Rollen entsprechend zuzuweisen. Wenn Sie Ihre Kunden bei komplexen Problemstellungen zur Seite stehen, unterstützt Sie Knowledge Management dabei. Ein effektives Knowledge Management liefert Kunden mit Hilfe eines benutzerfreundlichen und einfach zu navigierenden Prozesses schnell die richtigen Lösungen.

Um Wissen effektiv zu verwalten, gehen Sie wie folgt vor:

- Erstellen Sie eine sinnvolle Inhaltshierarchie.
- Stellen Sie fest, ob das bestehende Knowledge lückenhaft ist.
- Aktualisieren und pflegen Sie das Knowledge, damit es stets relevant bleibt.
- Ermitteln Sie, welchen Wert das vorhandene Knowledge hat.

Weitere Informationen:

[Konfigurieren von Knowledge Management-Datenpartitionseinschränkungen für rollenbasierte Berechtigungen](#) (siehe Seite 332)

Suchen von Prozeduren für das Knowledge Management

Mit CA SDM können Sie das Knowledge Management schrittweise konfigurieren. Weitere Information dazu finden Sie in diesem Handbuch und in der *Online-Hilfe*.

So finden Sie schrittweise Prozeduren zum Knowledge Management in der *Online-Hilfe*:

1. Melden Sie sich bei CA SDM an.
Die Hauptseite von CA SDM wird angezeigt.
2. Führen Sie eine der folgenden Aktionen aus:
 - Klicken Sie im Hauptmenü auf "Hilfe" > "Hilfe" und navigieren Sie in der *Online-Hilfe* zu "Administration" > "Knowledge-Administration".
Die Hilfethemen zu "Knowledge Management" erscheinen, und Sie können darin navigieren, um die benötigten Informationen zu suchen.
 - Klicken Sie im Hauptmenü auf "Hilfe" > "Hilfe zu diesem Fenster".
Die *Online-Hilfe* wird mit einem Hilfethema für die gewünschte Seite angezeigt.

Knowledge und Mandantenfähigkeit

Knowledge-Dokumente und Knowledge-Kategorien können spezifisch für einen Mandanten sein oder für alle Mandanten (öffentlich) freigegeben sein. Wenn Sie ein Knowledge-Dokument suchen, sind die Ergebnisse auf Dokumente begrenzt, die für den Mandanten, der mit dem Ticket verknüpft ist, anzeigbar sind. FAQ-Suchergebnisse sind mandantenspezifisch. Bewertungen für öffentliche Mandantendokumente müssen für jeden Mandanten getrennt verwaltet werden.

Folgende Elemente können Sie auf Mandantenebene verwalten:

- Aktionsinhalte
- Dokumentvorlagen
- Knowledge-Genehmigungsvorgang
- Empfohlene Dokumente
- Knowledge Management-ROI
- Berichte

Alle anderen Knowledge Management-Systemeinstellungen werden global, auf Service-Provider-Ebene verwaltet.

Hinweis: Die Mandantenfähigkeit wird im Optionsmanager über die Registerkarte "Administration" konfiguriert.

So richten Sie eine Knowledge Base ein:

Zu einem effektiven Knowledge Management gehört mehr als nur die Entwicklung einer umfassenden Knowledge Base. Es beinhaltet auch die Implementierung von Prozessen und Verfahren zur Pflege relevanter und exakter Inhalte.

Um eine Knowledge Base einzurichten, sind die folgenden Aufgaben erforderlich:

1. Analysieren Sie, wie die Knowledge Base verwendet werden wird und welchen Umfang sie haben wird.
2. Berücksichtigen Sie, wer die Kunden sein werden, und welche Informationen sie wahrscheinlich benötigen werden.
3. Entwickeln Sie einen strategischen Plan, der die potenziellen Probleme identifiziert, die zu einer Nachfrage des Kundendienstes führen können. Die von Ihnen benannten Probleme helfen Ihnen zu bestimmen, welche Art von Inhalten in Ihrer Knowledge Base erfasst werden sollte.
4. Führen Sie die Entwicklung Ihrer Knowledge Base durch. Erstellen, gliedern, pflegen und sichern Sie diese Daten. All diese Funktionen können Sie mit Knowledge Management problemlos ausführen.

Importieren von Knowledge-Beispieldaten

Es stehen Ihnen Beispiel-Knowledge-Daten aus Knowledge Broker, HowTo und Right Answers zur Verfügung.

Um die Beispiel-Knowledge-Daten zu verwenden, importieren Sie die Daten in die Knowledge Management-Datenbank.

Hinweis: Weitere Informationen zu KT-Beispieldaten finden Sie im *Implementierungshandbuch*.

Überwachen der Knowledge Base

Sie können die Effizienz der Knowledge Base mit den folgenden Berichterstellungs-Tools überwachen. Mit diesen Tools können Sie Statistiken über den Nutzen Ihrer Dokumente und deren Wirksamkeit beim Lösen von Problemen anzeigen.

Knowledge-Berichtskarte

Zeigt Statistiken für Dokumente, die Sie erstellt haben. Jeder Benutzer besitzt eine eigene Knowledge-Berichtskarte.

Webbasierte Berichte

Zeigt Indikatoren darüber an, wie Knowledge unseren Bedürfnissen gerecht wird. Zu den häufig verwendeten Funktionen gehören:

- Anzeigen der am häufigsten aufgerufenen Dokumente
- Anzeigen von Benutzersuchen, die zu keinen Ergebnissen geführt haben

Neuindizierung der Knowledge Base

Bei den folgenden Einstellungen handelt es sich um Sucheinstellungen, und sie erfordern, dass Sie die Knowledge Base mit dem Hilfsprogramm zur Neuindizierung von Knowledge überarbeiten:

- Nach dem Import von Knowledge
- Nach dem Ändern von Einstellungen für die Suchsyntax
- Nach Massenlöschungen
- Bei Suchfehlern

Eine Neuindizierung ist notwendig, weil vorhandene Dokumente Änderungen an Synonymen, Füllwörtern, Sonderbegriffen und anderen Suchparametern erst dann berücksichtigt werden, wenn sie neu indiziert worden sind. Alle neuen Synonyme, Füllwörter und Sonderbegriffe müssen neu indiziert werden, um sicherzustellen, dass Schlüsselwortsuchen in der Knowledge Base aktuell und genau sind.

Sie können die Knowledge-Neuindizierung nur über eine Befehlszeile ausführen. "pdm_k_reindex.exe" lautet die ausführbare Datei für die Knowledge-Neuindizierung.

Hinweis: Die Neuindizierung der Dokumente in der Knowledge Base kann in Abhängigkeit von der Größe Ihrer Datenbank ein zeitaufwändiger Vorgang sein. Es wird empfohlen, das Hilfsprogramm zur Neuindizierung von Knowledge auszuführen, nachdem alle Änderungen hinzugefügt worden sind.

Indizieren der Warteschlangeneinstellungen für Batch-Verarbeitung und sofortige Verarbeitung bzw. Entfernen der Indizierung

Das Indizieren und das Entfernen der Indizierung führt einen Batch-Vorgang aus, um eine vordefinierte Anzahl von Dokumenten auf einmal zu bearbeiten. Diese Batch-Vorgänge werden für die Leistungsoptimierung verwendet. Wenn mehr Dokumente im Batch enthalten sind, erhöht sich die Systemleistung.

Sie können nur eine begrenzte Anzahl von Dokumenten verarbeiten. Die Anzahl richtet sich nach der Größe der Dokumente und nach den mit ihnen verknüpften Anhängen. Die Dokumentgröße wird auf Grundlage des Texts (Nur-Text) und den Anhängen berechnet. Bild- und Formatierungselemente werden nicht berechnet.

Hinweis: Sie können die Größe der Anhänge beschränken, indem Sie auf der Registerkarte "Administration" zu "Anhangsbibliothek" > "Repositorys" navigieren und das Repository bearbeiten, um die "Dateigrößenbeschränkung" (KB) festzulegen.

Die empfohlene maximale Batch-Größe sollte zwischen 2-12 MB liegen (gemäß Parameter "EBR_MAX_INDEX_BATCH_SIZE" der Datei "NX.env" und durchschnittlicher Dokumentgröße).

- Wenn die durchschnittliche Größe Ihres Dokuments (einschließlich Anhänge) ca. 0,1 MB beträgt, behalten Sie die Standardeinstellung in der Datei "NX.env" bei:

```
@EBR_MAX_INDEX_BATCH_SIZE=128
@NX_EBR_INDEX_QUEUE_TIMEOUT=10
@NX_EBR_REINDEX_QUEUE_TIMEOUT=1
@NX_EBR_INDEX_QUEUE_ONLINE=Yes
@NX_EBR_NON_KD_INDEX_QUEUE_ONLINE=Yes
```

Diese Einstellung gibt an, dass in einem Batch 128 Dokumente verarbeitet werden, dass Batch-Ausführungen in Intervallen von zehn Sekunden stattfinden und dass während einer Neuindizierung das Intervall zwischen zwei Batches 1 Sekunde beträgt.

- Wenn die durchschnittliche Größe Ihres Dokuments (einschließlich Anhänge) ca. 0,5 MB beträgt, behalten Sie die Standardeinstellung in der Datei "NX.env" bei:

```
@EBR_MAX_INDEX_BATCH_SIZE=25
@NX_EBR_INDEX_QUEUE_TIMEOUT=10
@NX_EBR_REINDEX_QUEUE_TIMEOUT=10
@NX_EBR_INDEX_QUEUE_ONLINE=No
@NX_EBR_NON_KD_INDEX_QUEUE_ONLINE=No
```

Diese Einstellung gibt an, dass in einem Batch 25 Dokumente verarbeitet werden, dass Batch-Ausführungen in Intervallen von zehn Sekunden stattfinden und dass während einer Neuindizierung das Intervall zwischen zwei Batches 1 Sekunde beträgt.

So verwenden Sie Dokumente in der Knowledge Base:

Knowledge-Dokumente bieten Ihnen Informationen zu Knowledge, das in der Knowledge Base gespeichert ist. Die Erstellung von qualitativ hochwertigem Knowledge erfordert die Zusammenarbeit mehrerer Personen. Jede Person ist für das Durchführen bestimmter Aufgaben in den verschiedenen Phasen des Lebenszyklus eines Knowledge-Dokuments verantwortlich. Knowledge-Dokumente befinden sich in der Knowledge Base und werden in folgendem kontinuierlichem Prozess verwaltet:

1. Identifizieren Sie die Inhalte, die in die Knowledge Base aufgenommen werden sollen.
2. Erstellen Sie ein Knowledge-Dokument.

Knowledge-Dokumente werden in Kategorien platziert, die manche Organisationen Eigentümern zuweisen.

Hinweis: Wenn ein Dokument erstellt oder aktualisiert wird, wird es im Posteingang des Eigentümers platziert. Elemente im Posteingang können erst nach ihrer Veröffentlichung als Lösungen angezeigt und der Knowledge Base hinzugefügt werden.

3. Überarbeiten Sie das Dokument.

Nachdem ein Dokument in einem Posteingangsordner im Scoreboard ankommt, können Anwender ihre zugewiesenen Aufgaben durch Ändern ihrer Dokumente entsprechend der ihnen zugewiesenen Rollen durchführen.

Alle Anwender mit voller (Schreib-/Lese-)Berechtigung für das Dokument können das Dokument ändern. Der aktuelle Eigentümer hat alle Rechte für das Dokument, verfügt aber möglicherweise nicht über eine ausdrückliche Schreibberechtigung. Anwender können neue Versionen bzw. Rollbacks zu einer früheren Version erstellen, wenn ein Problem mit dem Dokument aufgetreten ist.

4. Senden Sie das Dokument ab.

Knowledge kann vom Kunden oder Mitarbeiter über die Self-Service-Schnittstelle abgesendet werden, oder über CA SDM. Diese Option lässt Analysten eine neue Lösung für ein vorhandenes Ticket absenden. Dies bietet auch eine Verbindung zwischen einem Problem und seiner Lösung, und kann anderen Anwendern mit ähnlichen Problemen helfen, eine Lösung zu finden.

5. Veröffentlichen Sie das Dokument.

Nachdem ein Dokument den vollständigen Genehmigungsprozesszyklus durchlaufen hat, kann es veröffentlicht werden. Ein Dokument, das veröffentlicht wurde, wird zum angegebenen Startdatum, das standardmäßig dem aktuellen Datum entspricht, Teil der anzeigbaren Knowledge Base. Das Dokument ist nur für die Gruppen anzeigbar, die über die entsprechenden Zugriffsberechtigungen verfügen. Ein Anwender mit vollen Berechtigungen kann ein veröffentlichtes Dokument bearbeiten.

6. Prüfen Sie das Dokument und entscheiden Sie, ob Sie die folgenden Aufgaben durchführen:
- **Die Veröffentlichung des Dokuments rückgängig machen** – Der Eigentümer des Dokuments, ein Knowledge-Manager oder der Administrator hat die Möglichkeit, die Veröffentlichung des Dokuments rückgängig zu machen, wenn noch Bearbeitungsbedarf besteht.
 - **Eine Überarbeitungsversion erstellen** – Anwender mit vollen Bearbeitungsrechten können eine Überarbeitungsversion eines veröffentlichten Dokuments erstellen, während es online und für die Anzeige und Suche verfügbar bleibt. Eine Arbeitsversion ist zunächst eine Kopie des Dokuments, die in der Knowledge Base nach dem Verifizieren und erneuten Veröffentlichen ersetzt wird.
 - **Das Dokument deaktivieren** – Der Eigentümer des Dokuments, ein Knowledge-Manager oder ein Systemadministrator kann das Dokument über die Knowledge Base deaktivieren.

Welche Aufgaben durchgeführt werden und wer die einzelnen Aufgaben durchführt, kann gemäß der in der Organisation bestehenden Genehmigungsstruktur definiert werden.

Hinweis: Sie können Knowledge-Aktivitäten auf der Registerkarte "Ereignisprotokoll" auf den Kontaktdetailseiten nachverfolgen. Wenn beispielsweise ein Endanwender ein Knowledge-Dokument anzeigt, wird das Ereignisprotokoll aktualisiert und zeigt die ausgeführte Aktion und eine Verknüpfung mit dem Dokument an. In dem Ereignisprotokoll wird auch festgehalten, wie lange der Anwender das Dokument geöffnet hat.

Knowledge-Einreichung in CA SDM

Wenn Sie Knowledge erlangen, von dem Sie denken, es sollte der Knowledge Base hinzugefügt werden, können Sie es zur Berücksichtigung absenden. Neben der Self-Service-Schnittstelle können Sie Knowledge auch über CA SDM absenden. Ein Analyst kann eine neue Lösung von einem vorhandenen Ticket aus einreichen, das eine Verbindung zwischen einem Problem und seiner Lösung darstellt. Außerdem kann es anderen Benutzern mit ähnlichen Problemen helfen, eine Lösung zu finden. In einer Organisation, in der Hunderte von Tickets gleichzeitig geöffnet sind, kann dies wertvolle Zeit sparen.

Alle Knowledge-Dokumente müssen einer Knowledge-Kategorie zugewiesen werden. Wenn der Incident-/Anfragebereich in CA SDM mit der Knowledge-Kategorie in Knowledge Management übereinstimmt, wird die Kategorie automatisch für die Knowledge-Einreichung ausgewählt.

Knowledge-Einreichung über Self-Service

Standardmäßig kann jeder Benutzer, der bei Knowledge Management angemeldet ist, über die Seite "Knowledge absenden" Knowledge absenden. Dies bedeutet, dass ein Kunde Knowledge senden kann, ohne den lokalen Service Desk-Vertreter kontaktieren zu müssen. Nach dem Absenden von Knowledge wird es durch einen Veröffentlichungsprozess geleitet, in dem es überprüft und bearbeitet wird, bevor es der Knowledge Base hinzugefügt wird.

Es ist wichtig, Informationen in jedes Feld einzugeben, das auf der Seite "Knowledge absenden" angezeigt wird. Besondere Aufmerksamkeit sollten Sie dem Feld "Zusammenfassung" widmen. In der Regel enthält dieses Feld einen knappen Überblick über das Dokument, das Sie absenden.

Dokument-Attribute

Dokument-Attribute helfen Ihnen bei der Verwaltung der Dokumente in Ihrem Knowledge-Pool. Dokument-Attribute können aktualisiert werden, um einem Dokument einen neuen Experten oder Eigentümer zuzuweisen. Sie können auch das Datum angeben, zu dem das Dokument in der Knowledge Base verfügbar wird, und das Datum, zu dem es abläuft. Durch Auswählen verschiedener Dokumentvorlagen können Sie das Layout jedes Dokuments ändern.

Dokumentberechtigungen

Sie können Berechtigungen für ein Dokument festlegen, anzeigen und bearbeiten. Diese Berechtigungen können verschiedenen Gruppen von Individuen zugewiesen werden. Beim Einstellen der Berechtigungen können Sie wählen, ob Berechtigungen von der Hauptkategorie eines Dokuments geerbt werden sollen oder neue Berechtigungen angeben. Standardmäßig erben Dokumente die Berechtigungen ihrer Hauptkategorie. Dies ermöglicht das Bearbeiten von Zugriffsberechtigungen auf Kategorieebene anstatt auf Dokumentenebene.

Wichtig! Achten Sie beim Erstellen eines Knowledge-Dokuments darauf, die Benutzer in der Dokumentberechtigung zu berücksichtigen, die dem Dokument später im Genehmigungsverfahren zugeteilt werden könnten. Wenn eine Gruppe einem Dokument zugewiesen wird, kann es vorkommen, dass Benutzer aus dieser Gruppe nicht zum Anzeigen des Dokuments berechtigt sind. Wenn das Dokument einem bestimmten Anwender zugewiesen wird, eröffnen die Standard-Datenpartitionseinschränkungen dem Anwender die Möglichkeit, das Dokument anzuzeigen.

Bearbeiten der Lösung

Sie können Knowledge-Dokumente in Knowledge Management mit dem HTML-Editor erstellen. Diese Funktion gibt Ihnen die Möglichkeit, das Lösungsfeld in einem Knowledge-Dokument im Modus *WYSIWYG* (what you see is what you get, engl. etwa für: ziemlich genaue Bildschirmdarstellung des Ausgabeformates) zu ändern. Die Verwendung des HTML-Editors verbessert den Erstellungsprozess, da Sie Dokumente erstellen können, ohne im HTML-Code schreiben zu müssen, und dabei Text formatieren, Grafiken und Tabellen einfügen sowie Verknüpfungen zu anderen Dokumenten erstellen können. Dies beschleunigt den Schreibprozess und stellt eine einfache Methode dar, Dokumente zu bearbeiten.

Der HTML-Editor dient zum Durchführen folgender Aufgaben:

- **HTML-Code anzeigen:** Über die Registerkarten "Design-Modus" und "Quellmodus" in der Symbolleiste des HTML-Editors können Sie zwischen den verschiedenen Ansichten hin- und herschalten.
- **Text formatieren:** Sie können Dokumenttext direkt in das Fenster des HTML-Editors eingeben. Anschließend können Sie den Text über die Optionen in der Symbolleiste und über die Menüoptionen formatieren.
- **Grafiken einfügen:** Sie können eine Grafik in Ihren HTML-Text einfügen, indem Sie ein Bild aus der Bildbibliothek auswählen oder eine eigene Grafik hochladen.
- **Tabellen einfügen:** In einem Knowledge-Dokument können Sie große Informationsmengen übersichtlich für Benutzer zur Verfügung stellen. Sie können Tabellen anlegen, um diese Informationen klar gegliedert in Reihen und Spalten anzuzeigen.
- **Hyperlinks zu anderen Dokumenten hinzufügen:** Sie können Hyperlinks in Knowledge-Dokumente einfügen, wenn Sie ein Knowledge-Dokument erstellen oder verändern. Auf diese Weise kann ein Knowledge-Dokument mit anderen relevanten Dokumenten oder URLs verknüpft werden. Wenn der HTML-Editor im Entwurfsmodus verwendet wird, werden Hyperlinks als blauer, unterstrichener Text angezeigt.
- **Aktionsinhalte einfügen:** Sie können Aktionsinhalte (eine Live-URL) in das Lösungsfeld eines Knowledge-Dokuments einfügen. Wenn der Benutzer auf sie klickt, wird so ein Incident erstellt oder eine andere Aktion ausgeführt.

Vorbereiten der Dokumentveröffentlichung

Nachdem Sie ein Knowledge-Dokument gesendet haben, bereiten Sie es durch das Festlegen von Attributen und Genehmigungen für die Veröffentlichung vor. Solche Steuerungen sind wichtig, um Dokumente effizient zu organisieren.

Weitere Informationen:

[So verwenden Sie Dokumente in der Knowledge Base:](#) (siehe Seite 954)

[Dokument-Attribute](#) (siehe Seite 956)

[Dokumentberechtigungen](#) (siehe Seite 956)

Dokumentveröffentlichung

Nachdem ein Dokument den vollständigen Genehmigungsprozesszyklus durchlaufen hat, kann es veröffentlicht werden. Ein Dokument, das veröffentlicht wurde, wird zum angegebenen Startdatum, das standardmäßig dem aktuellen Datum entspricht, Teil der anzeigbaren Knowledge Base. Das Dokument ist nur für die Gruppen anzeigbar, die über die entsprechenden Zugriffsberechtigungen verfügen.

Wenn ein Knowledge-Dokument veröffentlicht wird, ist der Benutzer in der Regel nicht berechtigt, das Dokument zu bearbeiten, es sei denn, die Veröffentlichung wird rückgängig gemacht. Dann können Änderungen vorgenommen werden. Während dieser Zeit ist das Knowledge-Dokument offline und für Benutzer nicht verfügbar. Der Eigentümer des Dokuments, ein Knowledge Manager oder ein Systemadministrator, kann die Veröffentlichung eines Dokuments über die Schaltfläche "Überarbeiten" und das Kontrollkästchen "Veröffentlichung rückgängig machen". Ein Dokument, dessen Veröffentlichung rückgängig gemacht wurde, erhält wieder den Status „Entwurf“. Ein Administrator-Benutzer kann dann den nächsten Schritt im Workflow-Vorgang auswählen.

Versionsdokumente

Mithilfe der Funktionen zur Dokumentversionskontrolle von Knowledge Management kann ein Analyst mit der entsprechenden Bearbeitungsberechtigung eine *Überarbeitungsversion* des Dokuments erstellen. Eine Arbeitsversion ist zunächst eine Kopie des Dokuments, die in der Knowledge Base nach dem Verifizieren und erneuten Veröffentlichen ersetzt wird. Die Notwendigkeit, die Veröffentlichung des Dokuments zuerst rückgängig zu machen, wird dadurch umgangen.

Anwender mit Bearbeitungsberechtigungen können auch die folgenden Versionskontrollen ausführen:

- Speichern Sie eine Entwurfsversion des Dokuments.
- Führen Sie ein Rollback auf eine frühere Version eines Dokuments durch, falls ein Problem mit der aktuellen Version ('Entwurf' oder 'Veröffentlicht') aufgetreten ist. Auf der Registerkarte 'Versionen' im Fenster 'Dokumentvorlage aktualisieren' können Anwender verschiedene Versionen für das Rollback markieren, die die aktuelle Version ersetzen sollen.
- Verfolgen Sie die Anzahl der Dokumentversionen, die gespeichert, gelöscht und in der Knowledge Base archiviert werden.

Der Knowledge-Dokument-Posteingang auf dem CA SDM-Scoreboard ist das Repository für Dokumente mit allen Status, einschließlich gespeicherter und zugewiesener Entwurfs- und Überarbeitungsdokumente.

Verwalten von Dokumentversionen

Administratoren können Dokumentversionen einrichten und verwalten, indem sie die folgenden Schritte ausführen:

1. Legen Sie fest, wer veröffentlichte Dokumente bearbeiten kann, und erstellen Sie Arbeitsversionen. Die Rolle, die für einen bestimmten Kontaktdatensatz benutzt wird, verfügt über die Berechtigung zur Bearbeitung.
2. Definieren Sie eine Vorlage für einen Genehmigungsvorgang, in der Aufgaben oder Schritte gruppiert sind, die während des Dokumentlebenszyklus ausgeführt werden sollen. Standardmäßig ermöglicht eine integrierte Vorlage für den Genehmigungsvorgang Ihnen die Erstellung von Dokumenten.
3. Legen Sie fest, ob der Genehmigungsvorgang für Dokumente verwendet werden soll. Analysten, die den Genehmigungsvorgang überspringen dürfen, können bestimmen, welche Aufgaben sie bei der Erstellung einer Arbeitsversion zuerst ausführen wollen.
4. Erstellen Sie Archivierungs- und Lösungsregeln für die Pflege von Dokumentversionen.

Dokumentablauf

Wenn ein veröffentlichtes Dokument sein Ablaufdatum erreicht, wird es durch die Software in der Regel zurückgezogen (das heißt, das Dokument wird aus der Wissensdatenbank und dem Genehmigungsverfahren gelöscht).

Archivieren und Bereinigen von Dokumenten

Sie können die Größe Ihres Knowledge-Pools über die CA SDM-Funktion "Archivieren und Löschen" verwalten, mit der alte und nicht mehr verwendete Dokumente automatisch entfernt werden. Die Funktion "Archivieren und Löschen" sorgt dafür, dass die Suche nach Knowledge effizienter verläuft, indem nur ein aktuelles Dokument ausgegeben wird.

Archivierung und Löschung wird als Hintergrundprozess ausgeführt und entfernt entsprechend den von Ihnen festgelegten Regeln automatisch inaktive Datensätze aus der CA SDM-Datenbank. Diese Regeln werden in bestimmten Zeitintervallen auf CA SDM-Objekte angewendet.

Knowledge-Suche

Knowledge Management bietet Anwendern die folgenden Möglichkeiten, Knowledge abzurufen:

Durchsuchen von Kategorien

Lösungen auf Grundlage von Kategorien finden In jeder Kategorie können zusätzliche Unterkategorien verwendet werden, um die Suchergebnisse auf eine Lösungsmenge einzuengen, die wahrscheinlich für ein Problem relevant ist.

Hinweis: Wenn Sie mithilfe der Kategorie nach Knowledge-Dokumenten suchen, zeigt das Suchergebnis die Anzahl der Schlüsselwörter an, die für die Suche mit der Liste der Dokumente verwendet wurde. Die Anzahl innerhalb der Klammern ist die Gesamtanzahl der Dokumente in der Knowledge Base, die mindestens ein Vorkommen des Schlüsselworts enthält. Wenn Sie zum Beispiel die Zeichenfolge, "Live-Unterstützung" suchen und 3 Dokumente mindestens einmal dieses Schlüsselwort enthalten, dann wird "Live-Unterstützung(3)" angezeigt.

Die Anzahl wird nicht entsprechend den angegebenen Suchkriterien gefiltert. Möglicherweise stimmt die Anzahl der aufgelisteten Dokumente nicht überein. Zusätzlich enthält die Anzahl nur Dokumente, die von "pdm_k_reindex" bearbeitet wurden. Deshalb werden Dokumente, die die angegebene Zeichenfolge enthalten, jedoch nach dem aktuellsten "pmd_k_reindex" veröffentlicht wurden, nicht in die Anzahl eingeschlossen.

Um die eingeklammerte Anzahl abzustellen, fügen Sie Folgendes zur Datei "\$NX_ROOT/NX.env" hinzu:

```
@EBR_SHOW_WORDS_DF=No
```

Knowledge-Baumstruktur

Stellt eine Reihe von Fragen, um den Anwender zu möglichen Lösungen zu führen. Die zur Auswahl stehenden Antworten führen den Anwender zu einer Lösung, die am relevantesten erscheint.

Lesezeichen

Bietet Zugriff auf häufig angesehene Dokumente, die in einer Lesezeichenliste enthalten sind.

So rufen Sie das CAFedSearch-Servlet über einen REST-Webservice auf

Das CAFedSearch-Servlet stellt eine RESTful-Schnittstelle bereit, an die Such-Clients ihre Suchanfrage senden können. Dieses Servlet enthält einen Plug-in-Adapter, um Kunden zu erlauben, ihre eigenen Suchmaschinen zu integrieren.

Die RESTful-Schnittstelle akzeptiert GET-Anfragen von der HTTP-Collection mit dem OpenSearch-Format.

Gehen Sie wie folgt vor:

1. Um einen REST-Zugriffsschlüssel zu erhalten, senden Sie die HTTP-POST-Anforderung auf der `rest_access`-Ressource mit Anmeldeinformationen.
2. Um ein BOPSID-Token mit dem REST-Zugriffsschlüssel zu erhalten, senden Sie eine HTTP-POST-Anforderung auf der `bopsid`-Ressource. Weitere Informationen finden Sie unter *Webservices-Methoden* im *Administrationshandbuch*.

Sie können sich auch die Beispieldateien in den folgenden Speicherorten ansehen:

`NX_ROOT\samples\sdk\rest\java`

Verwenden Sie eine föderierte Such-API, um die Suche auszuführen. Senden Sie die HTTP-GET-Anforderung auf der `search`-Ressource, und übergeben Sie die Suchkriterien und das BOPSID-Token über die CA SDM-URL. Weitere Informationen finden Sie im *Administrationshandbuch*.

Foren

In Foren können Sie über vorhandene Themen kommunizieren. Foren ermöglichen die globale Freigabe von Dokumenten innerhalb von vordefinierten Gruppen, die gemeinsames Knowledge nutzen und an der Lösung vorhandener Herausforderungen arbeiten.

Foren ermöglichen die Diskussion von allgemeinen Fragen, nützlichen Hinweisen zur Verwendung usw. und erweitern so den Umfang des Knowledge-Bestands. Sie können ein neues Forum über die Registerkarte "Knowledge" oder über ein Service Desk-Ticket erstellen.

Knowledge-Baumstrukturdokumente

Der Knowledge-Baumstrukturdesigner ist ein visuelles Tool, das verwendet wird, um schnell und problemlos Knowledge-Baumstrukturen zu erstellen. Eine Knowledge-Baumstruktur ist eine Darstellung von Fachwissen in einem bestimmten Gebiet. Der Knowledge-Baumstrukturdesigner ermöglicht Analysten und Knowledge-Entwicklern die Erstellung ausführlicher Baumstrukturen, mit deren Hilfe Benutzer durch eine Reihe von Fragen und möglichen Antworten zu einer Lösung geführt werden. Dank diesem Tool sind spezialisierte Skripterstellungs- oder Programmierkompetenzen nicht mehr erforderlich, sodass ein Analyst und ein Experte für die Erstellung eines Baumstruktur-Designs genügen.

Knowledge-Baumstrukturen können sehr komplex sein. Deshalb wird empfohlen, ein Diagramm zu erstellen, um die Struktur vor dem eigentlichen Erstellen der Knowledge-Baumstruktur grafisch abzubilden. Das Diagramm muss eine Reihe von Fragen, möglichen Antworten und verknüpften Lösungen enthalten. Die Hierarchie der Fragen und Antworten in diesem Diagramm ist die Grundlage, auf der die Knowledge-Baumstruktur erstellt wird.

Nachdem Sie ein Diagramm Ihrer Knowledge-Baumstruktur erstellt haben, erstellen Sie die eigentliche Baumstruktur mit Hilfe des Knowledge-Baumstrukturdesigners.

Knowledge-Dokument-Ablaufplan

Der Knowledge-Dokument-Ablaufplan stellt Change Managern, Knowledge Managern und Analysten der Ebene 2 eine umfangreiche Ansicht auf Schlüssel-Events im Knowledge Management-Lifecycle bereit. Die folgenden Events können für ein Knowledge-Dokument geplant werden:

- Absenden
- Veröffentlichung
- Überprüfung
- Ablaufdatum

Auf der Registerkarte 'Knowledge Management-Ablaufplan' wird ein ähnliches Kalenderformat wie beim Change-Kalender angezeigt, anstelle von Start- und Endzeiten werden jedoch nur bestimmte Daten angezeigt.

[Konfigurieren der Ablaufplaner-Ansichten](#) (siehe Seite 822) beinhaltet das Festlegen von Anweisungen für Makros.

Der Knowledge-Dokument-Ablaufplan kann auch in das iCalendar-Format exportiert werden.

Hinweis: Wenn Ablaufpläne in einigen Kalenderprogrammen exportiert werden, führt die Auswahl der Option 'Öffnen' anstatt der Option 'Auswählen' zu einem inkorrekten Import der Datei. Um dieses Problem in Knowledge Management- und Change-Ablaufplänen zu vermeiden, wählen Sie anstelle der Option "Öffnen" die Option "Speichern". Nachdem Sie die exportierte Datei gespeichert haben, importieren Sie sie über die Kalenderprogrammschnittstelle.

Knowledge - Ablaufplanfilter

Der Knowledge-Ablaufplanfilter zeigt die folgenden Felder an:

Mandant

Filtert die Suche nach Mandanten. Dieses Feld wird dem berechtigten Anwender in einer Installation für mehrere Mandanten angezeigt.

Event-Typ

Filtert die Suche nach den folgenden Event-Typen:

- Absenden
- Überprüfung
- Veröffentlichung
- Deaktivierung

Startdatum des Ablaufplans

Gibt das Datum für den Beginn eines Zeitraums zum Filtern des Verlaufs an, um nur Einträge eines bestimmten Zeitraums anzuzeigen.

Enddatum des Ablaufplans

Gibt das Datum für das Ende eines Zeitraums zum Filtern des Verlaufs an, um nur Einträge eines bestimmten Zeitraums anzuzeigen.

Zeitzone des Ablaufplans

Gibt eine Zeitzone für die Anzeige Ihrer Suchergebnisse an.

Hinweis: Wenn keine Zeitzone ausgewählt wird, werden die Events in der aktuellen Zeitzone angezeigt.

Eigentümer

Definiert den Namen des Kontakts, der für die Pflege des Dokuments zuständig ist. Geben Sie den Namen des Kontakts im Format "Nachname, Vorname" ein, oder öffnen Sie das Dialogfeld "Kontakte – Suche", um einen Kontakt zu suchen und auszuwählen.

Verantwortlicher

Definiert den Namen des Kontakts, der für die Verarbeitung des Datensatzes zuständig ist. Geben Sie den Namen des Kontakts im Format "Nachname, Vorname" ein, oder öffnen Sie das Dialogfeld "Kontakte – Suche", um einen Kontakt zu suchen und auszuwählen.

Experte

Definiert der Name eines Kontakts mit Sachkenntnissen bezüglich des Inhalt des Dokuments. Geben Sie den Namen des Kontakts im Format "Nachname, Vorname" ein, oder öffnen Sie das Dialogfeld "Kontakte – Suche", um einen Kontakt zu suchen und auszuwählen.

Status

Wählen Sie einen der folgenden Dokumentstatus aus, um Ihre Suche auszuführen:

- Entwurf
- Veröffentlicht
- Deaktiviert

Kategorie

Definiert eine Kategorie, nach der die abgerufenen Dokumente gefiltert werden sollen. Geben Sie den Namen der Kategorie in das Feld ein, oder öffnen Sie das Fenster "Kategorien - Suche". Wenn Sie auf "Suche" klicken, werden nur die Dokumente abgerufen, die mit der angegebenen Kategorie verknüpft sind.

Anfangsansicht

Markieren Sie die Ansicht des Knowledge Management-Kalenders, die Sie anzeigen möchten:

Monat

Zeigt einen Kalender für den ganzen Monat an, der das früheste Startdatum für die Implementierung beinhaltet. Es ist in dem Feld "Startdatum" angegeben. Der Kalender enthält zusammenfassende Informationen zu jedem Change innerhalb des Zeitbereichs (Change-Nummer, Start- und Endzeit und die ersten zehn betroffenen CIs).

Woche

Zeigt sieben aufeinander folgende Tage in einer einzigen Spalte an. Zuerst wird das früheste Startdatum der Implementierung angezeigt, es wird im Feld "Startdatum" angegeben. Der Kalender enthält zusammenfassende Informationen zu jedem Change innerhalb des Zeitbereichs (Change-Nummer, Start- und Endzeit, zusammenfassende Beschreibung, Zuständiger, Gruppe und die ersten zehn betroffenen CIs).

Tag

Zeigt eine ähnliche Ansicht wie die Wochenansicht, mit dem Unterschied, dass nur der im Feld "Startdatum" angegebene Tag angezeigt wird.

***n* Tage**

Zeigt eine Ansicht ähnlich der Wochenansicht an, die jedoch die festgelegte Anzahl der Tage enthält.

Liste

Zeigt eine standardmäßige CA SDM-Listenseite an.

Hinweis: Sie können auf das Symbol "Mehr" klicken, um das Feld "Weitere Suchargumente" anzuzeigen. Dieses Feld ist nur für erfahrene Anwender gedacht, die mit SQL und Majic umgehen und bestimmte weitere Suchargumente angeben können, die im Standard-Suchbereich nicht zur Verfügung stehen. Sie können eine SQL WHERE-Klausel in dieses Feld eingeben, um ein weiteres Suchargument festzulegen.

Ansichten von Knowledge-Ablaufplänen

Für den Ablaufplan von Knowledge-Dokumenten sind die folgenden Ansichten verfügbar:

Monat

Zeigt einen Kalender für den ganzen Monat an, der das früheste Startdatum für die Implementierung beinhaltet. Es ist in dem Feld "Startdatum des Ablaufplans" angegeben. Der Kalender enthält zusammenfassende Informationen zu jedem Change innerhalb des Zeitbereichs (Change-Nummer, Start- und Endzeit und die ersten zehn betroffenen CIs).

Der Knowledge-Dokument-Ablaufplan hat eine ähnliche Funktion wie die Monatsansicht von Changes, mit den folgenden Ausnahmen:

- Knowledge-Events haben nur ein Datum (keine Uhrzeit) und werden nach Event-Typ gruppiert. Sie ähneln somit Changes, die für jeden Zeitraum und Change-Typ gruppiert werden.
- Event-Typen verwenden schedGroup-Makros und haben die folgenden vordefinierten Farben:
 - Absenden – Schwarz
 - Überprüfung – Grün
 - Veröffentlichung – Blau
 - Deaktivierung – Rot

Hinweis: Wenn Sie ein in der Vergangenheit liegendes Überprüfungsdatum sehen, heißt das, dass die Überprüfung wahrscheinlich nicht durchgeführt wurde.

Woche

Zeigt sieben aufeinander folgende Tage in einer einzigen Spalte an. Zuerst wird das früheste Startdatum der Implementierung angezeigt, es wird im Feld "Startdatum des Ablaufplans" angegeben. Der Kalender enthält zusammenfassende Informationen zu jedem Change innerhalb des Zeitbereichs (Change-Nummer, Start- und Endzeit, zusammenfassende Beschreibung, Zuständiger, Gruppe und die ersten zehn betroffenen CIs).

Tag

Zeigt eine ähnliche Ansicht wie die Wochenansicht, mit dem Unterschied, dass nur der im Feld "Startdatum des Ablaufplans" angegebene Tag angezeigt wird.

n Tage

Zeigt eine Ansicht ähnlich der Wochenansicht an, die jedoch die festgelegte Anzahl der Tage enthält.

Liste

Zeigt eine standardmäßige CA SDM-Listenseite an.

Konfigurieren von Planungsansichten

Sie konfigurieren die monatlichen und wöchentlichen Planungsansichten, indem Sie "pdm_macro"-Anweisungen im Abschnitt <head> der HTML-Formulare angeben, die den Ablaufplan definieren. Es wird empfohlen, das Quellansicht von Web Screen Painter zu benutzen, um diese Formulare zu bearbeiten.

Jedes Formular, das einen Ablaufplan anzeigt, muss Folgendes enthalten:

- Ein "schedConfig"-Makro
- Mindestens ein schedAttr-Makro
- Mindestens ein schedGroup-Makro

Die Konfigurationsmakros befinden in einer separaten Quelldatei, die von einer pdm_include-Anweisung in der Hauptquelldatei referenziert wird. Diese ermöglicht Ihnen, Ihren Ablaufplan zu konfigurieren, ohne die Hauptquelldatei zu ändern.

Die Konfigurationsmakros für das Change-Kalender-Formular "list_chgsched.html" befinden sich beispielsweise in der Datei "list_chgsched_config.html". Für den Knowledge-Lebenszyklus-Ablaufplan können Sie die Datei "list_kdsched_config.html" mit denselben Makros ändern.

Sie können list_chgsched_config.html und list_kdsched_config.html im folgenden Verzeichnis finden:

\$NX_ROOT\bopcfg\www\html\web\analyst\

"schedConfig"-Makro – Konfigurieren von Schichten

Das "schedConfig"-Makro gibt an, dass ein Formular einen Ablaufplan enthält und grundlegende Konfigurationsinformationen bietet. Folgende Werte sind gültige Makroargumente:

autosearch=1|0

Gibt an, ob das Ablaufplanformular erneut Daten vom Server laden soll oder nicht, wenn der Anwender eine Ansicht außerhalb des derzeit ausgewählten Datumsbereichs auswählt. Die Festlegung des Werts auf 1 (Standard) hat zur Folge, dass das Formular automatisch sucht, wenn der Anwender eine Ansicht mit einem oder mehr Tagen außerhalb des Datumsauswahlbereichs des Suchfilters auswählt. Bei der Festlegung des Werts auf 0 muss der Anwender die Schaltfläche "Suche" drücken, um die Suche zu starten.

defaultView=0|1|7|30|99

Gibt die Standardansicht für den Suchfilter als 0 (Liste), 1 (Tag), 7 (Woche), 30 (Monat), oder 99 (n-Tage) an.

Die Angabe für defaultView wirkt sich nur auf die anfängliche Anzeige des Suchfilters aus. Sobald der Ablaufplan angezeigt wird, stimmt CA SDM automatisch die Ansichtsauswahl des Filters auf die aktuelle Ansicht ab.

Standard: 30

firstday=0|1|2|3|4|5|6|7

Gibt den ersten Wochentag in der Monatsansicht als eine Zahl zwischen 0 (Sonntag) und sechs (Samstag) an.

Standard: 0

export=xxx|0

Gibt den Codenamen der Vorlage an, der für den Export in das iCalendar-Format verwendet wird. Durch Festlegen des Werts auf 0 wird angegeben, dass die Exportfunktion und die Export-Schaltfläche deaktiviert sind.

Standard: ChangeSchedule

legend=1|2|0

Gibt die Lokation der Ablaufplanlegende an, die den Namen und die Formatierung der Gruppen im Ablaufplan anzeigt. Sie können den Wert auf 1 einstellen, um die Legende über dem Ablaufplan zu platzieren, oder auf 2, um die Legende unter dem Ablaufplan zu platzieren. Setzen Sie den Wert auf 0, um die Legende zu deaktivieren.

Standard: 2

maxGroups=0/n

Gibt die größtmögliche Anzahl von Gruppen an, die in einer einzigen Zelle der Kalendermonatsansicht angezeigt werden sollen.

Wenn mehr als maxGroups für einen einzelnen Tag geplant sind, zeigt CA SDM nur die erste maxGroups-1 an und ersetzt die letzte durch einen "...nn zusätzliche Changes"-Hyperlink, über den der Anwender den Mauszeiger führen oder darauf klicken kann, damit die komplette Liste zu sehen ist. Setzen Sie den Wert auf 0, um die Funktion zu deaktivieren und eine unbegrenzte Anzahl von Events in einer Kalenderzelle zu ermöglichen.

Standard: 4

nday=(n,n...)

Gibt die Auswahlen für die Dropdown-Liste für die n-Tage-Ansicht an.

Die Angabe ist eine Liste von Tageszählungen, die in die Dropdown-Liste aufgenommen werden sollen; die Angabe von 0 bedeutet, dass die n-Tage-Dropdown-Liste vom Ablaufplan ausgeschlossen ist. Der erste angegebene Wert ist der Standard für die Dropdown-Liste.

Standard: (3,7,14,28)

round=(hr,min)|0

Gibt an, ob das Start- und Enddatum des Ablaufplans gerundet werden soll, wenn Changes oder Knowledge-Dokumente in Gruppen zusammengestellt werden. Geben Sie "round=0" an, um das Runden zu deaktivieren.

Standardmäßig gruppiert das Start- und Enddatum des Ablaufplans Objekte. Alle CA SDM-Daten beinhalten eine Uhrzeit, und ohne Auf- bzw. Abrundung befänden sich Objekte mit einem Zeitabstand von weniger als einer Minute in separaten Gruppen. Die Auf- bzw. Abrundung legt die Gruppe nach der Anpassung des Startdatums auf eine frühere Stunde oder Minute und des Enddatums auf eine spätere Stunde oder Minute fest.

Der Wert der Rundung gibt entweder eine Stunde oder eine Minute (aber nicht beide) an. Uhrzeiten werden auf das nächste Vielfache des angegebenen Werts gerundet. Beispiel:

round=(0,15) rundet auf die nächste Viertelstunde auf

round=(0,30) rundet auf die nächste halbe Stunde auf

round=1 rundet auf die nächste Stunde auf

round=12 rundet auf den nächsten halben Tag (12:00 oder 24:00) auf

round=24 rundet auf den nächsten Tag auf

Standard: (0,15)

timefmt=24hr|([am],[pm])

Gibt das Format der Uhrzeiten in den Kalenderansichten des Ablaufplans an.

Der Standardwert 24 St. gibt an, dass die Uhrzeiten im 24-Stunden-Format (0:01 - 23:59) angezeigt werden. Der alternative Wert (am,pm) gibt ein Suffix für Uhrzeiten am Vormittag oder Nachmittag oder für beide an.

Hinweis: Alle schedConfig-Argumente sind optional.

schedAttr-Makro – Gespeichertes Attribut angeben

Das schedAttr-Makro gibt ein Attribut an, das für jedes Element gespeichert wird, welches für die Liste ausgewählt ist. Gespeicherte Attribute stehen für Popup-Infos in der Monatsansicht, für die detaillierten oder zusammenfassenden Informationen in Ansichten außer der Monatsansicht und in der setSchedEvents()-JavaScript-Funktion zur Verfügung. Folgende Werte sind gültige Makroargumente:

attr=xxxx

(Obligatorisch) Gibt ein Attribut aus dem Objekt auf dem Ablaufplan an, z. B. ein Change oder Knowledge-Dokument. Attribute mit Punkten sind zulässig. Der Schlüsselwort-Attributname "CInn" kann auf dem Change-Kalender verwendet werden, um anzugeben, dass die ersten mit dem Change verknüpften *nn*-Cls in die gespeicherten Informationen aufgenommen werden sollen.

Hinweis: Dieses Argument ist das einzige erforderliche Argument für das schedAttr-Makro.

attrRef=.COMMON_NAME|xxxx

Speichert das Attribut der referenzierten Tabelle, die für ein SREL-Attribut gespeichert wird (und für Nicht-SREL-Attribute ignoriert wird). Dem angegebene Attributname muss ein Punkt vorangestellt werden.

Standard: .COMMON_NAME

label=

Zeigt eine Beschriftung für das Attribut auf der n-Tage-Ansicht an.

Standard: der Majic DISPLAY_NAME des Attributs

ident=1|0

Gibt an, ob das Attribut als Kennzeichen für das Objekt fungieren soll (z. B. eine Referenznummer für einen Change). Kennzeichen-Attribute werden ohne eine Bezeichnung vor dem Gruppennamen in Popup-Infos und der n-Tage-Ansicht angezeigt.

Standard: 0

detail=1|0

Gibt an, ob das Attribut in die Detailinformationen aufgenommen wird, die in anderen Ansichten als der Monatsansicht angezeigt werden. Detailinformationen sind die Informationen, die angezeigt werden, wenn das Kontrollkästchen "Nur Zusammenfassung" für die Ansicht nicht aktiviert ist.

Standard: 1

hoverInfo=1|0

Gibt an, ob das Attribut im Popup-Info enthalten ist, welche in der Monatsansicht angezeigt wird, wenn der Mauszeiger über eine Gruppe bewegt wird oder der Benutzer Alt+Pfeil-nach-rechts drückt, wenn der Schwerpunkt auf der Gruppe liegt.

Standard: 0

summary=1|0

Gibt an, ob das Attribut in die Detailinformationen aufgenommen wird, die in anderen Ansichten als der Monatsansicht angezeigt werden. Detailinformationen sind die Informationen, die angezeigt werden, wenn das Kontrollkästchen "Nur Zusammenfassung" für die Ansicht nicht aktiviert ist.

Standard: 0

Hinweis: CA SDM zeigt Attribute in der Zusammenfassungs-, der Detail- oder der Popup-Info in derselben Reihenfolge wie ihre schedAttr-Makros an.

Makro "schedGroup" – Ereignisgruppe angeben

Das schedGroup-Makro gibt den Namen und Farbcodierung einer Gruppe von Elementen an. Die Monatsansicht führt alle Elemente in einer Gruppe in ein einzelnes Ereignis zusammen. Ansichten mit Ausnahme der Monatsansicht zeigen einzelne Elemente im Format für die Gruppe, zu der sie gehören. Folgende optionale Werte sind gültige Makroargumente:

grpname=xxx

(Obligatorisch) Gibt den Namen der Gruppe an. Das Makro weist der Gruppe automatisch eine Zahl zu und weist die Zahl einer JavaScript-Variablen mit einem Namen in der Form schedGroup_xxx zu, wobei xxx der Name der Gruppe ist. Diese Variable kann in der setSchedEvents()-JavaScript-Funktion benutzt werden, um ein der Gruppe angehöriges Ereignis zu erstellen.

Hinweis: Dieses Argument ist das einzige obligatorische Argument für das schedGroup-Makro.

label=xxx

Gibt für die Gruppe eine Bezeichnung an. Falls angegeben, wird die Bezeichnung in allen Ansichten angezeigt.

legend=xxx|0

Zeigt eine Beschreibung der Gruppe für die Legende an, die unten im Ablaufplan angezeigt wird. Gruppen erscheinen in der Legende, wenn mindestens ein Beispiel der Gruppe in der aktuellen Ansicht existiert. Durch die Angabe von 0 wird die Gruppe immer von der Legende ausgeschlossen.

Standard: 0

color=schwarz|Farbe

Gibt die Farbe des Texts in Elementen dieser Gruppe an. Sie können die Farbe im CSS-Format angeben: entweder eine gültige Web-Farbe oder einen Hexadezimalwert mit einem vorangestellten Rautezeichen.

Beispiel: Geben Sie entweder "#FF0000" oder "rot" für Rot ein.

Standard: schwarz

bgcolor=weiß|Farbe

Gibt die Hintergrundfarbe von Elementen dieser Gruppe an. Sie können die Hintergrundfarbe im CSS-Format angeben: entweder eine gültige Web-Farbe oder einen Hexadezimalwert mit einem vorangestellten Rautezeichen.

Beispiel: Geben Sie entweder "#FF0000" oder "rot" für Rot ein.

Standard: weiß.

style=normal|fett|kursiv

Formatiert Text dieser Gruppe normal, fett oder kursiv.

Standard: normal

Die JavaScript-Funktion "setSchedEvents()"

Die JavaScript-Funktion "setSchedEvents()" erstellt Events im Ablaufplan. Ändern Sie diese Funktion, wenn Sie neue Gruppenobjekte anzeigen möchten. Die vordefinierten Gruppenobjekte werden standardmäßig angezeigt.

CA SDM ruft "setSchedEvents()" je einmal für jedes Objekt (Change oder Knowledge-Dokument) auf, das über den Suchfilter des Ablaufplans ausgewählt wurde. Die Funktion erstellt Events für das Objekt durch Aufrufen einer zweiten Funktion, schedEvent() und Weitergeben der Gruppen-ID, des Startdatums und des Enddatum des Event.

Die Funktion kann eine beliebige Anzahl von Events (einschließlich Null) für ein Objekt erstellen. Die Standardfunktion "setSchedEvents()" für den Change-Kalender ("list_chgsched.html") erstellt je ein Event pro Change und gruppiert Changes nach dem Change-Typ. Diese Funktion wird folgendermaßen kodiert:

```
1.      Funktion "setSchedEvents( chg )"  
2.      {  
3.      var grpnum;  
4.      switch( chg["chgtype"] - 0 ) {  
5.          case 100: grpnum = schedGroup_std; break;  
6.          case 300: grpnum = schedGroup_emer; break;  
7.          default: grpnum = schedGroup_norm; break;  
8.      }  
9.      chg. schedEvent (grpnum, chg["sched_start_date"], chg["sched_end_date"]);  
10.     }
```


Der "case"-Parameter gibt die Change-Typ-ID an. Eine Liste der Fall-IDs finden Sie unter Erstellen von Change-Typen.

Die Funktion hat ein einzelnes Argument eines JavaScript-Objekts, das die von schedAttr-Makros angegebenen Attribute enthält. Die "switch"-Anweisung in Zeile 4 bis 8 untersucht das "chgtype"-Attribut des Change und weist die richtige Gruppennummer aus einer der "schedGroup_xxxx"-Variablen zu, die von früheren "schedGroup"-Makros definiert wurden. In Zeile 9 wird die Funktion "schedEvent()" aufgerufen, um ein Event im Ablaufplan zu erstellen, wobei die zuvor zugewiesene Gruppennummer und das Start- und Enddatum für den Ablaufplan übergeben werden. Die Daten sind im Argumentobjekt verfügbar, da sie in früheren schedAttr-Makros angegeben wurden.

Zugreifen auf Export/Import

Das Knowledge-Import-/Export-Tool migriert und synchronisiert Daten zwischen verschiedenen Knowledge Management-Systemen und ermöglicht das Exportieren/Importieren von Knowledge-Dokumenten. Verwenden Sie dieses Tool, um Export-/Importtransaktionen zu definieren

Hinweis: Wenn die Mandantenfähigkeit installiert ist, werden alle Mandantenkategorien und öffentliche Kategorien, die aus einem früheren System importiert wurden, im neuen mandantenfähigen System als öffentlich angezeigt; die importierten Dokumente sind jedoch unter Umständen mandantenspezifisch.

Um auf die KEIT-Seite zuzugreifen, wählen Sie auf der Registerkarte "Administration" die Option "Knowledge" > "Dokumente" > "Export/Import".

Das Dialogfeld "Export/Import" wird mit folgenden Elementen angezeigt:

Exportieren von Transaktionen

Zeigt eine Liste von Exporten an.

Export-/Importvorlagen

Zeigt eine Liste mit Vorlagen an, die Sie bearbeiten können.

Importieren

Zeigt eine Liste von Paketen an, die zum Importieren verfügbar sind.

Importieren von Transaktionen

Zeigt eine Liste von Importen an.

Hinweis: Beim Importieren oder Exportieren von Informationen in die Web-Schnittstelle bzw. aus der Web-Schnittstelle verwendet Knowledge Management die Rolle des Standard-Befehlszeilendienstprogramms und nicht die aktuelle Rolle, mit der der Anwender bei CA SDM angemeldet ist. Die Rolle des Standard-Befehlszeilendienstprogramms wird auf dem Zugriffstyp für den Anwender gesetzt.

So exportieren/importieren Sie Knowledge:

Mit Export-/Importvorlagen können Sie Export-/Importtransaktionen definieren.

Gehen Sie wie folgt vor:

1. Führen Sie eine der folgenden Aktionen aus:
 - Erstellen Sie eine Export-/Importvorlage, um ein Export-Paket zu erstellen.
 - Verwenden Sie eine bestehende Export-/Importvorlage, um ein Export-Paket zu erstellen.
2. Exportieren Sie die Daten zu einem anderen System, indem Sie eine der folgenden Aktionen ausführen:
 - Klicken Sie in der konventionellen Konfiguration auf der Seite Export-/Importvorlage - Detail auf Exportieren.
 - In der Konfiguration für erweiterte Verfügbarkeit können Sie mithilfe der Webschnittstelle keine Pakete vom Anwendungsserver exportieren. Verwenden Sie das Hilfsprogramm "pdm_ket", um Pakete von einem Server zu exportieren.
 - Klicken Sie auf der Seite Exporttransaktion mit der rechten Maustaste auf eine Transaktion, und klicken Sie im Kontextmenü auf Erneut versuchen.
 - [Verwenden des Dienstprogramms "pdm_ket"](#) (siehe Seite 987)

3. Importieren Sie Knowledge-Daten aus dem Paket, indem Sie abhängig von Ihrer CA SDM-Konfiguration eine der folgenden Aktionen durchführen:
 - Kopieren Sie in der konventionellen Konfiguration das gewünschte Knowledge-Paket aus dem Standardverzeichnis "\$NX_ROOT/site/keit/export", und fügen Sie es in das Verzeichnis "\$NX_ROOT/site/keit/import" ein. Klicken Sie auf der Seite Knowledge-Importpakete - Liste mit der rechten Maustaste auf ein Knowledge-Paket, und klicken Sie im Kontextmenü auf Importieren.
 - Kopieren Sie in der Konfiguration für erweiterte Verfügbarkeit das gewünschte Knowledge-Paket aus dem Verzeichnis "*UNC Shared Location*/export", und fügen Sie es in das Verzeichnis "*UNC Shared Location*/import" ein. Sie können Pakete nicht mithilfe der Webschnittstelle aus dem Anwendungsserver importieren, aber Sie können das Hilfsprogramm "pdm_kit" verwenden, um Pakete aus einem Server zu importieren.
 - Kopieren Sie das Knowledge-Paket in eine Ziel-CA SDM-Installation, und platzieren Sie es im Verzeichnis "\$NX_ROOT/site/keit/import".
 - Klicken Sie auf der Seite Knowledge-Importpakete - Liste mit der rechten Maustaste auf ein Knowledge-Paket, und klicken Sie im Kontextmenü auf Importieren.
 - Klicken Sie auf der Seite Importtransaktion mit der rechten Maustaste auf eine Transaktion, und klicken Sie im Kontextmenü auf Erneut versuchen.
 - [Verwenden des Dienstprogramms "pdm_kit_txt"](#) (siehe Seite 988)

Hinweis: Der Knowledge-Paketname muss mit "package_" beginnen, damit er auf der Seite "Knowledge-Import" aufgeführt werden kann.

Wichtig! Das Import-Hilfsprogramm von Version 11,0 wurde in "pdm_kit_txt.exe" umbenannt, so dass auch der Import von Textdateien aus Version 11,0 möglich ist. Dieses Dienstprogramm unterstützt nicht die Importverbesserungen von r12.0.

Weitere Informationen:

[Exportieren/Importieren von Paketen](#) (siehe Seite 978)

Exportieren von Transaktionen

Sie können Transaktionen nach Paket, Vorlage und Status sortieren. Alle KEIT-Transaktionen werden in den folgenden Protokolldateien aufgezeichnet:

stdlog

Zeichnet CA SDM-Informationen auf.

keitstat.log

Stellt statistische Informationen über die KEIT-Vorgänge zur Verfügung

keitinfo.log

Stellt detaillierte Informationen über die KEIT-Vorgänge zur Verfügung.

Hinweis: Wenn die Mandantenfähigkeit installiert ist, zeigt die Listenseite die Einstellungen für Mandant und öffentliche Daten im Suchfilter an. Öffentliche Daten können in Mandantendaten eingeschlossen oder aus diesen ausgeschlossen werden. Es werden ausschließlich öffentliche Objekte gesucht. Wählen Sie auf Detailseiten den geeigneten Mandanten in der Liste aus. Wenn Sie <leer> wählen, ist das Objekt öffentlich.

Die Seite "Transaktionen exportieren" enthält die folgenden Felder:

Paket

Gibt den Namen des Exportpakets an.

Ausführen nach

Zeigt den Anwender an, der den Export ausgeführt hat.

Startzeit

Zeigt die Startzeit der Transaktion an.

Endzeit

Zeigt die Endzeit der Transaktion an.

Dokumentanzahl

Zeigt die Anzahl der exportierten Dokumente an.

Fehleranzahl

Zeigt die Anzahl der fehlgeschlagenen Exporte an.

Fortschritt (%)

Zeigt den Fortschritt der Transaktion an.

Status

Zeigt den Transaktionsstatus an.

Importieren von Transaktionen

Über die Seite "Transaktionen importieren" können Sie Transaktionen nach Paket, Vorlage und Status sortieren, indem Sie auf eine der Spalten klicken.

Hinweis: Wenn die Mandantenfähigkeit installiert ist, zeigt die Listenseite die Einstellungen für Mandant und öffentliche Daten im Suchfilter an. Öffentliche Daten können in Mandantendaten eingeschlossen oder aus diesen ausgeschlossen werden. Es werden ausschließlich öffentliche Objekte gesucht. Wählen Sie auf Detailseiten den geeigneten Mandanten in der Liste aus. Wenn Sie <leer> wählen, ist das Objekt öffentlich.

Die Seite enthält die folgenden Felder:

Paket

Gibt den Namen des Importpakets an.

Ausführen nach

Zeigt den Anwender an, der den Import ausgeführt hat.

Startzeit

Zeigt die Startzeit der Transaktion an.

Endzeit

Zeigt die Endzeit der Transaktion an.

Dokumentanzahl

Zeigt die Anzahl der importierten Dokumente an.

Fehleranzahl

Zeigt die Anzahl der fehlgeschlagenen Importe an.

Fortschritt (%)

Zeigt den Fortschritt der Transaktion an.

Status

Zeigt den Transaktionsstatus an.

Weitere Informationen:

[Anzeigen der Importeinstellungen](#) (siehe Seite 983)

Exportieren/Importieren von Dokumenten

Um Daten zwischen verschiedenen Knowledge Management-Systemen zu migrieren und zu synchronisieren, verwenden Sie das Knowledge-Export-/Import-Tool in der Knowledge-Administration, das Sie Knowledge-Dokumente exportieren und importieren lässt.

Sie können KEIT-Vorlagen erstellen und damit eine Export- und Importtransaktion definieren.

Hinweis: Verwenden Sie das Dienstprogramm "pdm_kit-txt", um r11.0 Knowledge-Daten zu importieren.

Exportieren/Importieren von Paketen

Die folgenden Syntaxnamen exportieren Pakete:

- Servername
- Datum
- Startzeit

In konventioneller Konfiguration können Sie Paketverzeichnisse definieren, indem Sie auf der Registerkarte "Administrator" auf der Seite "Allgemeine Einstellungen" die Option "Pfad Für Knowledge-Import-/Exportdateien" aktualisieren. Standardmäßig wird "\$NX_ROOT/site/keit" verwendet. [Starten Sie die CA SDM-Server neu](#) (siehe Seite 52), nachdem Sie diesen Pfad geändert haben.

Pakete werden in den folgenden Standardverzeichnissen gespeichert:

- Pakete exportieren
\$NX_ROOT/site/keit/export
- Pakete importieren
\$NX_ROOT/site/keit/import

In der Konfiguration für erweiterte Verfügbarkeit können Sie Paketverzeichnisse definieren, indem Sie auf der Registerkarte "Administrator" auf der Seite "Allgemeine Einstellungen" die Option "Pfad Für Knowledge-Import-/Exportdateien" aktualisieren. Dieser Pfad muss ein freigegebenes UNC-Laufwerk sein. [Starten Sie die CA SDM-Server neu](#) (siehe Seite 52), nachdem Sie diesen Pfad geändert haben. Pakete werden in den folgenden Verzeichnissen gespeichert:

- Pakete exportieren
UNC Shared Location/export
- Pakete importieren
UNC Shared Location/import

Um zusätzliche Attribute für die Export-/Importverfügbarkeit hinzuzufügen, können Sie der Datei 'NX.env' die folgenden Attributnamen hinzufügen:

@NX_KEIT_AVAILABLE_FIELDS

Fügt den Attributnamen hinzu.

@NX_KET_ADDL_FIELDS

Fügt den Attributnamen hinzu, und wenn es sich beim neuen Attribut um ein SREL für ein anderes Objekt handelt, fügt es den Attributnamen hinzu, mit dem die Synchronisation zwischen Quell- und Zielsystem erfolgt.

Beispiel: Attribute hinzufügen

```
@NX_KEIT_ADDL_FIELDS = STATUS_ID.STATUS,DOC_TEMPLATE_ID.TEMPLATE_NAME
```

Die Export und Importverzeichnisse enthalten die folgenden Dateien:

keit_config.xml

Enthält die Konfigurationsdatei für ein Export- oder Importpaket.

data.xml

Enthält die Daten-Datei, die Werte der Knowledge-Dokumente enthält.

rep.xml

Enthält die Repositories, auf die in der Datei "data.xml" verwiesen wird.

Bilder

Gibt die Bilddateien an, die in Knowledge-Dokumenten eingebettet werden.

Anzeigen von Export-/Importvorlagen

Die Knowledge-Export-/Import-Tool (KEIT) - Vorlagen werden verwendet, um Export-/Importtransaktionen zu definieren.

Hinweis: Die Standard-Export-/Importvorlage heißt "All-Docs" und enthält kein STATUS_ID-Feld. Mit dieser Vorlage werden die data.xml-Datei erstellt und Dokumente mit Entwurfsstatus importiert. Wenn Sie vor dem Export der All-Docs-Vorlage manuell das STATUS_ID-Feld hinzufügen, wird der ursprüngliche Dokumentstatus beim Import erhalten.

Anzeigen von Knowledge-Export-/Importvorlagen

1. Klicken Sie auf die Registerkarte "Administration".
Die Admin-Konsole wird angezeigt.
2. Klicken Sie auf "Knowledge" > "Dokumente"
Klicken Sie auf "Export/Import" > "Export/Import-Vorlagen"
Die Liste mit den Knowledge-Export-/Importvorlagen wird angezeigt.
3. Klicken Sie auf eine Vorlage in der Spalte "Name".
Die KEIT-Vorlage wird geöffnet.

Hinweis: Sie können Ergebnislisten nach Excel exportieren, um sie außerhalb von CA SDM zu verwenden. Klicken Sie dazu auf der Listenseite auf die Schaltfläche "Exportieren".

Suchen nach Export- und Importvorlagen

Sie können Vorlagen auf der Seite "Knowledge-Export-/Importvorlagen - Einstellungen" suchen

Hinweis: Wenn die Mandantenfähigkeit installiert ist, wählen Sie in der Dropdown-Liste den entsprechenden Mandanten aus. Mit der Option "öffentlich (freigegeben)" wird das Objekt für alle Mandanten erstellt. Eine Dropdown-Liste der Mandanten wird im Suchfilter angezeigt. Wenn Sie in dieser Dropdown-Liste "<leer>" auswählen, ist die Suche öffentlich. Auf der Listenseite wird auch eine Mandantenspalte angezeigt.

Suchen von Knowledge-Export-/Importvorlagen

1. Wählen Sie auf der Registerkarte "Administration" die Option "Knowledge" > "Dokumente" > "Export/Import" > "Export-/Importvorlagen".
Die Liste mit den Knowledge-Export-/Importvorlagen wird angezeigt.
2. Klicken Sie auf "Suchen", und geben Sie Ihre Suchparameter ein.
Das Fenster "Suchergebnisse" wird angezeigt.

3. Klicken Sie auf "Filter anzeigen".
Der Filter wird angezeigt.
4. Ändern Sie Ihre Suche mit den folgenden Optionen:
 - Paket**
Suchen nach Paketnamen.
 - Frühestes Änderungsdatum**
Suchen nach frühestem Änderungsdatum.
 - Spätestes Änderungsdatum**
Suchen nach spätestem Änderungsdatum.
 - Weitere Suchargumente**
Bietet weitere Suchargumente.
Das Fenster "Suchergebnisse" wird angezeigt.
5. Klicken Sie auf eine Vorlage in den Suchergebnissen.
Die Vorlage wird geöffnet.

Erstellen von Export-/Importvorlagen

Sie können Vorlagen auf der Seite "Knowledge-Export-/Importvorlagen - Einstellungen" erstellen und ändern.

So erstellen Sie Knowledge-Export-/Importvorlagen

1. Wählen Sie auf der Registerkarte "Administration" die Option "Knowledge" > "Dokumente" > "Export/Import" > "Export-/Importvorlagen".
Die Liste mit den Knowledge-Export-/Importvorlagen wird angezeigt.
2. Klicken Sie auf "Neu erstellen".
Die Seite "Neue Export-/Importvorlage erstellen" wird angezeigt.
3. Füllen Sie die folgenden Felder aus:
 - Vorlagenname**
Gibt den Namen der Vorlage an.
 - Beschreibung**
Bietet eine kurze Beschreibung der Vorlage.

4. Füllen Sie die entsprechenden Felder in den folgenden Registerkarten aus:

- [Exportfelder](#) (siehe Seite 982)
- [Exportfilter](#) (siehe Seite 983)
- [Importeinstellungen](#) (siehe Seite 983)

Klicken Sie auf "Speichern".

Die Vorlage wird erstellt.

Weitere Informationen:

[Exportieren von Transaktionen](#) (siehe Seite 975)

[Importieren von Transaktionen](#) (siehe Seite 976)

Anzeigen von Exportfeldern

Erstellen Sie eine "Knowledge Export-/Import-Vorlage" (KEIT), um sich Exportfelder anzeigen zu lassen.

Die Registerkarte "Exportfelder" wird mit folgenden Feldern angezeigt:

Verfügbar

Zeigt die Knowledge-Dokument-Felder, die für den Export verfügbar sind.

Hinweis: Wenn Sie den Status der Dokumente (beispielsweise wie "Entwurf") für Import- und Export erhalten wollen, fügen Sie STATUS_ID in die Spalte "Exportiert" ein.

Exportiert

Spezifiziert zu exportierende Dokumentfelder.

Anhänge exportieren

Exportiert Dateianhänge von Knowledge-Dokumenten

Sie können die Pfeile im Bereich "Dokumentattribute auswählen" verwenden, um Dokumentattribute für den Export hinzuzufügen.

Hinweis: Wenn Sie die Export/Import-Vorlagen mit Firefox bearbeiten, ändert sich die Größe der Liste nicht, nachdem Sie die Pfeile in der ersten Bearbeitung verwendet haben. Wenn Sie die Vorlage im Bearbeitungsmodus schließen und wieder öffnen, und wenn sie dann die Pfeile wieder verwenden, wird die Listengröße geändert. Dieses Verhalten tritt nicht auf, wenn Sie Internet Explorer verwenden.

Wichtig! Exportierte Felder in KEIT haben eine höhere Priorität als die Felder, die standardmäßig in der Registerkarte "Importeinstellungen" ausgewählt sind. Wenn Sie auf der Registerkarte "Importeinstellungen" ein Standard-Exportfeld markieren, wird dies nicht als Standardfeld weiterverarbeitet.

Anzeigen des Exportfilters

Erstellen Sie eine "Knowledge Export-/Import-Vorlage" (KEIT), um den Exportfilter anzeigen zu lassen.

Das Dialogfeld "Export/Import" wird mit folgenden Feldern angezeigt:

Kategorie

Öffnet die Seite "Knowledge-Kategorie". Verwenden Sie die Option, um der Liste auf der Registerkarte "Export-Filter" Kategorien hinzuzufügen.

Entfernen einer Kategorie

Entfernen einer Kategorie aus der Liste auf der Registerkarte "Export-Filter".

Kategorie löschen

Löscht die Kategorie aus der Liste auf der Registerkarte "Export-Filter".

Untergeordnete Kategorien einschließen

Exportiert Dokumente aus untergeordneten Kategorien von exportierten Kategorien.

Sekundäre Kategorien einschließen

Exportiert sekundäre Kategorien von exportierten Dokumenten.

Alle Dokumente, die mit der ausgewählten Kategorie verknüpft sind, einschließen

Exportiert alle Dokumente, die mit der ausgewählten Kategorie verknüpft sind.

Hinweis: Ist nur aktiviert, wenn Sie die Option "Sekundäre Kategorien einschließen" gewählt haben.

Zusätzlicher Filter

Eine zusätzliche WHERE-Klausel wird zur Verfügung gestellt.

Anzeigen der Importeinstellungen

Erstellen Sie eine "Knowledge Export-/Import-Vorlage" (KEIT), um sich Importeinstellungen anzeigen zu lassen.

Die Registerkarte "Importeinstellungen" wird mit folgenden Feldern angezeigt:

Grenzwert für Fehler (%):

Hält den Importvorgang an (setzt den Status auf "Fehlgeschlagen"), wenn der Fehler-Prozentsatz die spezifizierte Zahl überschreitet.

Veröffentlichte Dokumente überschreiben

Ermöglicht, dass importierte Dokumente veröffentlichte Dokumente auf dem CA SDM-Server überschreiben.

Dokumente überschreiben, die nicht den Status "Veröffentlicht" aufweisen

Ermöglicht, dass importierte Dokumente nicht-veröffentlichte Dokumente auf dem CA SDM-Server überschreiben.

Beim Überschreiben von Dokumenten Standardwerte verwenden

Verwendet Standardwerte für definierte Felder in überschriebenen Dokumenten.

Dokumente sofort indizieren

Indiziert das Dokument nach dem Importprozess.

Status

Wählen Sie "Entwurf", "Veröffentlicht" oder "Deaktiviert".

Priorität

Legt die Prioritätsstufe der Importeinstellungen fest.

Vorlage

Wählt eine der folgenden Standardvorlagen

- Integriert - Knowledge-Dokument
- Integriert - Knowledge-Baumstruktur
- Integriert - Schnellbearbeitung

Eigentümer

Ermöglicht Ihnen, den Eigentümer durch Öffnen der Seite "Kontakt - Suche" zu setzen.

Author

Ermöglicht Ihnen, den Autor durch Öffnen der Seite "Kontakt - Suche" zu setzen.

Experte

Ermöglicht Ihnen, den Experten durch Öffnen der Seite "Kontakt - Suche" zu setzen.

Verantwortlicher

Ermöglicht Ihnen, den Zuständigen durch Öffnen der Seite "Kontakt - Suche" zu setzen.

Ablaufdatum

Öffnet die Datumshilfe.

Prüfungsdatum

Öffnet die Datumshilfe.

Produkt-ID

Ermöglicht Ihnen, die Produkt-ID durch Öffnen der Seite "Kontakt - Suche" zu setzen.

Asset

Öffnet die Seite "Configuration Item - Suche".

Ursache

Öffnet die Seite "Ursachen - Suche".

Service Desk-Priorität

Legt die Service Desk-Priorität der Importeinstellungen fest.

Relevanz

Legt die Relevanz der Importeinstellungen fest.

Impact

Legt den Auswirkungsgrad der Importeinstellungen fest.

Urgency

Legt die Dringlichkeitsstufe der Importeinstellungen fest.

Bearbeiten von Export-/Importvorlagen

Sie können Export- und Importvorlagen auf der Seiten "Knowledge-Export-/Importvorlagen" bearbeiten.

Bearbeiten einer Export-/Importvorlage

1. Navigieren Sie zu "Knowledge" > "Dokumente" > "Export/Import" > "Export/Import-Vorlagen".

Die Liste mit den Knowledge-Export-/Importvorlagen wird angezeigt.

2. Wählen Sie eine Vorlage aus.

Die Seite "Vorlagen-Detail" wird angezeigt.

3. Klicken Sie auf "Bearbeiten".

Bearbeiten Sie die entsprechenden Felder:

Vorlagenname

Gibt den Namen der Vorlage an.

Beschreibung

Bietet eine kurze Beschreibung der Vorlage.

4. Ändern Sie die entsprechenden Felder in den folgenden Registerkarten:

- [Exportfelder](#) (siehe Seite 982)
- [Exportfilter](#) (siehe Seite 983)
- [Importeinstellungen](#) (siehe Seite 983)

5. Klicken Sie auf "Speichern".

Ihre Änderungen werden gespeichert.

Weitere Informationen:

[Importieren von Transaktionen](#) (siehe Seite 976)

Hilfsprogramm "pdm_ket": Knowledge-Export-Tool

Das Hilfsprogramm "pdm_ket" exportiert Knowledge von einem Quellcomputer in ein Knowledge-Paket. Der Export basiert auf einer Vorlage, die in der Web-Schnittstelle erstellt wurde.

Anhänge und die entsprechenden Links werden während des Exports nach "data.xml" exportiert. Bevor Sie die Anhänge importieren, verschieben Sie diese manuell in das folgende Verzeichnis auf dem Hintergrundserver:

\$NX_ROOT/site/attachments/default

Hinweis: Für die Konfiguration für erweiterte Verfügbarkeit können Sie das Hilfsprogramm "pdm_ket" ausführen, indem Sie den UNC-Pfad der Anhänge verwenden.

Mit diesem Hilfsprogramm haben Sie die folgenden Möglichkeiten:

- Erstellen Sie die Konfigurationsdatei auf der Grundlage der entsprechenden Knowledge-Exportvorlage.
- Exporten Sie die Daten mit der UUID des Dokuments und den Inhalt, wie z. B. Titel, Zusammenfassung, Problem, Behebung und andere Dokumentattribute, wie Eigentümer, Status usw.
- Exportieren Sie alle eindeutigen von den exportierten Dokumenten verwendeten Bilder (diese müssen immer exportiert werden).
- Exportieren Sie alle eindeutigen von den exportierten Dokumenten verwendeten Anhänge (Feld EXP_ATTMNT).

Die Dateien werden von einer Remote-Repository in den lokalen Paketordner kopiert.

Das Dienstprogramm rufen Sie wie folgt auf:

```
pdm_ket -n <template name> [-h] ]-v]
```

-n <template name>

Definiert den Namen der für den Export verwendeten Vorlage (Groß-/Kleinschreibung beachten).

-h

(Optional) Zeigt Hilfe zum Hilfsprogramm an.

-v

(Optional) Aktiviert eine umfassende Protokollierung (bop_logging) von programmspezifischen Events. Diese Option wird in der Regel zum Beheben von internen Problemen verwendet.

Beispiel: Verwendung von "pdm_ket", um Knowledge mit der Vorlage "my_template" zu exportieren.

```
pdm_ket -n my_template
```

Das Hilfsprogramm "pdm_ket" kann mit einem Planungsmodul eines Drittanbieters für das Exportieren von Dokumenten konfiguriert werden.

Hilfsprogramm "pdm_kit": Knowledge- Import-Tool

Das Hilfsprogramm "pdm_kit" importiert Daten zum Zielsystem, gemäß den Einstellungen in der Konfigurationsdatei eines Pakets.

Wichtig! Bevor Sie das pdm_kit-Hilfsprogramm vom Anwendungsserver ausführen, stellen Sie sicher, dass auf den Pfad (Lokal oder UNC) des Pakets vom Hintergrundserver zugegriffen werden kann. Wenn der Hintergrundserver nicht auf diesen Pfad zugreifen kann, wird das Paket nicht vom Anwendungsserver importiert.

Wichtig! Das Import-Hilfsprogramm von Version 11.0 wurde in "pdm_kit_txt.exe" umbenannt, so dass auch der Import von Textdateien aus Version 11.0 möglich ist. Dieses Hilfsprogramm unterstützt nicht die Importverbesserungen von Version 12.9.

Die Daten, die früher mit dem Hilfsprogramm "pdm_ket" verknüpft wurden, erhalten den tatsächlichen UUID- oder ID-Wert des Zielsystems. Wenn man das Hilfsprogramm "pdm_kit" ausführt, wird ein neuer userid-Parameter angewandt. Das Hilfsprogramm "pdm_kit" funktioniert folgendermaßen:

1. Das Hilfsprogramm importiert Dokumente, indem der Wert der Anwender-ID (für Kontakte) oder der verknüpfte Name (für Felder wie Asset) mit einer geeigneten UUID des Zielsystems ersetzt wird.
2. Import von Bildern
3. Import von Anhängen
4. Export von Dateien vom lokalen Paketordner zu Remote-Repositorys

Hinweis: Wenn das Bearbeiten von öffentlichen Dokumenten nicht möglich ist, wird das importierte Dokument als Überarbeitungsversion erstellt.

Das Dienstprogramm rufen Sie wie folgt auf:

```
pdm_kit [-h] -f -u [-v]
```

-h

(Optional) Zeigt in der Schnittstelle eine Hilfe zum Hilfsprogramm an.

-f

Gibt den Pfad zum Paket an.

-u

Gibt den Standardanwender an.

-v

(Optional) Aktiviert eine umfassende Protokollierung (bop_logging) von programmspezifischen Events. Diese Option wird in der Regel zum Beheben von internen Problemen verwendet.

Hinweis: Für die Konfiguration für erweiterte Verfügbarkeit können Sie das Hilfsprogramm "pdm_kit" auf dem Hintergrundserver ausführen. Unter Windows können Sie das Hilfsprogramm "pdm_kit" auch auf einem Anwendungsserver ausführen, wenn sich das Paket auf einem gemeinsamen UNC-Laufwerk befindet. Auf einer Plattform (nicht Windows) können Sie das Hilfsprogramm "pdm_kit" nicht auf einem Anwendungsserver ausführen.

Beispiel: Verwenden von "pdm_kit" für den Import eines Pakets

```
pdm_kit -f c:\package_path -u ServiceDesk
```

Exportieren oder Importieren von Knowledge durch Benutzer

Sie können Analysten den Export und den Import erlauben, indem Sie Ihre Rollenliste auf der Registerkarte "Administration" verwalten.

So erteilen Sie Export-/Importberechtigungen

1. Navigieren Sie zu "Sicherheits- und Rollenmanagement" > "Rollenmanagement" > "Rollenliste".

Die Rollenliste wird angezeigt.

2. Wählen Sie eine Rolle vom Schnittstellentyp "Analyst" aus.

Die Seite "Rolle - Detail" wird angezeigt.

3. Klicken Sie auf "Bearbeiten".

Die Seite "Rolle aktualisieren" wird angezeigt.

4. Klicken Sie auf die Registerkarte "Knowledge".

Führen Sie eine der folgenden Aktionen aus:

- Aktivieren Sie das Kontrollkästchen "Export zulassen".
- Aktivieren Sie das Kontrollkästchen "Import zulassen".
- Aktivieren Sie beide Kontrollkästchen.

5. Klicken Sie auf "Speichern".
Die Seite "Rolle - Detail" wird wieder geöffnet.
6. Überprüfen Sie Ihre Änderungen in der Registerkarte "Knowledge".
Die Seite "Rolle - Detail" wird geschlossen.

Sie können Benutzern das Exportieren und Importieren auch untersagen, indem Sie die Kontrollkästchen auf der Registerkarte "Knowledge" der Seite "Rolle - Detail" deaktivieren.

Webservices

Auf Knowledge kann über SOAP-Webservices zugegriffen werden. Dabei stehen verschiedenen Optionen zur Verfügung, die die Suche, den Abruf, die Erstellung und die Aktualisierung von Dokumenten sowie eine ganze Reihe weiterer Vorgänge ermöglichen.

Hinweis: Weitere Informationen zu SOAP-Webservices finden Sie im *Implementierungshandbuch*.

Kapitel 23: Verwalten von Knowledge Management

Dieses Kapitel enthält folgende Themen:

[Knowledge-Verwaltung](#) (siehe Seite 991)

[Suchen von Prozeduren für die Knowledge-Administration](#) (siehe Seite 992)

[Rollen und Funktionen von Knowledge Management](#) (siehe Seite 992)

[So verwalten Sie Rollenberechtigungen und die Dokumentsichtbarkeit:](#) (siehe Seite 1004)

[Aktionsinhalte](#) (siehe Seite 1004)

[Genehmigungsvorgang für Dokumente](#) (siehe Seite 1010)

[Automatisierungsrichtlinien](#) (siehe Seite 1018)

[Knowledge-Dokumentsteuerung](#) (siehe Seite 1023)

[Knowledge Management-Systemeinstellungen](#) (siehe Seite 1083)

Knowledge-Verwaltung

Sie können Verwaltungseinstellungen für Knowledge Management konfigurieren. Sie können [Self-Service-Knowledge-Optionen](#) (siehe Seite 995) konfigurieren, um den Anforderungen der Anwender zu entsprechen und um eine produktive Umgebung für die Verwaltung und Bereitstellung von Wissen zu schaffen. Auf der Registerkarte "Administration" können Sie Systemoptionen festlegen. Sie können Knowledge-Berechtigungen in Abhängigkeit von der Gruppenzugehörigkeit und Rolle eines Kontakts festlegen. Sie können Einstellungen festlegen, um die Funktionen und die Verwendung von Knowledge Management zu bestätigen.

Wichtig! Die Neuindizierung von Dokumenten in der Knowledge Base sowie die Ausführung der Berechnung für Automatisierungsrichtlinien und die Ausführung der Knowledge-Berichtskarte kann zeitaufwändig sein. Es wird deshalb empfohlen, diese Vorgänge nicht während der Geschäftszeiten auszuführen bzw. dann auszuführen, wenn Ihr System nicht sehr ausgelastet ist.

Suchen von Prozeduren für die Knowledge-Administration

Mit CA SDM können Sie die Knowledge-Administration schrittweise konfigurieren. Weitere Information dazu finden Sie in diesem Handbuch und in der *Online-Hilfe*.

So finden Sie schrittweise Prozeduren zur Knowledge-Administration in der *Online-Hilfe*:

1. Melden Sie sich bei CA SDM an.
Die Hauptseite von CA SDM wird angezeigt.
2. Führen Sie eine der folgenden Aktionen aus:
 - Klicken Sie im Hauptmenü auf "Hilfe" > "Hilfe" und navigieren Sie in der *Online-Hilfe* zu "Administration" > "Knowledge-Administration".
Die Hilfethemen zu "Knowledge-Administration" erscheinen, und Sie können darin navigieren, um die benötigten Informationen zu suchen.
 - Klicken Sie im Hauptmenü auf "Hilfe" > "Hilfe zu diesem Fenster".
Die *Online-Hilfe* wird mit einem Hilfethema für die gewünschte Seite angezeigt.

Rollen und Funktionen von Knowledge Management

Knowledge Management ist für verschiedenste Anwender konzipiert, von Systemadministratoren und Knowledge Managern, die das Produkt pflegen, bis hin zu Kunden und Mitarbeitern, die das System nutzen, um Lösungen für ihre Probleme zu finden. Obwohl eine Person mehrere Rollen innehaben kann, sind die folgenden Rollen die grundlegenden in Knowledge Management verfügbaren Anwenderrollen:

- **Kunde:** Ein externer Endanwender, der grundlegende Self-Service-Aufgaben ausführt.
- **Mitarbeiter:** Ein interner Endanwender, der grundlegende Self-Service-Aufgaben ausführt.
- **Knowledge-Analyst:** Ein Anwender, der für einen oder mehrere Schritte innerhalb des Knowledge Managements verantwortlich ist. Dieser Anwender interagiert mit Service Desk-Analysten, um eine Datenbank mit relevanten Lösungsvorschlägen zu verwalten.
- **Knowledge Manager:** Ein Supervisor des Knowledge-Analysten. Diese Rolle steuert die Neuzuweisung und Eskalation von Knowledge-Dokumenten. Ebenso verwaltet sie im Tagesgeschäft die administrativen Aspekte von Lösungen, wie z. B. das Erstellen der Kategoriestruktur, die Definition des Genehmigungsvorgangs, das Verwalten von Füllwörtern, spezielle Terminologie, Synonyme sowie andere Einstellungen und Optionen, die dynamischer als das sind, was der Knowledge Management-Administrator steuert.

- **Administrator:** Der Administrator, der innerhalb einer einzelnen Rolle Zugriff auf alle Funktionen in CA SDM- und Knowledge Management-Produkten hat. Diese Rolle kommt für gewöhnlich dann zur Anwendung, wenn CA SDM implementiert wird und sicher gestellt werden muss, dass alle Anwender und Rollen richtig eingerichtet werden. Sie kommt auch dann zur Anwendung, wenn es sich um eine <USDK-Umgebung handelt, in der eine einzelne Person alle Administrationsaufgaben wahrnimmt.
- **Knowledge Management-Administrator:** Ein Administrator, der dafür verantwortlich ist, den Knowledge-Management-Prozess zu konfigurieren und zu überwachen. Zu den Aufgaben dieser Rolle gehören auch das Erstellen der Kategoriestructur, die Definition des Genehmigungsvorgangs sowie die Konfiguration der Standardeinstellungen für Suchen und Sicherheit.

Jeder Rolle in der CA SDM-Umgebung ist eine bestimmte Zugriffsebene zugeordnet. Diese Ebenen helfen dabei, die Aufgaben zu definieren, die jede Rolle erfüllt.

Weitere Informationen:

[Knowledge Management-Benutzeroberflächen](#) (siehe Seite 993)

[Konfiguration und Verwaltungsfunktionen von Knowledge Management](#) (siehe Seite 994)

[Optionen für Self-Service-Knowledge](#) (siehe Seite 995)

[Dokumente und Anwender](#) (siehe Seite 1000)

[So verwalten Sie Rollenberechtigungen und die Dokumentsichtbarkeit:](#) (siehe Seite 1004)

Knowledge Management-Benutzeroberflächen

Die folgenden Benutzeroberflächen helfen Ihnen, Knowledge zu verwalten:

- **Self-Service** - In der Self-Service-Schnittstelle können Kunden und Mitarbeiter, die CA SDM verwenden, auf Knowledge-Dokumente zugreifen und Knowledge für die spätere Nutzung absenden. Kunden können Knowledge-Dokumente suchen, durchsuchen oder mit Hilfe von Lesezeichen markieren und anzeigen.
- **Knowledge-Dokumente** - In der Schnittstelle 'Knowledge-Dokumente', die über den Knoten 'Knowledge-Dokumente' im CA SDM-Scoreboard zugänglich ist, können alle Benutzer des Systems ihren Posteingang anzeigen und Kommentare verfolgen. Der *Administrator* verwaltet die nicht zugewiesenen/nicht indizierten Dokumente der Benutzer sowie die automatisierten Richtlinien für den Dokumentlebenszyklus und die Benutzerforen.

- **Knowledge Management** - In der Schnittstelle 'Knowledge Management', die über die Registerkarte 'Knowledge' in CA SDM zugänglich ist, können *Knowledge-Analysten* und *Knowledge-Manager* Knowledge finden, organisieren und veröffentlichen. Außerdem können die angezeigten Dokumente mithilfe von erweiterten Optionen gefiltert werden. Die Ergebnisse können nach Relevanz, Änderungsdatum und vielem mehr sortiert werden.
- **Knowledge-Verwaltung** - In der Schnittstelle 'Knowledge-Verwaltung', die über den Knoten 'Knowledge' auf der CA SDM-Registerkarte 'Verwaltung' zugänglich ist, können *Administratoren*, *Knowledge-Manager* und *Knowledge Management-Administratoren* Systemoptionen festlegen. Einstellungen können dabei helfen, die Funktionalität und Verwendung von Knowledge Management anzupassen.

Konfiguration und Verwaltungsfunktionen von Knowledge Management

Sie können in Knowledge Management die folgenden Konfigurations- und Verwaltungsfunktionen ausführen:

- Erstellen von "Aktionsinhalten" (eine aktive Aktions-URL), die Sie in das Lösungsfeld eines Dokuments einfügen können.
- Einrichten des Genehmigungsvorgangs und Definieren des Knowledge-Dokument-Lebenszyklus.
- Einrichten von automatisierten Richtlinien für bestimmte Aufgaben im Genehmigungsvorgang für Knowledge-Dokumente.
- Einrichten von Dokumentoptionen in Bezug auf Kommentare, das Absenden von Knowledge, Vorlagen und Dokumenteinstellungen.
- Erstellen von Vorlagen zur Steuerung des Layouts von Dokumentinformationen.
- Verwalten der standardmäßigen Knowledge Management-Suchmaschine und Konfiguration von Füllwörtern, spezieller Terminologie sowie von Synonymen, die bei Suchvorgängen basierend auf Schlüsselwörtern und basierend auf natürlicher Sprache verwendet werden.
- Erstellen Sie "empfohlene Dokumente", die in der Self-Service-Schnittstelle angezeigt werden, wenn Anwender nach Knowledge-Lösungen suchen.
- Verwalten der Struktur der Knowledge-Kategorien, um den Zugriff auf Dokumente zu erleichtern.
- Einrichten der Knowledge-Berichtskarte und allgemeiner Systemeinstellungen.
- Definition von Umfragen, die Kundenfeedback über die Nützlichkeit von Knowledge-Dokumenten sammeln und analysieren.
- Verwalten der Integration von Knowledge Management in CA SDM, einschließlich Feldzuordnung und Suchkonfiguration für Requests und Issues.

Optionen für Self-Service-Knowledge

Kunden und Mitarbeiter, die CA SDM verwenden, haben über die Self-Service-Schnittstelle Zugriff auf Knowledge-Dokumente. Kunden können Knowledge-Dokumente suchen, durchsuchen oder mit Hilfe von Lesezeichen markieren und anzeigen. Durch den Zugriff auf diese Dokumente und Services können Kunden selbst Antworten finden, und die Auslastung der Ressourcen in Ihrer Organisation wird dadurch reduziert.

In der Self-Service-Benutzerschnittstelle können Mitarbeiter und Kunden die folgenden Knowledge-Lösungsoptionen anzeigen:

- **Suchen von Knowledge-Lösungen** - Mitarbeiter und Kunden können Schlüsselwörter und Wortfolgen in einem Suchfeld eingeben, um eine Liste von Knowledge-Lösungen abzurufen. Sie können diese Option hier konfigurieren: 'Verwaltung', 'Knowledge', 'Suche', 'Sucheinstellungen'.
- **Beste Lösungen anzeigen** - Mitarbeiter und Kunden können eine Liste der besten Lösungen in der Self-Service-Schnittstelle anzeigen. Die folgende Administrator-Einstellung bestimmt die Anzahl der anzuzeigenden Dokumente: 'Verwaltung', 'Knowledge', 'System', 'Allgemeine Einstellungen', 'Beste Lösungen - Anzuzeigende Anzahl der Dokumente'.
- **Eingabeaufforderung für Knowledge-Umfrage** - Nach dem Öffnen eines Knowledge-Dokuments kann der Benutzer das Dokument lesen und hat Zugriff auf eine Reihe von Umfragefunktionen. Eine dieser Funktionen besteht in der Möglichkeit anzugeben, ob Kunden meinen, dass ihr Problem behoben sei. Sie können diese Option hier konfigurieren: 'Verwaltung', 'Knowledge', 'Lösungsumfrage', 'Umfrageeinstellungen'.
- **Knowledge vorschlagen** - Mitarbeiter und Kunden können (mit entsprechender Berechtigung) eine Liste der Knowledge-Vorschläge abrufen, wenn sie ein neues Ticket in der Self-Service-Schnittstelle erstellen. Sie können diese Option hier konfigurieren: 'Verwaltung', 'Knowledge', 'Service Desk-Integration', 'Knowledge vorschlagen'.

Erweiterte Suche

In den erweiterten Sucheinstellungen können Kunden und Angestellte die folgenden Optionen verwenden, um eine Problemlösungssuche zu verfeinern:

Knowledge Management-Suche

Sucht nach bestimmten Schlüsselwörtern, die vorläufige Übereinstimmungen darstellen.

Suche in natürlicher Sprache

Sucht nach Wörtern und berücksichtigt Wortnähe, Wortstellung und Relevanz.

Die Suchergebnisse werden nach Relevanz aufgelistet. Die Relevanz wird durch die angegebenen Suchkriterien bestimmt (als AUSGEZEICHNET, GUT usw. ausgedrückt). Dokumente mit der höchsten Relevanz (SEHR GUT) sind zuerst aufgeführt.

Jedes Ergebnis verfügt möglicherweise über einen als eine Verknüpfung angezeigten Titel, eine Zusammenfassung des Dokuments sowie zusätzliche Statistiken, die für das Dokument relevant sind, wie z. B. die Relevanzbewertung, die Dokument-ID, das Änderungsdatum, die FAQ-Einstufung und die Anzahl der erhaltenen Treffer.

Je nachdem, wie der Systemadministrator Knowledge Management konfiguriert hat, können Anwender einen Incident öffnen, ein Dokument bewerten oder kommentieren, wenn ein Knowledge-Dokument offen ist.

Informationen über Knowledge-Dokumente

Jedes Knowledge-Dokument enthält wichtige, informative Dokumentfelder. In Abhängigkeit von der verwendeten Dokumentvorlage können unterschiedliche Felder bzw. Felder unterschiedlich angezeigt werden.

Ein Titel identifiziert das Dokument. Das Dokument enthält darüber hinaus die folgenden Informationen:

Übersicht

Fass das Dokument zusammen und beschreibt kurz das Problem.

Problem

Beschreibt das Problem.

Lösung

Beschreibt, wie das Problem im Nur-Text- oder HTML-Format zu lösen ist.

Siehe auch:

Listet Dokumente auf, die sich auf das aktuelle Dokument beziehen. Wenn Sie auf einen Dokument-Hyperlink klicken, wird das entsprechende Dokument in einer neuen Seite angezeigt.

Anhänge

Listet die Dateien auf, die dem Dokument angehängt werden und heruntergeladen werden können. Anhänge bieten ergänzende Informationen zum Dokument.

Verwandte Kategorien

Listet die Kategorien auf, die sich auf das Dokument beziehen. Wenn Sie auf einen Kategorie-Hyperlink klicken, wird die Seite 'Suchwerkzeuge' aktualisiert und die entsprechende Kategorie angezeigt.

Zugehörige Tickets

Stellt eine Verknüpfung zu Anfragen, Incidents, Problemen, Issues und Dokumenten her, die aufgrund des Dokuments geöffnet wurden oder mit Hilfe des Dokuments gelöst wurden.

Eigenschaften

Zeigt zusätzliche Dokumenteigenschaften an, die in der Dokumentvorlage ausgewählt wurden. Standardmäßig werden das Änderungsdatum und die Dokument-ID angezeigt.

Kommentare

Listet Benutzerkommentare für das Dokument auf. Jeder Kommentar enthält den Kontaktnamen, die E-Mail-Adresse und das Datum.

Bewertung & Kommentar

Bietet weitere Kommentare und Feedback darüber, ob das Dokument bei der Beantwortung Ihrer Frage hilfreich war. Ermöglicht Ihnen, auf Grundlage der folgenden Fragen die Nützlichkeit des Dokuments zu bewerten:

- Hat dieses Dokument zur Lösung des Problems beigetragen?
- Wie hilfreich war dieses Forum?

Sie können auch einen Kommentar hinzufügen und einem anderen Analysten zur Nachverfolgung zuweisen, indem Sie einen der folgenden Kommentartypen verwenden:

- Fehlerhafte Verknüpfung
- Für Veröffentlichung vorgeschlagen
- Für Deaktivierung vorgeschlagen
- Falsche Informationen
- Fehlende Informationen
- Neuen Inhalt empfehlen
- Überprüfung
- Lösung funktioniert nicht

Der Abschnitt 'Seitenoptionen' bietet mehrere mögliche Aktionen:

- Bearbeiten
- Lesezeichen hinzufügen/entfernen
- Abonnieren
- Bewertung & Kommentar

- E-Mail
- Neues Forum
- Neuer Incident
- Neuer Incident auf Grundlage dieses Dokuments
- Druckbare Version

Weitere Informationen:

[Erstellen von Kommentartypen](#) (siehe Seite 1025)

[Konfigurieren von Self-Service-Richtlinien](#) (siehe Seite 1079)

Ankündigungen

Ankündigungen sind eine schnelle Möglichkeit, Lösungen für ein Problem bereitzustellen. Sie dienen dazu, Lösungen für ein weit verbreitetes Problem bereitzustellen und Anrufe beim Service Desk erfolgreich zu beantworten.

Aktuelle Ankündigungen werden im rechten Fensterbereich des CA SDM-Hauptfensters angezeigt, wenn Sie sich das erste Mal beim System anmelden.

Sortieren von Dokumenten

Sie können Dokumente in verschiedener Reihenfolge sortieren.

So sortieren Sie Dokumente:

1. Wählen Sie auf der Registerkarte "Knowledge" - einen Strukturknoten aus der Liste "Kategorie" im linken Fenster aus.
2. Erweitern Sie den Knoten und klicken Sie auf eine Kategorie.
Die Seite "Dokument - Liste" wird angezeigt.
3. Sortieren Sie die Dokumente, indem Sie die Option "Ordnen nach" verwenden.

- FAQ-Einstufung
- Anzahl der Treffer
- Recently modified documents
- Lösungsanzahl

Die Dokumente werden in der von Ihnen gewählten Reihenfolge aufgelistet.

Durchsuchen von Dokumenten

Sie können Knowledge-Dokumente kategorisieren, um Kunden auf Grundlage häufig gestellter Fragen (FAQs) nach Informationen suchen zu lassen. Durch Auswählen einer Knowledge-Kategorie werden verwandte Unterkategorien und Knowledge-Dokumente angezeigt. Sie können das gewünschte Dokument auswählen oder eine Unterkategorie auswählen, um Ihre Suche weiter einzuengen.

Zur Verbesserung der Self-Service-Funktionalität wird eine dynamisch erstellte Liste häufig verwendeter Dokumente angezeigt.

Hinweis: Benutzer können Kriterien zu relevanten Elementen eingeben. Die Such-Engine sucht die passenden Knowledge-Dokumente und zeigt diese auf der Seite "Suchergebnisse" als Gruppe von Verknüpfungen unter dem Titel "Empfohlene Dokumente" an. Die Suchanfrage kann als ein Schlüsselwort oder durch mehrere Wörter (Wortfolge) ausgedrückt werden, die das gewünschte Konzept definieren, das ein oder mehrere Dokumente enthalten können. Weitere Informationen dazu finden Sie unter [Erstellen neuer empfohlener Dokumente](#) (siehe Seite 1066).

Erstellen von Lesezeichen für Dokumente

Sie können Lesezeichen für Dokumente erstellen, auf die häufig zugegriffen wird. Nachdem für ein Dokument ein Lesezeichen erstellt wurde, wird es der Liste "Lesezeichen" hinzugefügt. Diese Liste hilft Ihnen, häufig verwendete Dokumente schnell zu finden. Nachdem Sie ein Dokument einer Lesezeichenliste hinzugefügt haben, wird im Feld "Lesezeichen" die Schaltfläche "Entfernen" angezeigt. Sie können Lesezeichen aus dieser Liste entfernen, wenn nicht mehr häufig auf diese zugegriffen wird.

Im Ordner "Eigene Lesezeichen" werden Verknüpfungen zu den am häufigsten verwendeten Dokumenten gespeichert. Wenn Sie auf der Registerkarte "Knowledge" im Bereich "Kategorie" auf "Meine Lesezeichen" klicken, werden die mit Lesezeichen versehenen Dokumente im Bereich "Knowledge-Dokument – Liste" angezeigt.

Incidents und Probleme

Häufig treten Probleme auf, die nicht einfach durch das Suchen von Knowledge gelöst werden können. Nicht zu allen Problemen gibt es eine direkte Lösung in der Knowledge Base. Wenn ein Kunde ein Problem hat, das nicht gelöst werden kann, kann dieser einen Incident erstellen, der für die weitere Bearbeitung zu einem Analysten gesendet wird. Der Incident, der auch auf einem vorhandenen Knowledge-Dokument beruhen kann, beschreibt das Problem. Je mehr Informationen ein Incident enthält, desto einfacher ist es für den Analysten, das Problem zu lösen.

Viele ITIL-definierte Aktivitäten werden von Knowledge Management unterstützt, so z. B.:

- Vorfallverwaltung
 - Die Knowledge-Suche kann dazu verwendet werden, bei der weiteren Incident-Untersuchung und -diagnose bekannte Fehler zu finden.
 - Incident-Kategorisierung
- Problemverwaltung
 - Zugriff auf Informationen über bekannte Fehler und Unterstützung bei der Problemzuordnung, um eine Lösung zu finden, wenn das Problem bereits früher auftrat.
 - Pflege von und Zugriff auf Informationen zur Problemumgehung
 - Aufzeichnen von Informationen über Prozeduren, Arbeitsanweisungen, Diagnose-Skripts und bekannte Fehler (bei gleichzeitiger Unterstützung von reichhaltigen Inhalten, Bearbeitungs-Tools, Messungen und definierbaren Genehmigungsvorgängen für die Lösungsentwicklung)
 - Problemanalyse (über die Verknüpfung und Analyse von Incidents)

Dokumente und Anwender

In der Schnittstelle "Knowledge-Dokumente", die über den Knoten "Knowledge-Dokumente" im USDK>-Scoreboard zugänglich ist, können alle Anwender des Systems ihren Posteingang anzeigen und Kommentare verfolgen. Der Administrator verwaltet die nicht zugewiesenen/nicht indizierten Dokumente der Anwender sowie die automatisierten Richtlinien für den Dokumentlebenszyklus und die Anwenderforen.

Dokument-Posteingang

Der Knowledge-Dokument-Posteingang (und der Gruppen-Posteingang) im CA SDM-Scoreboard enthält die Dokumente, die Ihnen oder Ihrer Gruppe zugewiesen wurden. Dies ist das zentrale Repository für Dokumente mit allen Statusangaben (auch für gespeicherte und zugewiesene Entwurfs- und Überarbeitungsdokumente).

Der Posteingang ist der Ablagekorb für Ihre täglichen Aufgaben und ein wichtiges Tool zum Verwalten des Genehmigungsprozesses. Wenn ein Dokument erstellt oder aktualisiert wird, wird es im Posteingang des Eigentümers platziert. Beim Veröffentlichen erfordern Elemente im Posteingang die Aufmerksamkeit des Anwenders. Elemente im Posteingang können erst nach ihrer Veröffentlichung als Lösungen angezeigt und der Knowledge Base hinzugefügt werden. Prüfen Sie regelmäßig Ihren Posteingang auf neue Dokumente.

Anzeigen von Nachverfolgungskomentaren

Die Posteingang für Nachbearbeitungskommentare im CA SDM-Knowledge-Dokument-Scoreboard enthält die Kommentare, die Ihnen oder Ihrer Gruppe zugewiesen wurden.

Zusammenfassungen der Ihnen zugewiesenen Nachverfolgungskommentare können Sie auf der Seite "Kommentar – Liste" anzeigen.

Um Ihre Nachbearbeitungskommentare anzuzeigen, gehen Sie zu "Knowledge-Dokumente" > ", Nachbearbeitungskommentare".

Dokument-Attribute

Dokument-Attribute helfen Ihnen bei der Verwaltung der Dokumente in Ihrem Knowledge-Pool. Dokument-Attribute können aktualisiert werden, um einem Dokument einen neuen Experten oder Eigentümer zuzuweisen. Sie können auch das Datum angeben, zu dem das Dokument in der Knowledge Base verfügbar wird, und das Datum, zu dem es abläuft. Durch Auswählen verschiedener Dokumentvorlagen können Sie das Layout jedes Dokuments ändern.

Dokumentberechtigungen

Sie können Berechtigungen für ein Dokument festlegen, anzeigen und bearbeiten. Diese Berechtigungen können verschiedenen Gruppen von Individuen zugewiesen werden. Beim Einstellen der Berechtigungen können Sie wählen, ob Berechtigungen von der Hauptkategorie eines Dokuments geerbt werden sollen oder neue Berechtigungen angeben. Standardmäßig erben Dokumente die Berechtigungen ihrer Hauptkategorie. Dies ermöglicht das Bearbeiten von Zugriffsberechtigungen auf Kategorieebene anstatt auf Dokumentebene.

Wichtig! Achten Sie beim Erstellen eines Knowledge-Dokuments darauf, die Benutzer in der Dokumentberechtigung zu berücksichtigen, die dem Dokument später im Genehmigungsverfahren zugeteilt werden könnten. Wenn eine Gruppe einem Dokument zugewiesen wird, kann es vorkommen, dass Benutzer aus dieser Gruppe nicht zum Anzeigen des Dokuments berechtigt sind. Wenn das Dokument einem bestimmten Anwender zugewiesen wird, eröffnen die Standard-Datenpartitionseinschränkungen dem Anwender die Möglichkeit, das Dokument anzuzeigen.

Knowledge-Kategorien

Sie müssen jedes Dokument einer Hauptkategorie zuordnen. Zum Beispiel muss jedes Knowledge, das sich auf Microsoft Word bezieht, der Kategorie "Microsoft Word" hinzugefügt zu werden. Außerdem können Sie in Knowledge Management ein Dokument mit mehreren sekundären Kategorien und anderen Dokumenten verknüpfen. Auf diese Weise kann ein Dokument unter vielen verschiedenen zutreffenden Kategorien klassifiziert werden und erfolgreichere Suchergebnisse liefern. Nachdem Sie eine Dokumentverknüpfung erstellt haben, wird die Verknüpfung *Siehe auch* angezeigt, wenn eines der verknüpften Dokumente angezeigt wird. Die Verknüpfung "Siehe auch" ermöglicht Ihnen, direkt von einem verknüpften Dokument zu einem anderen zu springen.

Anhangsberechtigungen

Sie verwalten die Anhangsberechtigungen in der Anhangsbibliothek, im Repositorys-Knoten auf der Registerkarte 'Verwaltung'. Sie können auf den Anforderungen Ihres Unternehmens basierte Repository-Ordnerberechtigungen einrichten.

Hinweis: Für ein Dokument können andere Berechtigungen vorhanden sein als für die damit verknüpften Anlagen.

Hinzufügen von Dokumentanhängen

Beim Arbeiten mit einem Knowledge-Dokument können Sie ergänzende Dateien oder URLs an das Dokument anhängen. Diese ergänzenden Dateien oder URLs bieten einfachen Zugriff auf weitere Informationen, die sich auf die Knowledge-Dokumente beziehen. Angehängte Dateien sind in einem Repository gespeichert.

Verwenden Sie die Registerkarte "Anhänge", um die Anhänge von Dateien und URLs im aktuellen Dokument zu verwalten. In Dokumenten, die mit der Standardvorlage "Integriertes Knowledge-Dokument" oder "Integrierte Knowledge-Baumstruktur" erstellt wurden, werden Verknüpfungen zu den Anhängen unter der Überschrift "Anhänge" angezeigt.

Hinweis: Die Registerkarte "Anhänge" wird nur für veröffentlichte Dokumente angezeigt. Für unveröffentlichte Dokumente werden auf der Registerkarte "Anhang" die Bereiche "Repositories", "Dateien" und "Anhänge" sowie eine Liste von URLs und Dateien angezeigt, die derzeit an das Dokument angehängt sind.

So fügen Sie einem Dokument einen Dateianhang hinzu

1. Öffnen Sie das Dokument zum Bearbeiten.
2. Klicken Sie auf die Registerkarte "Anlagen".
3. Geben Sie die URL ein, die Sie anhängen wollen.

4. Führen Sie einen der folgenden Schritte aus:

- Klicken Sie auf "Datei anhängen", um eine Datei aus Ihrem System hinzuzufügen.
- Klicken Sie auf "Datei aus Bibliothek anhängen", um in der Liste der Repositorys den Namen der Datei auszuwählen, die angehängt werden soll.

Der Name wird auf der Registerkarte "Anhänge" angezeigt.

Dokumentverlauf anzeigen

Sie können einen Datensatz aller Aktionen überprüfen, die im Zusammenhang mit einem Dokument durchgeführt wurden.

Um den Dokumentverlauf anzuzeigen, klicken Sie auf die Registerkarte "Verlauf" auf der Seite "Dokument aktualisieren".

In einer Ereignisliste werden die Details für jedes Ereignis angezeigt. Informationen, die auf der Registerkarte "Verlauf" angezeigt werden, existieren nur zu Referenzzwecken und können nicht geändert werden.

Dokument-Benachrichtigungen

In CA SDM können Sie eine Liste von Benutzern einrichten, die als Kontakte bezeichnet werden und die bei Eintreten bestimmter Ereignisse benachrichtigt werden können. Der Benachrichtigungsprozess informiert Personen über den Änderungsstatus eines Dokuments und hält sie so über den Fortschritt des Dokuments auf dem Laufenden. Nur Benutzer, die in dieser Liste enthalten sind, können die Benachrichtigungen erhalten, die diesem Dokument zugewiesen wurden.

Dokument-Änderungen

Nachdem ein Dokument in einem Posteingangsordner auf dem Scoreboard eingeht, können Benutzer die ihnen zugeteilten Aufgaben durchführen, indem sie ihre Dokumente entsprechend den zugewiesenen Rollen ändern (zum Beispiel kann ein Analyst für die Prüfung des technischen Inhalts des Dokuments verantwortlich sein, während ein anderer die Formatierung prüft).

Alle Anwender mit voller Berechtigung für das Dokument können das Dokument ändern. Der aktuelle Eigentümer hat die volle Berechtigung für das Dokument, hat aber möglicherweise keine ausdrücklichen Schreibberechtigungen. Nur der Eigentümer kann den Eigentümer des Dokuments ändern (auf der Registerkarte „Attribute“).

So verwalten Sie Rollenberechtigungen und die Dokumentsichtbarkeit:

Sie können Knowledge Management-Sicherheitsrechte einrichten, indem Sie die Rollenberechtigungen für Benutzer in Ihrer Umgebung verwalten. Mit diesen Rechten können Sie festlegen, welche Benutzer Zugang erhalten, wenn sie Knowledge anzeigen oder erstellen wollen, und wie Benutzer authentifiziert werden, wenn sie sich im System anmelden.

Sie können Rollenberechtigungen und Dokumentsichtbarkeit für Knowledge Management verwalten, indem Sie die folgenden Schritte ausführen:

1. Von der Registerkarte "Administration" navigieren Sie zu "Sicherheit und Rollenverwaltung" > "Rollenverwaltung" > "Rollenliste".

Die Seite "Rollenliste" wird angezeigt.

2. Wählen Sie die gewünschte Rolle aus, z. B. "Knowledge Manager".

Auf den Seiten "Rolle - Detail" und "Rolle aktualisieren" werden die folgenden Registerkarten angezeigt:

Knowledge Management

Gibt die Knowledge Management-Berechtigungen für die Rolle an.

KT-Dokumentsichtbarkeit

Gibt an, welchen Dokumentstatus die Rolle ansehen darf, wie "Entwurf", "Deaktiviert" und "Veröffentlicht".

3. Füllen Sie die Registerkarten aus, und speichern Sie die Änderungen.

Sicherheit und Rollenberechtigungen werden definiert.

Hinweis: Weitere Informationen zur Einstellung der Sicherheit und zur Definition von Rollen finden Sie in der *Online-Hilfe*.

Aktionsinhalte

Sie können Aktionsinhalt (ein Live-URL) erstellen, der ins Lösungsfeld eines Knowledge-Dokuments eingefügt werden kann. Wenn der Endanwender es anklickt, wird ein Incident erstellt oder eine andere Aktion ausgeführt. Durch das Verwenden von Aktionsinhalt kann ein erhebliches Maß an Definition und Klassifizierung erreicht werden, ohne dass dies dem Anwender bewusst ist.

Die Schritte zur Einfügung einer Verknüpfung von "Live-Aktionsinhalt" in ein Dokument sind einfach und es ist kein Codieren erforderlich. Der Knowledge Management-HTML-Editor verarbeitet die Erstellung des HTML-Codes.

Hinweis: Aktionsinhalt wird hauptsächlich für die Interaktion mit externen Anwendungen verwendet.

Weitere Informationen:

[Anzeigen von Aktionsinhalten](#) (siehe Seite 1006)

[Erstellen von Aktionsinhalten \(Aktions-URL\)](#) (siehe Seite 1007)

[Erstellen von Aktionsinhalt \(interner HTML\)](#) (siehe Seite 1008)

[Bearbeiten von Aktionsinhalten](#) (siehe Seite 1008)

[Suchen nach Aktionsinhalten](#) (siehe Seite 1009)

Anzeigen von Aktionsinhalten

Sie können die Details der Live-URLs anzeigen, mit denen Sie Aktionen für Endanwender festlegen können. Mit Hilfe von Knowledge Management können Sie Knowledge-Dokumente mit automatisierten Aufgaben verknüpfen. Auf diese Weise können Sie Self-Service-Skripts in Knowledge-Dokumente einbetten.

So zeigen Sie Aktionsinhalte an:

1. Wählen Sie auf der Registerkarte "Administration" die Option "Knowledge" > "Aktionsinhalte" aus.

Die Seite "Aktionsinhalte - Liste" wird angezeigt.

2. Die Seite zeigt Aktionsdetails und Ausführungsoptionen an.

Name

Zeigt den Namen des Aktionsinhalts an.

Code

Gibt den HTML-Code an, der den Aktionsinhalt mit dem Dokument verknüpft.

Aktions-URL

Gibt die URL-Verknüpfung an, mit der Sie Aktionen wie das Öffnen einer Website oder eines Formulars ausführen können.

Suchen

Sucht nach dem Namen der Elemente.

Filter anzeigen

Sucht auf der Seite "Kommentare - Liste" nach Elementen. Füllen Sie eines oder mehrere Suchfelder aus, und klicken Sie auf "Suchen". Auf der Seite "Aktionsinhalte - Liste" werden die Elemente angezeigt, die Ihren Suchkriterien entsprechen.

Neu erstellen:

Erstellt eine Verknüpfung mit einem Aktionsinhalt.

3. Suche oder Aktionsinhalt, die Sie mit Knowledge Management und Support-Automatisierung verwenden können.

Das Fenster "Suchergebnisse" wird angezeigt.

Erstellen von Aktionsinhalten (Aktions-URL)

Sie können Aktionsinhalte für Knowledge-Dokumente erstellen. Diese Aktions-URLs können eine Live-Website starten, die für alle Anwender Ihres Systems zugänglich ist. Sie können auch Aktions-URLs mit automatischen Aufgaben auf Ihrem Server (ein beliebiger Server, auf dem der KT-Daemon ausgeführt wird) verknüpfen und diese Skripts in Ihre Knowledge-Dokumente, Strukturdokumente, Dokumentvorlagen und Knowledge-Foren einbetten.

So erstellen Sie Aktionsinhalte (Aktions-URLs)

1. Wählen Sie auf der Registerkarte "Administration" die Option "Knowledge" > "Aktionsinhalte" aus.

Die Seite "Aktionsinhalte - Liste" wird angezeigt.

2. Klicken Sie auf "Neu erstellen".

Die Seite "Neuen Aktionsinhalt erstellen" wird angezeigt.

3. Füllen Sie die Felder aus. Die folgenden Felder erfordern eine Erklärung:

Code

Gibt eine eindeutige Kennung für diesen Aktionsinhalt an.

Internes HTML verwenden

[Erstellt eine interne Verknüpfung](#) (siehe Seite 1008) in der Anwendung, die dynamisch Informationen, wie Anwendernamen und Sitzungs-ID, von Knowledge-Dokumenten an Drittanbieteranwendungen weitergibt. Wählen Sie diese Option nicht aus.

Aktions-URL

Gibt ein URL an, dass mit einer Webseite, Vorlage oder mit einem automatisierten Skript verknüpft ist, z. B.: <http://www.ca.com>.

Klicken Sie auf "Speichern".

Der Aktionsinhalt wird erstellt.

Erstellen von Aktionsinhalt (interner HTML)

Sie können Aktionsinhalte für Knowledge-Dokumente erstellen. Diese Aktions-URLs können Self-Service-Skripts und auch Drittanbieteranwendungen starten. Diese Verknüpfung wird dynamisch erzeugt und überträgt automatisch Anwenderattribute, wie den Anwendernamen, in die Zielanwendung (z. B. <http://www.ca.com?USERNAME=BBB>). Anwenderattribute werden in einer HTML-Datei festgelegt.

So erstellen Sie Aktionsinhalt mit einer internen HTML-Datei:

1. Erstellen Sie eine interne HTML-Datei, die Daten in die Zielanwendung überträgt.

Hinweis: Die Datei "act_content_sample.html" ist in dem folgenden Verzeichnis verfügbar: NX_ROOT\bopcfg\www\html\default.

2. Speichern Sie die HTML-Datei im folgenden Verzeichnis:
NX_ROOT\site\mods\www\html\default.
3. Wählen Sie auf der Registerkarte "Administration" die Option "Knowledge" > "Aktionsinhalt" aus.

Die Seite "Aktionsinhalte - Liste" wird angezeigt.

4. Klicken Sie auf "Neu erstellen".

Die Seite "Neuen Aktionsinhalt erstellen" wird angezeigt.

5. Füllen Sie das folgende Feld aus:

Code

Gibt eine eindeutige Kennung für diesen Aktionsinhalt an.

6. Aktivieren Sie das Kontrollkästchen "Internes HTML verwenden".
7. Legen Sie die geeignete HTML-Datei im Feld "Aktions-URL" fest, z. B.:
act_content_sample.html.

Hinweis: Sie können in der URL Support-Automatisierungs-Skripts mit Hilfe des Formats *SA_SCRIPT=[Self Service Script ID]* verwenden.

8. Klicken Sie auf "Speichern".

Der Aktionsinhalt wird erstellt. Wenn der Anwender diese Aktionsinhalts-Verknüpfung innerhalb eines Knowledge-Dokuments anklickt, werden Anwenderattribute (z. B. der Anwendername) dynamisch an die Zielanwendung weitergegeben.

Bearbeiten von Aktionsinhalten

Sie können Aktionsinhalte bearbeiten, die bereits auf der Seite "Aktionsinhalte -Liste" erstellt worden sind.

So bearbeiten Sie Aktionsinhalte:

1. Wählen Sie auf der Registerkarte "Administration" die Option "Knowledge" > "Aktionsinhalte" aus.
Die Seite "Aktionsinhalte - Liste" wird angezeigt.
2. Wählen Sie das zu bearbeitende Element aus.
Die Seite "Aktionsinhalt - Details" wird angezeigt.
3. Klicken Sie auf "Bearbeiten".
Die Seite "Aktionsinhalt aktualisieren" wird angezeigt.
4. Bearbeiten Sie die Felder nach Bedarf.
5. Klicken Sie auf "Speichern".
Der Aktionsinhalt wird aktualisiert.

Suchen nach Aktionsinhalten

Sie können Suchkriterien zum Filtern der Liste mit den Aktionsinhalten eingeben, um nur die gewünschten Elemente anzuzeigen. Sie können auch nach einzelnen Elementen suchen, die Sie anzeigen oder bearbeiten möchten.

So suchen Sie Aktionsinhalte:

1. Wählen Sie auf der Registerkarte "Administration" die Option "Knowledge" > "Aktionsinhalte" aus.
Die Seite "Aktionsinhalte - Liste" wird angezeigt.
2. Klicken Sie auf "Filter anzeigen".
Der Suchfilter wird angezeigt.
3. Füllen Sie eins oder mehrere der Suchfelder aus:

Name

Gibt die Bezeichnung dieses Aktionsinhaltelements an.

Status

Zeigt an, ob dieses Element aktiv oder inaktiv ist.

Code

Gibt eine eindeutige Kennung für diesen Aktionsinhalt an.

Knowledge Management URL

Legt fest, dass die Aktions-URL mit der internen Webseite (.html) verknüpft ist.

4. (Optional) Klicken Sie auf "Weitere".

Es werden zusätzliche Felder angezeigt, mit deren Hilfe Sie die Anzahl der Elemente weiter beschränken können, die in der Liste der Aktionsinhalte angezeigt werden sollen.

5. Klicken Sie auf "Suche".

Auf der Seite "Aktionsinhalte - Liste" werden die Elemente angezeigt, die Ihren Suchenkriterien entsprechen. Sie können ein Element zur Anzeige oder Bearbeitung auswählen.

Hinweis: Sie können Ergebnislisten nach Excel exportieren, um sie außerhalb von CA SDM zu verwenden. Klicken Sie dazu auf der Listenseite auf die Schaltfläche "Exportieren".

Genehmigungsvorgang für Dokumente

Für Administratoren, die die Verwaltung ihrer Knowledge Base steuern müssen, ist es entscheidend, dass sie den Prozess der Bearbeitung und Genehmigung von Dokumenten individuell anpassen können. Sie können Vorlagen für den Genehmigungsvorgang entwerfen, die angeben, wie, wann und von wem das Dokument eines Mitarbeiters geändert und veröffentlicht werden kann. Vorlagen für den Genehmigungsvorgang können verwendet werden, um verschiedene Genehmigungsvorgänge zu bestimmen, die am besten zu Ihrer Geschäftsumgebung passen. Gegebenenfalls kann der Genehmigungsvorgang, den Sie implementieren, mit der Zeit geändert werden, um einfacher oder komplexer zu werden.

Der Manager für den Genehmigungsvorgang ermöglicht Ihnen, Vorlagen für den Genehmigungsvorgang zu definieren. Standardmäßig wird die vordefinierte Vorlage für den Genehmigungsvorgang verwendet. Sie können jedoch eine neue Vorlage erstellen oder eine vorhandene Vorlage bearbeiten. Beim Erstellen einer Vorlage für den Genehmigungsvorgang müssen Sie Statuswerte definieren und der Vorlage Aufgaben hinzufügen. Der Genehmigungsvorgang beinhaltet eine Reihe der Aufgaben, die mit einem Knowledge-Dokument durchgeführt werden. Der Eigentümer, dem eine Aufgabe in der Vorlage für den Genehmigungsvorgang zugewiesen wird, erfüllt jede Aufgabe.

Statuswerte sind die verschiedenen Zustände, mit denen das Dokument während der Phasen des Genehmigungsvorgangs verknüpft ist.

Entwurf

Gibt ein neues Dokument an.

Veröffentlicht

Gibt ein Dokument an, das den vollständigen Genehmigungszyklus durchlaufen hat und Teil der anzeigbaren Knowledge Base geworden ist.

Rework-Draft Version (Produktversion)

Gibt eine überarbeitete Version des Dokuments an, die in der Knowledge Base ersetzt wird, sobald die Version überprüft und erneut veröffentlicht ist.

Deaktiviert

Gibt ein Dokument an, das sein Ablaufdatum erreicht hat. Sie können auch eigene Statuswerte erstellen, die Sie später mit Aufgaben verknüpfen.

Manager für den Genehmigungsvorgang

Knowledge-Administratoren können auf die Manager für den Genehmigungsvorgang zugreifen, um diese Aktionen aufzuführen:

- Diese Berechtigungen bestimmen, welche Gruppen ein Knowledge-Dokument lesen und welche Gruppen ein Knowledge-Dokument schreiben (d. h. bearbeiten) dürfen.
- Bestimmen Sie die Aufgaben in einer Vorlage für den Genehmigungsvorgang. Diese Aufgaben bestimmen den Lebenszyklus der Dokumente, die mit der Vorlage erstellt wurden.
- Definieren Sie die verschiedenen Stati, denen das Dokument während des Genehmigungsvorgangs zugeordnet sein kann.

Wichtig! Achten Sie beim Erstellen eines Knowledge-Dokuments darauf, die Anwender in der Dokumentberechtigung zu berücksichtigen, die dem Dokument später im Genehmigungsvorgang zugeteilt werden könnten. Anwender jener Gruppe haben nicht unbedingt die Berechtigung, das Dokument anzusehen. Wenn das Dokument einem bestimmten Anwender zugewiesen wird, eröffnen die Standard-Datenpartitionseinschränkungen dem Anwender die Möglichkeit, das Dokument anzuzeigen.

Festlegen eines Genehmigungsvorgangs für die Dokumentbearbeitung

Knowledge-Administratoren können festlegen, wer Dokumente vor dem Genehmigungsvorgang und nach der Veröffentlichung bearbeiten kann.

Hinweis: Anwender mit allen Berechtigungen (Lesen/Schreiben) können veröffentlichte Dokumente bearbeiten.

So legen Sie einen Genehmigungsvorgang für die Dokumentbearbeitung fest:

1. Navigieren Sie auf der Registerkarte "Administration" zu "Knowledge" > "Manager für den Genehmigungsvorgang" > "Einstellungen für den Genehmigungsvorgang".

Die Seite "Einstellungen für den Genehmigungsvorgang" wird angezeigt.

2. Legen Sie fest, wer Dokumente bearbeiten kann, *bevor* die Dokumente veröffentlicht werden. Wählen Sie eine der folgenden Optionen:

Dokumente können von den Personen bearbeitet werden, denen die Aufgabe zugewiesen wurde, von den Eigentümern oder von Anwendern mit den entsprechenden Zugriffstypansichten.

Gibt an, dass die folgenden Kontakte Dokumente bearbeiten können:

- Ein Kontakt, der der aktuellen Aufgabe zugewiesen wurde.
- Ein Kontakt, der als Eigentümer des Dokuments für die aktuelle Aufgabe angegeben wurde.
- Ein Knowledge-Manager.
- Ein Systemadministrator.

Dokumente können auch von Anwendern bearbeitet werden, die über volle Berechtigung verfügen.

Legt fest, dass jeder dafür schreibberechtigte Anwender das Dokument bearbeiten kann.

3. Legen Sie fest, wer Dokumente bearbeiten kann, *nachdem sie* veröffentlicht wurden. Wählen Sie eine der folgenden Optionen:

Nachdem Dokumente veröffentlicht wurden, können sie von Anwendern mit voller Berechtigung bearbeitet werden.

Legt fest, dass ein Anwender mit allen Berechtigungen veröffentlichte Dokumente bearbeiten kann.

Anwender mit allen Berechtigungen können die Attribute des veröffentlichten Dokuments ändern.

Legt fest, dass alle für das Dokument schreibberechtigte Anwender nur solche Attribute von veröffentlichten Dokumenten wie Configuration Items oder Produkte verändern können.

Vor dem Bearbeiten des Dokuments muss die Veröffentlichung rückgängig gemacht werden.

Legt fest, dass der Anwender die Veröffentlichung eines Dokuments rückgängig machen muss, bevor er es bearbeitet.

Klicken Sie auf "Speichern".

Der Genehmigungsvorgang wird definiert.

Erstellen einer Genehmigungsvorgangsvorlage

Die Aufgaben in einer Vorlage für den Genehmigungsvorgang definieren den Lebenszyklus von Dokumenten, die mit der Vorlage erstellt wurden.

Hinweis: Wenn die Mandantenfähigkeit installiert ist, wählen Sie in der Dropdown-Liste den entsprechenden Mandanten aus. Mit der Option "öffentlich (freigegeben)" wird das Objekt für alle Mandanten erstellt.

So erstellen Sie eine Vorlage für den Genehmigungsvorgang:

1. Wählen Sie auf der Registerkarte "Administration" die Option "Knowledge" > "Manager für den Genehmigungsvorgang" > "Vorlagen für Genehmigungsvorgang" aus.

Die Liste mit den Vorlagen für den Genehmigungsvorgang wird angezeigt.

2. Klicken Sie auf "Neu erstellen".

Die Seite "Vorlage für den Genehmigungsvorgang – Detail" wird angezeigt.

3. Geben Sie einen Namen und eine Beschreibung für die Vorlage ein.

4. Klicken Sie auf "Speichern".

Die Seite "Vorlage für Genehmigungsvorgang - Detail" zeigt zusätzliche Felder an.

5. Wählen Sie die Aufgabe aus, die Sie ausführen wollen, wenn Sie eine Arbeitsversion des Dokuments mit Hilfe der Vorlage erstellen.

6. Wählen Sie die Aufgabe aus, die Sie ausführen wollen, wenn Sie ein Dokument erneut aktivieren, das mit Hilfe der Vorlage erstellt wurde.

7. Klicken Sie auf "Aufgabe einfügen", um eine neue Aufgabe zu erstellen und in die Vorlage aufzunehmen.

Die Seite "Neuen Aufgaben erstellen" wird angezeigt.

8. Füllen Sie die Felder aus. Die folgenden Felder erfordern eine Erklärung:

Aufgabe

Bezeichnet die Aufgabe.

Verantwortlicher

Weist der Aufgabe eine Person zu. Um einen Namen auszuwählen, klicken Sie auf das Suchsymbol.

Hinweis: Sie können nach dem Erstellen der Aufgabe [eine alternative Liste von Zuständigen hinzufügen](#) (siehe Seite 1014).

Klicken Sie auf "Speichern".

Die Vorlage für den Genehmigungsvorgang wird erstellt.

Weitere Informationen:

[Hinzufügen von alternativen Zuständigen zu einer Aufgabe](#) (siehe Seite 1014)

[Bearbeiten von Vorlagen für den Genehmigungsvorgang](#) (siehe Seite 1015)

[Suchen nach Vorlagen für den Genehmigungsvorgang](#) (siehe Seite 1015)

Hinzufügen von alternativen Zuständigen zu einer Aufgabe

Sie können beim Bearbeiten einer Aufgabe alternative Zuständige hinzufügen.

So fügen Sie einer Aufgabe alternative Zuständige hinzu:

1. Wählen Sie aus der Vorlageliste für Genehmigungsvorgänge die Aufgabe aus, die Sie bearbeiten wollen.
Die Seite "Aufgabendetail" wird angezeigt.
2. Bearbeiten Sie die Felder nach Bedarf.
3. Klicken Sie in der Liste der Zuständigen auf die Schaltfläche "Hinzufügen" .
Die Seite "Neuen Zuständigen erstellen" wird angezeigt.
4. Geben Sie im Feld "Zuständiger" den Namen der Person ein, die Sie der Aufgabe zuweisen wollen, oder klicken Sie auf das Suchsymbol, um nach dem Namen zu suchen.
5. Wiederholen Sie diesen Vorgang je nach Bedarf, und stellen Sie eine Liste alternativer Zuständiger zusammen.
6. Klicken Sie auf "Speichern".
Die alternativen Zuständigen werden der Aufgabe hinzugefügt.

Bearbeiten von Vorlagen für den Genehmigungsvorgang

Sie können die Vorlage für einen Genehmigungsvorgang bearbeiten.

So bearbeiten Sie eine Vorlage für den Genehmigungsvorgang:

1. Wählen Sie auf der Registerkarte "Administration" die Option "Knowledge" > "Manager für den Genehmigungsvorgang" > "Vorlagen für Genehmigungsvorgang" aus.

Die Liste mit den Vorlagen für den Genehmigungsvorgang wird angezeigt.

2. Wählen Sie die Vorlage aus, die Sie bearbeiten möchten, und klicken Sie auf ihren Namen.

Die Seite "Vorlage für den Genehmigungsvorgang – Detail" wird angezeigt.

3. Klicken Sie auf "Bearbeiten".

Die Seite "Vorlage für Genehmigungsvorgang aktualisieren" wird angezeigt.

4. Bearbeiten Sie die Felder nach Bedarf.

5. Klicken Sie auf "Speichern".

Die Vorlage für den Genehmigungsvorgang wird aktualisiert.

Suchen nach Vorlagen für den Genehmigungsvorgang

Sie können Suchkriterien zum Filtern der Liste mit den Vorlagen für Genehmigungsvorgänge eingeben, um nur die gewünschten Elemente anzuzeigen. Sie können auch nach einzelnen Elementen suchen, die Sie anzeigen oder bearbeiten möchten.

Hinweis: Wenn die Mandantenfähigkeit installiert ist, zeigt die Listenseite die Einstellungen für Mandant und öffentliche Daten im Suchfilter an. Öffentliche Daten können in Mandantendaten eingeschlossen oder aus diesen ausgeschlossen werden. Es werden ausschließlich öffentliche Objekte gesucht. Wählen Sie auf Detailseiten den geeigneten Mandanten in der Liste aus. Wenn Sie <leer> wählen, ist das Objekt öffentlich.

So suchen Sie eine Vorlage für den Genehmigungsvorgang:

1. Wählen Sie auf der Registerkarte "Administration" die Option "Knowledge" > "Genehmigungsvorgang" > "Vorlagen für Genehmigungsvorgang" aus.

Die Seite "Vorlage für den Genehmigungsvorgang – Liste" wird angezeigt.

2. Klicken Sie auf "Filter anzeigen".

3. Geben Sie die ersten paar Zeichen des Namens der gewünschten Vorlage ein.

4. (Optional) Klicken Sie auf "Weitere".

Es werden zusätzliche Felder angezeigt, mit deren Hilfe Sie die Anzahl der Elemente beschränken können, die in der Vorlageliste für Genehmigungsvorgänge angezeigt werden sollen.

5. Klicken Sie auf "Suche".

Auf der Seite "Vorlage für Genehmigungsvorgang - Liste" werden die Elemente angezeigt, die Ihren Suchkriterien entsprechen. Sie können ein Element zur Anzeige oder Bearbeitung auswählen.

Hinweis: Sie können Ergebnislisten nach Excel exportieren, um sie außerhalb von CA SDM zu verwenden. Klicken Sie dazu auf der Listenseite auf die Schaltfläche "Exportieren".

Definitionen für den Dokumentstatus

Sie können anwenderspezifische Dokumentstati hinzufügen und löschen sowie die Namen und Beschreibungen von vordefinierten Dokumentstati ändern.

Weitere Informationen:

[Erstellen eines neuen Dokumentstatus](#) (siehe Seite 1016)

[Suchen nach dem Dokumentstatus](#) (siehe Seite 1017)

[Bearbeiten des Dokumentstatus](#) (siehe Seite 1017)

Erstellen eines neuen Dokumentstatus

Sie können in Ihrem CA SDM-System einen Dokumentstatus für Knowledge-Dokumente erstellen.

So erstellen Sie einen Dokumentstatus:

1. Wählen Sie auf der Registerkarte "Administration" die Option "Knowledge" > "Manager für den Genehmigungsvorgang" > "Dokumentstatus".

Das Fenster "Dokumentstatus – Liste" wird angezeigt.

2. Klicken Sie auf "Neu erstellen".

Die Seite "Dokumentstatus – Detail" wird angezeigt.

3. Geben Sie eine Bezeichnung und eine Beschreibung für den Status ein.

4. Klicken Sie auf "Speichern".

Der Dokumentstatus wird erstellt.

Suchen nach dem Dokumentstatus

Sie können Suchkriterien zum Filtern der Dokumentstatusliste eingeben, so dass nur die gewünschten Elemente angezeigt werden. Sie können auch nach einzelnen Elementen suchen, die Sie anzeigen oder bearbeiten möchten.

So suchen Sie einen Dokumentstatus:

1. Wählen Sie auf der Registerkarte "Administration" die Option "Knowledge" > "Manager für den Genehmigungsvorgang" > "Dokumentstatus".

Die Seite "Dokumentstatus - Liste" wird angezeigt.

2. Klicken Sie auf "Filter anzeigen".
3. Geben Sie die ersten paar Zeichen des gesuchten Statusnamens ein.
4. (Optional) Klicken Sie auf "Weitere".

Es werden zusätzliche Felder angezeigt. Mit ihrer Hilfe können Sie die Anzahl der Elemente beschränken, die in der Dokumentstatusliste angezeigt werden sollen.

5. Klicken Sie auf "Suche".

Auf der Seite "Dokumentstatus - Liste" werden die Elemente angezeigt, die Ihren Suchkriterien entsprechen. Sie können ein Element zur Anzeige oder Bearbeitung auswählen.

Hinweis: Sie können Ergebnislisten nach Excel exportieren, um sie außerhalb von CA SDM zu verwenden. Klicken Sie dazu auf der Listenseite auf die Schaltfläche "Exportieren".

Bearbeiten des Dokumentstatus

Sie können den Dokumentstatus bearbeiten.

So bearbeiten Sie einen Dokumentstatus:

1. Wählen Sie auf der Registerkarte "Administration" die Option "Knowledge" > "Manager für den Genehmigungsvorgang" > "Dokumentstatus".

Das Fenster "Dokumentstatus – Liste" wird angezeigt.

2. Wählen Sie den Status aus, den sie bearbeiten möchten, und klicken Sie auf seinen Namen.

Die Seite "Dokumentstatus – Detail" wird angezeigt.

3. Klicken Sie auf "Bearbeiten".

Die Seite zur Aktualisierung des Dokumentstatus wird angezeigt.

4. Bearbeiten Sie die Felder "Status" und "Beschreibung" wie gewünscht.
5. Klicken Sie auf "Speichern".

Der Dokumentstatus wird aktualisiert.

Automatisierungsrichtlinien

Administratoren können, auf Grundlage der Lebenszyklus-Richtlinien und den darin festgelegten Aktionen, bestimmte Aufgaben im Genehmigungsvorgang für das Knowledge-Dokument automatisieren. Durch die Automatisierung von Aufgaben können Endanwender, die nach Lösungen suchen, Probleme schneller lösen. Sie können Problem eigenständig lösen, was einen Nutzen für Organisation darstellt.

Automatische Richtlinien arbeiten mit Events und Makros.

Weitere Informationen:

[Anzeigen von Automatisierungsrichtlinien](#) (siehe Seite 1018)

[Einrichten von Automatisierungsrichtlinien](#) (siehe Seite 1020)

[Erstellen von Automatisierungsrichtlinien](#) (siehe Seite 1020)

[Bearbeiten von Automatisierungsrichtlinien](#) (siehe Seite 1021)

[Planen von Automatisierungsrichtlinien](#) (siehe Seite 1021)

[Anzeigen von Berichten zu Lebenszyklusrichtlinien für Dokumente](#) (siehe Seite 1022)

Anzeigen von Automatisierungsrichtlinien

Eine Automatisierungsrichtlinie beschreibt, unter welcher Bedingung Dokumente für eine Korrektur gekennzeichnet werden, und ob sie in den verschiedenen Stadien ihres Lebenszyklus veröffentlicht oder zurückgezogen werden. Die Standardrichtlinie "Fehlerhafte Verknüpfungen reparieren" können Sie beispielsweise für alle Dokumente in der Knowledge Base mit fehlerhaften Verknüpfungen angeben. Die Fehlerbehebung selbst kann einem Analysten zugewiesen werden.

Hinweis: Wenn die Mandantenfähigkeit installiert ist, zeigt die Listenseite die Einstellungen für Mandant und öffentliche Daten im Suchfilter an. Öffentliche Daten können in Mandantendaten eingeschlossen oder aus diesen ausgeschlossen werden. Es werden ausschließlich öffentliche Objekte gesucht. Wählen Sie auf Detailseiten den geeigneten Mandanten in der Liste aus. Wenn Sie <leer> wählen, ist das Objekt öffentlich.

Um Automatisierungsrichtlinien anzuzeigen, wählen Sie auf der Registerkarte "Administration" die Option "Knowledge" > "Automatisierungsrichtlinien" > "Richtlinien" aus.

Auf der Seite mit der Liste der Automatisierungsrichtlinien werden die Details der Automatisierungsrichtlinien angezeigt. Sie können die Standardrichtlinien bearbeiten, oder Ihre eigenen Richtlinien definieren. Jede Richtlinie wird mit den folgenden Komponenten verknüpft:

Gespeicherte Abfrage

Enthält eine Reihe von Aktionsmakros, die ausgeführt werden, wenn die Richtlinien während der Verarbeitung ein Dokument identifizieren und als übereinstimmend definieren. Nach der Verarbeitung zeigt das Bedingungs-Event der gespeicherten Abfrage auf dem CA SDM-Scoreboard einen rollenbasierten Richtlinienbericht zum Knowledge Management-Lebenszyklus an.

Der Administrator ist für das Überwachen der Berichte sowie für Feedback und Empfehlungen für die entsprechenden Dokumentbearbeiter verantwortlich.

Aktionsmakro

Enthält Codes, mit deren Hilfe Sie eine Markierung festlegen, die Priorität erhöhen und andere Aktionen ausführen können. Sie können die Makros in dieser Liste bearbeiten oder eigene Makros definieren.

Hinweis: Sie können Ergebnislisten nach Excel exportieren, um sie außerhalb von CA SDM zu verwenden. Klicken Sie dazu auf der Listenseite auf die Schaltfläche "Exportieren".

Weitere Informationen:

[Anzeigen von Berichten zu Lebenszyklusrichtlinien für Dokumente](#) (siehe Seite 1022)
[Planen von Automatisierungsrichtlinien](#) (siehe Seite 1021)

Einrichten von Automatisierungsrichtlinien

Administratoren können die Funktion für die Automatisierungsrichtlinien einrichten, indem sie die folgenden Schritte ausführen:

1. (Erforderlich) Im Automatisierungsrichtlinien-Scheduler muss ein Batch-Vorgang definiert werden, der auf dem Hintergrundserver ausgeführt wird und die notwendigen Daten zum Anzeigen der Berichte über die Knowledge Management-Lebenszyklusrichtlinien liefert. Dieser Aktionsschritt bezieht sich auch auf die Knowledge-Berichtskarte.

Hinweis: Weitere Informationen über Automatisierungsrichtlinien finden Sie im *Implementierungshandbuch*.

2. (Erforderlich) Definieren Sie für Sicherheit und Rollenmanagement auf der Registerkarte "Sichtbarkeit von Knowledge-Dokumenten:" in "Rollenmanagement" die Phase, in der die Anwender Dokumente während ihres Lebenszyklus anzeigen und durchsuchen können.
3. Auf der Seite "Automatisierungsrichtlinien - Liste" können Sie die Standardrichtlinien bearbeiten oder eigene Richtlinien definieren.

Hinweis: Für neue Richtlinien muss der Administrator das Feld "Lebenszyklus-Richtlinien nicht berücksichtigen" in die gespeicherte Abfrage aufnehmen. Ansonsten wird es nicht auf der Registerkarte "Attribute" angezeigt.

Erstellen von Automatisierungsrichtlinien

Sie können eine Automatisierungsrichtlinie erstellen, die aktiviert wird, wenn eine Aktion stattfindet, z. B. wenn ein Dokument veröffentlicht oder in der Knowledge Base deaktiviert wird.

Hinweis: Wenn die Mandantenfähigkeit installiert ist, wählen Sie in der Dropdown-Liste den entsprechenden Mandanten aus. Mit der Option "öffentlich (freigegeben)" wird das Objekt für alle Mandanten erstellt.

So erstellen Sie eine Automatisierungsrichtlinie:

1. Wählen Sie auf der Registerkarte "Administration" die Option "Knowledge" > "Automatisierungsrichtlinien" > "Richtlinien" aus.
Die Seite "Neue Automatisierungsrichtlinie erstellen" wird angezeigt.
2. Geben Sie einen Namen und/oder eine Beschreibung in die entsprechenden Felder ein.
3. Geben Sie einen gespeicherten Abfragenamen ein, oder wählen Sie ihn mit Hilfe des Suchsymbols aus.
4. Klicken Sie auf "Aktion Hinzufügen".
Die Seite "Makroliste" wird angezeigt.

5. Wählen Sie auf der Makro-Listenseite eines der vordefinierten Aktionsmakros aus, oder definieren Sie Ihr eigenes Makro (klicken Sie auf "Neu erstellen").

Das Aktionsmakro wird auf der Seite "Neue Automatisierungsrichtlinie erstellen" in der Liste der Aktionsinformationen angezeigt.

Hinweis: Sie können ein Aktionsmakro löschen. Klicken Sie hierzu mit der rechten Maustaste auf den Namen und wählen Sie aus dem Kontextmenü die Option "Löschen".

6. Klicken Sie auf "Speichern".

Die neue Richtlinie wird in der Liste für Automatisierungsrichtlinien angezeigt.

7. (Optional) Klicken Sie mit der rechten Maustaste auf den Titel, um eine Richtlinie zu bearbeiten.

Die ausgewählte Richtlinie wird auf der Seite zur Aktualisierung von Richtlinien angezeigt und Sie können sie bearbeiten.

Bearbeiten von Automatisierungsrichtlinien

Sie können eine Automatisierungsrichtlinie aktualisieren.

So bearbeiten Sie eine Automatisierungsrichtlinie:

1. Wählen Sie auf der Registerkarte "Administration" die Option "Knowledge" > "Automatisierungsrichtlinien" > "Richtlinien" aus.

Die Liste für Automatisierungsrichtlinien wird angezeigt.

2. Klicken Sie mit der rechten Maustaste auf die zu bearbeitende Richtlinie, und wählen Sie dann im Kontextmenü die Option "Bearbeiten".

Die Seite "Automatisierungsrichtlinie aktualisieren" wird angezeigt.

3. Bearbeiten Sie die Eingabefelder nach Bedarf.
4. Klicken Sie auf "Speichern".

Die Automatisierungsrichtlinie wird aktualisiert.

Planen von Automatisierungsrichtlinien

Sie können das Datum und die Uhrzeit angeben, wann CA SDM die Berechnung und die Batch-Verarbeitung der Richtlinien ausführen soll.

So planen Sie Automatisierungsrichtlinien:

1. Wählen Sie auf der Registerkarte "Administration" die Option "Knowledge" > "Automatisierungsrichtlinien" > "Ablaufplanung" aus.

Die Seite "Automatisierungsrichtlinien" wird angezeigt.

2. Füllen Sie die folgenden Felder aus:

Letzte Aktualisierung:

Legt das Kontrollkästchen "Berechnung ausführen" fest.

Ablauf

Legt ein Datum fest, entweder im Textfeld oder im Kalender. Sie können das Zeitintervall auswählen, in dem CA SDM die Berechnung durchführt und die Richtlinien ausführt.

Klicken Sie auf "Speichern".

Die Richtlinien werden zum angegebenen Datum und der festgelegten Uhrzeit verarbeitet.

Anzeigen von Berichten zu Lebenszyklusrichtlinien für Dokumente

Sie können die Richtlinienberichte über Dokument-Lebenszyklen anzeigen, den Automatisierungsrichtlinien erstellen.

Um die Berichte anzuzeigen, wählen Sie auf der Registerkarte "Service Desk" die Option "Knowledge-Dokumente" > "Automatisierungsrichtlinien" > "Richtlinien".

Wenn Sie eine Richtlinie auswählen, werden die folgenden Zusammenfassung-Informationen auf der Seite "Liste der Dokumente" angezeigt:

Hinweis: Wenn die Mandantenfähigkeit installiert ist, zeigt die Listenseite die Einstellungen für Mandant und öffentliche Daten im Suchfilter an. Öffentliche Daten können in Mandantendaten eingeschlossen oder aus diesen ausgeschlossen werden. Es werden ausschließlich öffentliche Objekte gesucht. Wählen Sie auf Detailseiten den geeigneten Mandanten in der Liste aus. Wenn Sie <leer> wählen, ist das Objekt öffentlich.

Titel

Zeigt den Titel des Dokuments an, das für die Korrektur markiert ist oder für die Veröffentlichung oder Deaktivierung weitergeleitet wurde.

Richtlinien/Aktionen

Zeigt den für die Richtlinie definierten Richtlinienennamen und Aktionsinhalt an.

Attribute

Zeigt die Eigenschaften des Dokuments an, auf die sich die Richtlinie auswirkt.

Knowledge-Dokumentsteuerung

Öffnen Sie die Knowledge-Dokumente, und fügen Sie Kommentare hinzu, senden Sie die Knowledge ab, und zeigen Sie die Knowledge-Baumstrukturdokumente an. Sie können auch den Inhalt und die Form von Dokumenten durch das Auswählen einer Vorlage näher bestimmen.

So können Administratoren kontrollieren, wie Anwender mit Dokumenten interagieren:

- Definieren Sie die [Kommentartypen](#) (siehe Seite 1024), die in Knowledge-Dokumenten und Dropdown-Listen in der Endanwenderschnittstelle erscheinen.
- Geben Sie Dokument[einstellungen](#) (siehe Seite 1083) an, die sich auf Kommentare, das Absenden von Knowledge und auf das Ansehen von Dokumenten beziehen.
- Erstellen Sie [Dokumentvorlagen](#) (siehe Seite 1030), die den Inhalt und die Form von Dokumenten bestimmen.
- Exportieren (oder importieren) Sie Knowledge-Inhalte aus anderen Ressourcen oder Systemen. Für die Konfiguration für erweiterte Verfügbarkeit können Sie mithilfe der CA SDM-Web-Benutzeroberfläche keinen Export oder Import aus dem Anwendungsserver durchführen. Um einen Export oder einen Import mithilfe des Anwendungsservers durchzuführen, führen Sie das Hilfsprogramm "pdm_kit" oder "pdm_ket" aus, wenn sich das Paket auf einem freigegebenen UNC-Laufwerk befindet.
- Verwalten Sie die Möglichkeiten zur [Versionskontrolle](#) (siehe Seite 958) von Dokumenten.
- Verwalten Sie die [Planung für Knowledge-Dokumente](#) (siehe Seite 963).

Weitere Informationen:

[Kommentartypen](#) (siehe Seite 1024)

[Dokumentvorlagen](#) (siehe Seite 1030)

[Erstellen von Verknüpfungen für Knowledge-Dokumente](#) (siehe Seite 1038)

[Knowledge-Kategorien](#) (siehe Seite 1041)

[Berichte und Indikatoren](#) (siehe Seite 1051)

[Suchen](#) (siehe Seite 1053)

[Lösungsumfrage](#) (siehe Seite 1080)

Kommentartypen

Wenn Analysten einen Tippfehler oder ein Problem mit dem Inhalt in einem Dokument bemerken, können sie einen Kommentar hinzufügen, mit dem das Dokument zur Korrektur gekennzeichnet wird, und das Problem zur Nachbearbeitung dann einem anderen Analysten zuweisen.

Die Administratoren können die Kommentartypen definieren, die in den verschiedenen Listenansichten auf der Benutzeroberfläche aufgeführt werden.

Anzeigen von Kommentartypen

Wenn Sie ein Knowledge-Dokument öffnen, können Sie einen Kommentar hinzufügen, der das Dokument zur Korrektur, Weiterleitung, Deaktivierung usw. markiert. Mit Hilfe der Seite "Kommentartypen - Liste" können Sie die Details der Kommentartypen verwalten.

Um diese Seite anzuzeigen, wählen Sie auf der Registerkarte "Administration" die Option "Knowledge" > "Dokumente" > "Kommentartypen" aus.

Hinweis: Wenn die Mandantenfähigkeit installiert ist, zeigt die Listenseite die Einstellungen für Mandant und öffentliche Daten im Suchfilter an. Öffentliche Daten können in Mandantendaten eingeschlossen oder aus diesen ausgeschlossen werden. Es werden ausschließlich öffentliche Objekte gesucht. Wählen Sie auf Detailseiten den geeigneten Mandanten in der Liste aus. Wenn Sie <leer> wählen, ist das Objekt öffentlich.

Die Seite "Kommentartypen - Liste" wird mit den folgenden Spalten angezeigt:

Name

Zeigt die Liste der Kommentartypen an, die auf der Benutzerschnittstelle in Dokumenten und Dropdown-Listen auftauchen. Sie können die folgenden Standardkommentartypen bearbeiten, oder Ihren eigenen definieren:

- Fehlerhafte Verknüpfung
- Für Veröffentlichung vorgeschlagen
- Inhalt nicht klar
- Schwer zu finden
- Allgemeiner Kommentar
- Falsche Informationen
- Fehlende Informationen
- Neuen Inhalt empfehlen
- Überprüfung
- Lösung funktioniert nicht

In Anwenderansicht anzeigen

Zeigt den Kommentar in verschiedenen Listenansichten auf der Benutzeroberfläche an.

Nachverfolgung erforderlich

Gibt an, ob der Anwender auf diesen Kommentar reagieren muss.

Zeit bis Abschluss (Tage)

Legt fest, wie viele Tage der Anwender diesen Kommentartyp nachverfolgen muss.

Status

Gibt an, ob der Kommentartyp aktiv oder inaktiv ist.

Diese Seite enthält die folgenden Schaltflächen:

Suchen

Sucht nach dem Namen der Elemente.

Filter anzeigen

Sucht auf der Seite "Kommentare - Liste" nach einem Kommentar. Füllen Sie eines oder mehrere Suchfelder aus, und klicken Sie auf "Suchen". Auf der Seite "Kommentare - Liste" werden die Kommentare angezeigt, die Ihren Suchkriterien entsprechen.

Filterinhalt löschen

Leert den Filter.

Neu erstellen:

Erstellt einen Kommentartyp.

Hinweis: Sie können Ergebnislisten nach Excel exportieren, um sie außerhalb von CA SDM zu verwenden. Klicken Sie dazu auf der Listenseite auf die Schaltfläche "Exportieren".

Erstellen von Kommentartypen

Sie können die Kommentartypen definieren, die in den verschiedenen Listenansichten auf der Seite "Neuen Kommentartyp erstellen" aufgeführt werden.

Hinweis: Wenn die Mandantenfähigkeit installiert ist, wählen Sie in der Dropdown-Liste den entsprechenden Mandanten aus. Mit der Option "öffentlich (freigegeben)" wird das Objekt für alle Mandanten erstellt.

So erstellen Sie einen Kommentartyp

1. Wählen Sie auf der Registerkarte "Administration" die Option "Knowledge" > "Dokumente" > "Kommentartypen".

Die Seite "Kommentartypen - Liste" wird angezeigt.

2. Klicken Sie auf "Neu erstellen".

Die Seite "Neuen Kommentartyp erstellen" wird angezeigt.

3. Füllen Sie die Felder nach Bedarf aus. Die folgenden Felder erfordern eine Erklärung:

Zeit bis Abschluss (Tage)

Legt fest, wie viele Tage der Anwender diesen Kommentartyp nachverfolgen muss.

In Anwenderansicht anzeigen

Zeigt den Kommentar in verschiedenen Listenansichten auf der Benutzeroberfläche an.

Nachverfolgung erforderlich

Gibt an, ob der Anwender auf diesen Kommentar reagieren muss.

Klicken Sie auf "Speichern".

Der neue Kommentartyp wird auf der Seite "Kommentartyp - Liste" aufgeführt.

Bearbeiten von Kommentartypen

Sie können einen Kommentartyp aktualisieren, der bereits auf der Seite "Kommentartyp - Liste" erstellt worden ist.

So bearbeiten Sie einen Kommentartyp

1. Führen Sie in der Kommentartyp-Liste folgende Schritte aus:

- Wählen Sie einen Kommentar, und wählen Sie auf der Seite "Kommentartyp-Details" die Option "Bearbeiten".
- Klicken mit der rechten Maustaste auf einen Kommentar und wählen Sie aus dem Kontextmenü die Option "Bearbeiten".

Die Seite "Kommentartyp - Detail" wird angezeigt.

2. Füllen Sie die Felder nach Bedarf aus.

3. Klicken Sie auf "Speichern".

Der aktualisierte Kommentartyp wird auf der Seite "Kommentartyp - Liste" aufgeführt.

Dokument-Benachrichtigungen

In CA SDM können Sie eine Liste von Benutzern einrichten, die als Kontakte bezeichnet werden und die bei Eintreten bestimmter Ereignisse benachrichtigt werden können. Der Benachrichtigungsprozess informiert Personen über den Änderungsstatus eines Dokuments und hält sie so über den Fortschritt des Dokuments auf dem Laufenden. Nur Benutzer, die in dieser Liste enthalten sind, können die Benachrichtigungen erhalten, die diesem Dokument zugewiesen wurden.

Festlegen von Benachrichtigungen für Nachverfolgungskommentare

In einigen Standard-Aktivitätsbenachrichtigungen, die auf der Seite "Aktivitätsbenachrichtigungen-Liste" können Sie Benachrichtigungen an Anwender eingeben, wenn diesen ein Nachverfolgungskommentar zugewiesen ist.

Die Warteschlange "Nachverfolgungskommentare" im Scoreboard ist das Repository für zugewiesene und nicht-zugewiesene Nachverfolgungskommentare.

Einrichten von Benachrichtigungen für Nachverfolgungskommentare

1. Wählen Sie auf der Registerkarte "Administration" die Option "Benachrichtigungen" > "Aktivitätsbenachrichtigungen" aus.
Die Seite "Aktivitätsbenachrichtigungen - Liste" wird angezeigt.
2. Wählen Sie *eine* der folgenden Aktivitätsbenachrichtigungen aus:
 - Nachverfolgungskommentar zugewiesen
 - Nachverfolgungskommentar geschlossenDie Seite "Aktivitätsbenachrichtigung - Detail" wird angezeigt.
3. Klicken Sie auf "Bearbeiten".
Die Seite "Aktivitätsbenachrichtigung aktualisieren" wird angezeigt.
4. Ändern Sie die Felder nach Bedarf.
5. Klicken Sie auf "Speichern".
Die Seite "Aktivitätsbenachrichtigung - Detail" wird angezeigt.
6. Klicken Sie auf "Fenster schließen".
Die geänderte Aktivitätsbenachrichtigung wird in der Liste der Aktivitätsbenachrichtigungen aufgeführt, wenn Sie die Liste erneut anzeigen.

Festlegen der Dokumenteinstellungen

Wenn Sie Systemadministrator sind, können Sie Einstellungen festlegen, die mit Kommentaren, Absenden von Knowledge und Anzeigen von Knowledge-Baumstruktur-Dokumenten verbunden sind.

So legen Sie Dokumenteinstellungen fest

1. Wählen Sie auf der Registerkarte "Administration" die Option "Knowledge" > "Dokumente" > "Dokumenteinstellungen".

Die Seite "Dokumenteinstellungen" wird angezeigt.

2. Füllen Sie die folgenden Felder aus:

Knowledge-Baumstrukturdokument – Ansicht

Gibt den Ansichtsmodus an, in dem Knowledge-Baumstrukturdokumente geöffnet werden. Wählen Sie im Baumstrukturmodus (Standard) die Option "Öffnen", um die Knowledge-Baumstruktur direkt zu öffnen oder klicken Sie im Dokumentmodus auf "Öffnen", um das Dokument in der Dokumentansicht zu öffnen. Wenn Sie die Baumstruktur im Dokument-Modus öffnen, klicken Sie auf "Anzeigen", um die Knowledge-Baumstruktur anzuzeigen.

Kommentare

Gibt an, ob Anwender Kommentare für Dokumente absenden und Dokumentkommentare anzeigen können. Wählen Sie eine der folgenden Optionen:

- **Absenden und Anzeigen von Kommentaren zulassen (Standard)** - Zeigt ein Kommentarfeld unten in einem offenen Dokument, so dass Anwender Kommentare für das Dokument absenden können. Die Anwender können die Kommentare anzeigen, die mit dem geöffneten Dokument bereits verknüpft sind.
- **Absenden von Kommentaren zulassen, Anzeigen von Kommentaren nicht zulassen** - Zeigt ein Kommentarfeld rechts in einem offenen Dokument, so dass Anwender Kommentare für das Dokument absenden können. Die Anwender können keine Kommentare anzeigen, die mit dem geöffneten Dokument bereits verknüpft sind.

- **Weder Absenden noch Anzeigen von Kommentaren zulassen**-Verweigert Anwendern die Möglichkeit, Kommentare abzusenden oder anzusehen. Das Kommentarfeld wird in einem geöffneten Dokument nicht angezeigt.

Knowledge absenden

Legt das Repository für vom Anwender abgesendeten Dokumente. Die Liste wird automatisch mit den Namen der Repositories ausgefüllt, die im Bereich "Anhangsbibliothek" definiert wurden.

Lesen Sie sich folgende Informationen sorgfältig durch:

- Wenn ein Analyst ein Dokument in einer Kategorie erstellt, die einen Eigentümer hat, und das Dokument dem Eigentümer der Kategorie zuweist:

Der Eigentümer der Kategorie wird zum Verantwortlichen und zum Eigentümer dieses Dokuments.

Der Eigentümer der Kategorie sollte eine Benachrichtigung erhalten, die besagt, dass das Dokument zugewiesen wurde.

- Wenn ein Analyst ein Dokument in einer Kategorie erstellt, die keinen Eigentümer hat, und das Dokument dem Eigentümer der Kategorie zuweist:

Niemand wird zum Verantwortlichen oder Eigentümer dieses Dokuments.

Das Absenden der KD-Benachrichtigung sollte so gesendet werden wie vom Administrator definiert.

- Wenn ein Analyst ein Dokument erstellt und das Dokument dem Eigentümer der Kategorie zuweist:

Dieser Anwender wird zum Verantwortlichen und Eigentümer.

Es wird keine Benachrichtigung gesendet.

- Wenn ein Mitarbeiter oder Kunde neue Dokumente erstellt, führt CA SDM die in den ersten beiden Punkten dargelegten Aktionen aus.

Maximale Größe der Lösung:

Definiert die maximale Anzahl der Zeichen, die im Feld "Lösung" eines Dokuments enthalten sein können

Grenzwerte: Es können maximal 256.000 Zeichen verwendet werden.

Standard: 32768.

Doppelte Dokumente vermeiden

Erzwingt eine Suche nach ähnlichen Dokumenten, wenn der Anwender ein Knowledge-Dokument erstellt.

Benachrichtigung vor Ablauf

Definiert die Anzahl der Tage, bis das Dokument abläuft und eine Benachrichtigung gesendet wird.

Standard: 7

Hinweis: Dieser Wert gilt nur für Dokumente, die in CA SDM aktualisiert oder erstellt wurden. Wenn Sie Dokumente von CA SDM r11,2 migrieren, und die Ablaufdaten vor der Migration liegen, trifft diese Option nicht zu, es sei denn, Sie aktualisieren das Dokument nach der Migration.

Klicken Sie auf "Speichern".

Die Änderungen gelten, wenn Sie ein Knowledge-Dokument oder ein Knowledge-Baumstruktur-Dokument öffnen.

Dokumentvorlagen

Sie können Dokumentvorlagen benutzen, um das Layout und den Standardinhalt von Knowledge-Dokumenten festzulegen. Jedes Knowledge-Dokument verfügt über eine Dokumentvorlage, die seine Eigenschaften und das Layout näher bestimmen, wenn es von Anwendern geöffnet wird. Standardmäßig werden neue Knowledge-Dokumente mit einer vordefinierten Vorlage verknüpft.

Der HTML-Editor dient zum Durchführen folgender Aufgaben:

- Entwerfen von Dokumentvorlagen, die später auf der Seite "Dokument-Editor" > Registerkarte "Inhalte", mit einem Dokument verknüpft werden können.
- Ändern der vordefinierten und anderer Vorlagen.

Durch Bearbeiten vorhandener Vorlagen können Sie neue Vorlagen erstellen, die mit Dokumenten verknüpft werden können. Sie können die Option "Eigenschaften" auswählen und den Header sowie den Textabschnitt im HTML-Editor bearbeiten.
- Aktualisierung von Dokumentvorlagen aus einem vorherigen Release, um [Knowledge-Beziehungen](#) (siehe Seite 1037), wie z. B. übergeordnete/untergeordnete Beziehungen, zu unterstützen.

Dokumentvorlage erstellen

Eine Dokumentvorlage spezifiziert den Inhalt und das Format von Dokumenten in der Knowledge Base. Sie können die folgenden Standardvorlagen anwenden:

- Integriert: Knowledge-Dokument
- Integriert: Knowledge-Struktur
- Integriert: Schnellobarbeitung

Das Produkt verwendet die Standardvorlagen, wenn Sie Knowledge-Dokumente und Knowledge-Baumstruktur-Dokumente erstellen, es sei denn, es sind neue Dokumentvorlagen erstellt und mit Ihren Dokumenten verknüpft worden.

Hinweis: Wenn Sie ein Knowledge-Dokument erstellen, wählen Sie den entsprechenden Mandanten aus der Dropdown-Liste. Mit der Option "öffentlich (freigegeben)" wird das Objekt für alle Mandanten erstellt.

Erstellen einer Dokumentvorlage

1. Wählen Sie auf der Registerkarte "Administration" die Option "Knowledge" > "Dokumente" > "Dokumentvorlagen".

Die Seite "Dokumentvorlagen-Liste" wird angezeigt.

2. Klicken Sie auf "Neu erstellen".

Die Seite "Neue Dokumentvorlage erstellen" wird angezeigt.

3. Füllen Sie die folgenden Felder aus:

Vorlage

(Erforderlich) Definiert einen eindeutigen Namen für die Vorlage.

Detail

Zeigt den statischen Inhalt an, der in Dokumenten angezeigt wird, die mit der aktuellen Vorlage erstellt wurden. Wenn Sie die Option "HTML-Quelle" auswählen, können Sie den HTML-Code für den Textkörper direkt im Feld "Text" bearbeiten. Wenn Sie die Option "Schnellansicht" auswählen, wird das Feld "Text" als schreibgeschütztes Feld eingeblendet. Der statische Textkörperinhalt in diesem Feld wird so angezeigt, wie er während der Laufzeit dargestellt wird.

4. (Optional) Klicken Sie auf "Standardwerte festlegen".

Die Seite "Vorlage mit Standardwerten" wird angezeigt.

Sie können Standardwerte setzen, wenn Sie ein Dokument erstellen. Wenn Sie die Vorlage eines bestehenden Dokuments ändern, hat dies keine Auswirkungen.

5. (Optional) Sie können Titel, Zusammenfassung, Problem oder Lösung in Ihrer Vorlage ausblenden.

Sie können diese Felder ausblenden, wenn Sie ein einfaches Dokument wie eine Frage-und-Antwort-Vorlage haben möchten.

6. Klicken Sie auf "Details bearbeiten".

Die HTML-Editor-Seite wird angezeigt und Sie können den statischen Inhalt und das Layout von Dokumenten festlegen, welche die Vorlage verwenden. Sie können den Code mit der Symbolleiste bearbeiten, um Platzhalter-Tags einzufügen.

Wichtig! Sie können Knowledge-Beziehungen wie über- und untergeordnete sowie verwandten Verknüpfungen entfernen, indem Sie die {TAG_PARENT} and {TAG_RELATED}-Tags aus der Vorlage entfernen.

7. Klicken Sie auf "OK".

Im Feld "Detail" wird der aktualisierte Inhalt angezeigt.

8. (Optional) Klicken Sie auf "Schnellansicht".

Zeigt den Inhalt und wie er in Dokumenten angezeigt wird, die auf der Vorlage basieren.

9. (Optional) Klicken Sie auf "HTML".

Zeigt den Inhalt als HTML-Code.

10. Klicken Sie auf "Speichern".

Die Seite "Dokumentvorlage - Detail" wird angezeigt.

11. Klicken Sie auf "Fenster schließen".

In den neuen Dokumenten, die auf der Vorlage beruhen, werden der neue Inhalt und das neue Layout angezeigt.

Der Name der Vorlage wird in der Vorlage-Liste angezeigt, wenn Sie die Liste erneut anzeigen lassen.

Hinweis: Änderungen am Dokument, das die Vorlage verwendet, werden angezeigt, wenn nach dem eine neue Sitzung nach dem Anmelden gestartet wird.

Bearbeiten von Dokumentvorlagen

Sie können den Namen, das Layout und den Inhalt einer Vorlage mit Knowledge Management anpassen.

So aktualisieren Sie eine Dokumentvorlage:

1. Wählen Sie auf der Registerkarte "Administration" die Option "Knowledge" > "Dokumente" > "Dokumentvorlagen".

Der Fensterbereich "Dokumentvorlagen - Liste" wird angezeigt.

2. Wählen Sie einen Vorlagennamen aus.

Die Seite "Dokumentvorlage aktualisieren" wird angezeigt.

3. Klicken Sie auf "Details bearbeiten".

Der HTML-Editor wird geöffnet.

4. Ändern Sie den Namen, den Inhalt oder das Layout der Vorlage. Sie können folgende Felder ändern:

Vorlage

Definiert einen eindeutigen Namen für die Vorlage. Dieses Feld erfordert eine Eingabe.

Detail

Zeigt den statischen Inhalt an, der in Dokumenten angezeigt wird, die mit der aktuellen Vorlage erstellt wurden. Wenn Sie die Option "HTML-Quelle" auswählen, können Sie den HTML-Code für den Textkörper direkt im Feld "Text" bearbeiten. Wenn Sie die Option "Schnellansicht" auswählen, wird das Feld "Text" als schreibgeschütztes Feld eingeblendet. Der statische Textkörperinhalt in diesem Feld wird so angezeigt, wie er während der Laufzeit dargestellt wird.

5. Klicken Sie auf "Details bearbeiten", um den statischen Inhalt und das Layout von Dokumenten festzulegen, welche die Vorlage verwenden.

Das Fenster "HTML-Editor" wird geöffnet.

6. Bearbeiten Sie den Code mit der Symbolleiste, um Platzhalter-Tags einzufügen. Klicken Sie auf "OK".

Im Feld "Detail" wird der aktualisierte Inhalt angezeigt.

7. (Optional) Klicken Sie auf "Schnellansicht".

Der Inhalt wird als Dokument angezeigt, basierend auf der Vorlage.

8. (Optional) Klicken Sie auf "HTML".

Der Inhalt wird als HTML-Code angezeigt.

9. Klicken Sie auf "Speichern".

Die Seite "Dokumentvorlage - Detail" wird angezeigt.

10. Klicken Sie auf "Fenster schließen".

In den neuen Dokumenten, die auf der Vorlage beruhen, werden der neue Inhalt und das neue Layout angezeigt.

Eine Änderung des Vorlagennamens wird in der Liste immer dann angezeigt, wenn Sie die Liste aktualisieren.

Auflisten von Dokumentvorlagen

Auf der Seite "Dokumentvorlage – Liste" können Sie Dokumentvorlagen erstellen und verwalten, in denen der Inhalt und das Layout von Dokumenten in der Knowledge Base definiert wird.

Die folgenden Standardvorlagen werden mit der Anwendung installiert:

- Integriert: Knowledge-Dokument
- Integriert: Knowledge-Struktur
- Integriert: Schnellbearbeitung

Das Produkt verwendet die Standardvorlagen, wenn Sie Knowledge-Dokumente und Knowledge-Baumstruktur-Dokumente erstellen, es sei denn, es sind neue Dokumentvorlagen erstellt und mit Ihren Dokumenten verknüpft worden.

Hinweis: Wenn die Mandantenfähigkeit installiert ist, zeigt die Listenseite die Einstellungen für Mandant und öffentliche Daten im Suchfilter an. Öffentliche Daten können in Mandantendaten eingeschlossen oder aus diesen ausgeschlossen werden. Es werden ausschließlich öffentliche Objekte gesucht. Wählen Sie auf Detailseiten den geeigneten Mandanten in der Liste aus. Wenn Sie <leer> wählen, ist das Objekt öffentlich.

Um Dokumentvorlagen aufzulisten, wählen Sie auf der Registerkarte "Administration" die Option "Knowledge" > "Dokumente" > "Dokumentvorlagen".

Die Seite "Dokumentvorlagen" wird angezeigt; die folgenden Spalten werden aufgeführt:

Vorlagenname

Listet die Dokumentvorlagen auf die derzeit im System definiert sind. Wählen Sie einen Vorlagenname, um das Fenster "Dokumentvorlage aktualisieren" zu öffnen. Klicken Sie mit der rechten Maustaste auf einen Vorlagennamen, um das Kontextmenü "Vorlagenname" zu öffnen, in dem Befehle für das Arbeiten mit der ausgewählten Vorlage enthalten sind.

Standard

Ist mit einem Häkchen markiert, um anzuzeigen, dass eine Vorlage standardmäßig für ein neues Dokument verwendet wird oder wenn eine bestimmte Vorlage für ein Dokument gelöscht wurde. Um eine Vorlage als Standardvorlage festzulegen, klicken Sie mit der rechten Maustaste auf den Vorlagennamen. Wählen Sie dann im Kontextmenü die Option "Als Standard festlegen".

Hinweis: Wenn Sie ein neues Dokument erstellen oder eine mit einem Dokument verknüpfte Vorlage löschen, wird dem Dokument die Standardvorlage zugewiesen. (Es sei denn, Sie geben im Fenster "Neues Dokument erstellen" oder im Fenster "Knowledge-Dokument aktualisieren" auf der Registerkarte "Attribute" eine andere Vorlage an.)

Diese Seite enthält die folgenden Felder:

Vorlage

Definiert den Namen der Vorlage, nach der gesucht werden soll. Dieses Feld wird nur angezeigt, wenn Sie auf "Filter anzeigen" klicken.

Weitere Suchargumente

Definiert zusätzliche Kriterien für die Suche. Dieses Feld wird nur angezeigt, wenn Sie im Feld "Knowledge – Suche" auf die Verknüpfung "Weitere" klicken.

Diese Seite enthält die folgenden Schaltflächen:

Filterinhalt löschen

Setzt alle Filterfelder im Bereich oder Fenster auf die jeweiligen Standardwerte zurück.

Neu erstellen:

Öffnet das Fenster "Neue Dokumentvorlage erstellen", in dem Sie eine neue Dokumentvorlage definieren können.

Suchen

Führt eine Suche nach den Elementen durch, die den angegebenen Kriterien entsprechen. Wenn Sie keine Kriterien angeben, werden alle geeigneten Elemente abgerufen (z. B. Ordner/Dokumente, Kontakte, Vorlagen, Füllwörter oder Berechtigungsgruppen).

Filter anzeigen/Filter ausblenden

Blendet Felder ein/aus, mit denen ein Suchvorgang nach Elementen im aktuellen Fenster, Bereich oder Dialogfeld gefiltert werden kann.

Hinweis: Sie können Ergebnislisten nach Excel exportieren, um sie außerhalb von CA SDM zu verwenden. Klicken Sie dazu auf der Listenseite auf die Schaltfläche "Exportieren".

Filtern der Dokumentvorlagenliste

Die Standardvorlagen werden verwendet, wenn Sie Knowledge-Dokumente und Knowledge-Baumstruktur-Dokumente erstellen, es sei denn, es sind neue Dokumentvorlagen erstellt und mit Ihren Dokumenten verknüpft worden. Auf der Seite "Dokumentvorlage – Liste" können Sie Dokumentvorlagen erstellen und verwalten, in denen der Inhalt und das Layout von Dokumenten in der Knowledge Base definiert wird. Sie können von dieser Seite aus Vorlagen filtern.

So filtern Sie die Dokumentvorlagen-Liste

1. Klicken Sie auf die Registerkarte "Administration".
Die Seite "Administration" wird angezeigt.
2. Klicken Sie auf "Knowledge" > "Dokumente" > "Dokumentvorlagen".
Die "Dokumentvorlagen-Liste" wird angezeigt.
3. Führen Sie *einen* der folgenden Vorgänge aus:
 - Wählen Sie eine Vorlage aus der Spalte "Vorlagenname" aus.
Die Vorlage wird geöffnet.
 - Suchen einer Vorlage mit der Suchfunktion
Die Vorlagen-Suchergebnisse werden angezeigt.
 - Wählen Sie "Filter anzeigen", um Ihre Suche zu filtern.
Die Vorlagen-Suchergebnisse werden gefiltert.

Aktualisieren Sie "Dokumentvorlagen", um Knowledge-Beziehungs-Links zu zeigen.

Sie können Knowledge-Dokumentvorlagen aus einer früheren Version von CA SDM aktualisieren, um Knowledge-Beziehungen anzuzeigen. Sie können die Vorlage ändern, indem Sie {TAG_PARENT} und {TAG_RELATED} -Tags hinzufügen, so dass Dokumente, welche die Vorlage nutzen, Dokumentbeziehungen wie über- und untergeordnete Links anzeigen können.

So ändern Sie Vorlagen, um Knowledge-Beziehungen anzuzeigen

1. Öffnen Sie die Knowledge-Vorlage.

Die Seite "Dokumentvorlage aktualisieren" wird angezeigt.

2. Klicken Sie auf "Bearbeiten".

3. Wählen Sie die Ansicht "HTML-Quellcode".

Hinweis:Sie können auch auf "Detail bearbeiten" klicken, den HTML-Editor öffnen und die {TAG_PARENT}- und {TAG_RELATED}-Tags hinzufügen.

4. Klicken Sie im Dropdown-Menü "Detail bearbeiten" auf *Platzhalter für die Vorlage auswählen*, um der Dokumentvorlagen Tags hinzuzufügen.

Die Tags werden der Vorlage hinzugefügt.

5. Speichern und schließen Sie die Vorlage

Die Vorlage wird aktualisiert, um Knowledge-Beziehungen anzuzeigen.

Erstellen von Verknüpfungen für Knowledge-Dokumente

Sie können Ihre Knowledge Management-Umgebung durch das Erstellen von Dokumentverknüpfungen verwalten. Mit Hilfe von Knowledge-Beziehungen können Sie Dokumenthierarchien erstellen und Änderungen an Ihren Knowledge-Dokumenten verwalten.

Gehen Sie beim Erstellen von Knowledge-Beziehungen folgendermaßen vor:

1. Definieren Sie Vorlagen für Knowledge-Dokumente, um die Beziehungen für über-/untergeordnete Dokumente im Ansichtsmodus ein- oder auszublenden.
2. Erstellen oder bearbeiten Sie ein Knowledge-Dokument.

Hinweis: Sie können standardmäßig nur einem unveröffentlichten Knowledge-Dokument Verknüpfungen hinzufügen. Wenn das Dokument bereits veröffentlicht ist, öffnen Sie das Dokument im Bearbeitungs- oder Überarbeitungsmodus, um Dokumentverknüpfungen zu erstellen. Sie können die Berechtigungen für Dokumente vor dem Genehmigungsvorgang und nach dem Veröffentlichen bearbeiten.

3. Erstellen Sie je nach Bedarf für Ihre Knowledge Management-Umgebung auf der Registerkarte "Verwandtes Knowledge" *eine* von den folgenden Dokumentverknüpfungen:

- Verknüpfen Sie das Dokument mit einem nichthierarchischen "Siehe auch".
Sie können Knowledge-Dokumente auch mit anderen existierenden Dokumenten verknüpfen.
- Verknüpfen Sie das Dokument als ein über- oder untergeordnetes Dokument.
Sie können Knowledge-Dokumente in übergeordneten/untergeordneten Beziehungen verknüpfen.

Hinweis: Wenn Sie ein übergeordnetes Dokument bearbeiten, wird eine Warnung mit der Meldung angezeigt, dass dies Auswirkungen auf untergeordnete Dokumente haben kann.

- Verknüpfen Sie das globale Dokument mit einem Mandantendokument.
Sie können Knowledge-Dokumente mit einem einzigen oder mit mehreren Mandanten verknüpfen. Beispielsweise kann ein untergeordnetes Dokument einen anderen Mandanten als das übergeordnete Dokument haben.

Die Registerkarte "Verlauf" wird aktualisiert, wenn Sie Dokumentverknüpfungen zur Überwachung von Änderungen erstellen.

4. Speichern Sie das Dokument und überprüfen Sie, dass die Verknüpfungen angezeigt werden, wenn Sie das Dokument in der Anwenderansicht öffnen.

Sie können überprüfen, ob die Dokumentverknüpfungen entsprechend den von Ihnen festgelegten Berechtigungen angezeigt werden.

Erstellen von über-/untergeordneten Verknüpfungen

Sie können über-/untergeordnete Beziehungen für Knowledge-Dokumente erstellen. Verwenden Sie über-/untergeordnete Verknüpfungen, um zugehörige Dokumente für Benutzer in Ihrer Umgebung zu organisieren.

So erstellen Sie über-/untergeordneten Verknüpfungen

1. Erstellen Sie ein Knowledge-Dokument oder öffnen Sie ein Dokument im Bearbeitungsmodus.

Das Knowledge-Dokument wird angezeigt.

2. Wählen Sie die Registerkarte "Verwandtes Knowledge".

Die Seite "Kategorien" wird angezeigt.

Hinweis: Sie können Verknüpfungen auch auf der Registerkarte "Ähnliche suchen" erstellen. Verwenden Sie Suchkriterien, um Dokumente zu finden.

3. Suchen Sie das Dokument, das Sie mit dem Fensterbereich "Kategorien (X)" verknüpfen möchten.

Klicken Sie mit der rechten Maustaste auf das Dokument im Dokument-Fensterbereich und wählen Sie auf die Option *Als übergeordnetes Element verknüpfen* oder *Als untergeordnetes Element verknüpfen*, um die Dokumente zu verknüpfen.

Die Dokumentverknüpfung wird erstellt.

Erstellen einer "Siehe auch"-Verknüpfung

Sie können eine "Siehe auch"-Beziehung für Knowledge-Dokumente in Ihrer Umgebung erstellen. Verwenden Sie "Siehe auch"-Beziehungen, um Knowledge-Hierarchien in Ihrer Umgebung zu verwalten.

So erstellen Sie eine "Siehe auch"-Verknüpfung

1. Erstellen Sie ein Knowledge-Dokument oder öffnen Sie ein Dokument im Bearbeitungsmodus.

Das Knowledge-Dokument wird angezeigt.

2. Wählen Sie die Registerkarte "Verwandtes Knowledge".

Die Seite "Kategorien" wird angezeigt.

Hinweis: Sie können Verknüpfungen auch auf der Registerkarte "Ähnliche suchen" erstellen.

3. Suchen Sie das Dokument, das Sie mit dem Fensterbereich "Kategorien (X)" verknüpfen möchten.

Klicken Sie mit der rechten Maustaste auf das Dokument im Dokument-Fensterbereich und wählen Sie auf die Option *Dieses Dokument mit "Siehe auch" verknüpfen*.

Die Dokumentverknüpfung wird erstellt.

Entfernen von Dokumentverknüpfungen

Sie können Verknüpfungen aus einem unveröffentlichten Knowledge-Dokument, wie eine über-/untergeordnete Beziehung, entfernen. Wenn das Dokument bereits veröffentlicht ist, öffnen Sie das Dokument im Bearbeitungs- oder Überarbeitungsmodus, um Dokumentverknüpfungen zu entfernen.

So entfernen Sie eine Dokumentverknüpfung

1. Öffnen Sie das Knowledge-Dokument.

Das Dokument wird angezeigt.

2. Klicken Sie auf "Bearbeiten".

Die Seite "Dokument aktualisieren" wird angezeigt.

3. Wählen Sie die Registerkarte "Verwandtes Knowledge".

Die Seite "Kategorien" wird angezeigt.

4. Navigieren Sie zum Fensterbereich "Dokumentverknüpfungen".

5. Wählen Sie im Kontextmenü die Option *Diese Verknüpfung entfernen*, um diese Verknüpfung zu entfernen.

Die Dokumentverknüpfungen wurden entfernt.

Knowledge-Kategorien

Knowledge-Dokumente sind in *Knowledge-Kategorien* arrangiert.

Knowledge-Entwickler, Knowledge Manager, und Administratoren können diese Kategorien verwalten. Jede dieser Personen verwendet Knowledge Management, um Kategorien zu erstellen, zu kopieren und zu ändern. Jedoch können nur Knowledge Manager und Administratoren Kategorien löschen. Wenn Sie die Kategoriestructur der Knowledge-Kategorien erstellen, so ist dies die hierarchische Struktur, die Service Desk-Mitarbeiter, Kunden und Analysten verwenden, um relevante Dokumenten zu suchen.

Sie müssen jedes Dokument einer Hauptkategorie zuordnen. Zum Beispiel muss jedes Knowledge, das sich auf Microsoft Word bezieht, der Kategorie "Microsoft Word" hinzugefügt zu werden. Außerdem können Sie in Knowledge Management ein Dokument mit mehreren sekundären Kategorien und anderen Dokumenten verknüpfen. Auf diese Weise kann ein Dokument unter vielen verschiedenen zutreffenden Kategorien klassifiziert werden und erfolgreichere Suchergebnisse liefern.

Die Kategoriestructur dient Folgendem:

- Organisation von Knowledge-Lösungen in überschaubare Gruppen
 - Vereinfachung der Zuweisung von Zugriffsrechten
 - Suche nach Lösungen mit Hilfe von "FAQ"/"Durchsuchen"
- Um die Funktion, von einem Incident aus Kategorien zu durchsuchen, zu verwenden, müssen der Incident-Bereich und die Knowledge-Kategorie übereinstimmen. Wenn Sie einen Incident erstellen, der auf einem Knowledge-Dokument basiert, legt die Dokumentkategorie den Incident-Bereich fest. Deswegen stimmen die Kategorie und der Bereich immer überein.
- Erstellen einer Dokumentverknüpfung: Ein Verweis vom Typ "*Siehe auch*" erscheint, wenn ein beliebiges der verknüpften Dokumente angezeigt wird. Die Verknüpfung "*Siehe auch*" ermöglicht Ihnen, direkt von einem verknüpften Dokument zu einem anderen zu springen.

Erstellen von Knowledge-Kategorien

Für jede Kategorie können Sie Eigenschaften definieren, die Attribute oder Qualitäten identifizieren, die mit dem Ticket verbunden werden sollen. Außerdem können Sie einen Workflow erstellen, der alle einzelnen Aufgaben identifiziert, die zur Erfüllung des Tickets erforderlich sind.

Mithilfe von Kategorien können Sie Standardwerte für bestimmte Felder in Tickets angeben. Alternativ können Sie Kategorien einen Standardservicetyp zuweisen, um Tickets automatisch einem Service Level zuzuordnen. Wenn ein Analyst einem Ticket eine Kategorie zuweist, werden alle Informationen, die Sie mit der Kategorie verknüpfen, automatisch mit dem Ticket verknüpft.

Hinweis: Wenn Sie die Option Mandantenfähigkeit verwenden, wird im Suchfilter des Knowledge-Dokuments eine Mandanten-Dropdown-Liste angezeigt. Wenn Sie in dieser Dropdown-Liste "<leer>" auswählen, ist die Suche öffentlich. Auf der Listenseite wird auch eine Mandantenspalte angezeigt.

So erstellen Sie eine neue Kategorie

1. Wählen Sie auf der Registerkarte "Administration" die Option "Knowledge" > "Knowledge-Kategorien" aus.
Die Seite "Knowledge-Kategorien" wird angezeigt.
2. Klicken Sie mit der rechten Maustaste auf die Kategorie, unter der Sie die Kategorie erstellen möchten. Wählen Sie im Kontextmenü die Option "Neue Kategorie".
In der Registerkarte "Inhalt" wird das Fenster "Neue Kategorie erstellen" geöffnet.
3. Füllen Sie die [Felder](#) (siehe Seite 1044) nach Bedarf aus.
4. Klicken Sie auf "Berechtigungen".
Die Registerkarte "Berechtigungen" wird angezeigt.
5. Markieren Sie eine der folgenden Berechtigungsoptionen für die Kategorie:

Von übergeordnetem Element übernehmen

Legt fest, dass die neue Kategorie dieselben Berechtigungseinstellungen aufweist wie die übergeordnete Kategorie.

Hinweis: Die Option "Von übergeordnetem Element übernehmen" steht nicht zur Verfügung, wenn Sie die oberste Kategorie auswählen, bevor Sie das Fenster "Kategorie erstellen" öffnen.

Steuerung nach Gruppe

Gibt Kategorieberechtigungen für Gruppen an und gewährt Lese- oder Schreibzugriff auf die Kategorie.

Steuerung nach Rolle

Gibt Kategorieberechtigungen für Rollen an und gewährt Lese- oder Schreibzugriff auf die Kategorie.

Hinweis: Wenn Sie die Steuerung der Kategorieberechtigung beispielsweise von Gruppe in Rolle ändern, wird eine Warnung angezeigt, die Sie darauf hinweist, dass die vorigen Berechtigungen für diese Kategorie gelöscht werden.

Allen Anwendern Schreibberechtigung erteilen

Gibt an, dass alle Anwender Schreibzugriff auf die Kategorie haben. Schreibzugriff bedeutet, dass Sie diese Kategorie bearbeiten oder löschen können.

Hinweis: Das Kontrollkästchen "Allen Anwendern Leseberechtigung erteilen" wird automatisch aktiviert, wenn Sie das Kontrollkästchen "Allen Anwendern Schreibberechtigung erteilen" aktivieren.

Allen Anwendern Leseberechtigung erteilen

Gibt an, dass alle Anwender Lesezugriff auf die Kategorie haben. Leseberechtigung bedeutet, dass Sie die Kategorie anzeigen, jedoch nicht bearbeiten oder löschen können. Anwender mit Administratorrechten können einen Ordner bearbeiten, selbst wenn die ihnen zugeordnete Gruppe dies nicht kann. Gehört ein Anwender zu mehreren Berechtigungsgruppen mit unterschiedlichen Zugriffsebenen auf die Kategorie, erhält er die höchste verfügbare Zugriffsebene (wenn zum Beispiel eine Gruppe nur Lesezugriff und die andere Schreibzugriff hat, erhält der Anwender Schreibzugriff).

Hinweis: Das Kontrollkästchen "Allen Anwendern Leseberechtigung erteilen" wird automatisch aktiviert, wenn Sie das Kontrollkästchen "Allen Anwendern Schreibberechtigung erteilen" aktivieren.

Wichtig: Wenn Sie die Berechtigung für "Alle" vergeben, ist der Zugriff nach Rolle oder nach Gruppe derselbe. Wenn Sie "Alle" und "Steuerung nach Rolle" ausgewählt haben und die Berechtigungen speichern, wird "Steuerung nach Gruppe" markiert.

6. (Optional) Spezifizieren Sie die Berechtigungen für Lesen/Schreiben für bestimmte Gruppen oder Rollen aus den Listen "Verfügbar" und "Ausgewählt".

Mit dieser Option legen Sie fest, welche Gruppen oder Rollen über Lese- bzw. Schreibzugriff auf die Kategorie verfügen. In der Liste der verfügbaren Gruppen/Rollen können Sie eine oder mehrere Berechtigungsgruppen oder -rollen auswählen und diese mit den Schaltflächen "Hinzufügen" und "Entfernen" in die Listen der Gruppen/Rollen mit Schreibzugriff bzw. mit Lesezugriff übernehmen.

7. Klicken Sie auf "Speichern".

Die Seite "Change-Kategorie - Detail" wird angezeigt.

8. Klicken Sie auf "Fenster schließen".

Der Fensterbereich "Knowledge-Kategorien" wird aktualisiert und zeigt die neue Kategorie an.

Weitere Informationen:

[Kategoriefelder](#) (siehe Seite 1044)

Kategoriefelder

Titel

Bezeichnet die Kategorie.

Beschreibung

Beschreibt die Kategorie.

Eigentümer der Kategorie

Gibt die Person an, die für die Kategorie verantwortlich ist. Wenn ein Kontakt als Eigentümer einer Kategorie definiert ist, ist für ihn auf der Knowledge-Berichtskarte eine Verknüpfung mit der Bezeichnung "Meine Kategorien" angezeigt. Hier können Statistiken für die jeweilige Kategorie und die darin enthaltenen Dokumente angezeigt werden. Diese Person ist auch der Standardeigentümer für neue Dokumente in der Kategorie, wenn der die Dokumente erstellende Anwender kein Analyst ist, oder wenn ein Analyst die Dokumente mit der aktivierten Option "Eigentümer der Kategorie zuweisen" erstellt.

Dokumentenvorlage

Definiert die Dokumentvorlage, die für alle mit dieser Kategorie verknüpften Dokumente verwendet werden soll. Die Option "<empty>" bedeutet, dass keine Optionen definiert sind, jedoch standardmäßig die vordefinierte Vorlage verwendet wird.

Vorlage für den Genehmigungsvorgang

Definiert die Standardvorlage, die für den Genehmigungsvorgang für alle Dokumente verwendet werden soll, die mit dieser Kategorie verknüpft sind. Die Vorlage für den Genehmigungsvorgang definiert die Arbeitsschritte, durch die ein Dokument vor seiner Veröffentlichung gehen muss. Der Standardwert ist "<empty>". Das heißt, dass die Standardvorlage der Anwendung verwendet wird.

Zulassen, dass in dieser Kategorie Foren erstellt werden

Gibt an, ob Analysten in dieser Kategorie Foren erstellen können.

Request-/Incident-/Problembereich

Bezeichnet einen Request-/Incident-/Problembereich, den Ihr Administrator definiert, um einen Zuständigkeitsbereich zu bezeichnen. Klicken Sie auf das Suchsymbol, um aus den verfügbaren Bereichen auszuwählen.

Issue-Kategorie

Bezeichnet eine Issue-Kategorie, die Ihr Administrator definiert, um einen Zuständigkeitsbereich zu bezeichnen. Klicken Sie auf das Suchsymbol, um aus den verfügbaren Bereichen auszuwählen.

Ändern einer Kategorie

Sie können eine Kategorie in Ihrer Knowledge Management-Umgebung ändern. Kategorien bestimmen den Inhalt von Changes und Issues nach ihrer Erstellung. Für jede Kategorie können Sie Eigenschaften definieren, die Attribute oder Qualitäten identifizieren, die mit dem Ticket verbunden werden sollen. Außerdem können Sie einen Workflow erstellen, der alle einzelnen Aufgaben identifiziert, die zur Erfüllung des Tickets erforderlich sind.

Mithilfe von Kategorien können Sie Standardwerte für bestimmte Felder in Tickets angeben. Alternativ können Sie Kategorien einen Standardservicetyp zuweisen, um Tickets automatisch einem Service Level zuzuordnen. Wenn ein Analyst einem Ticket eine Kategorie zuweist, werden alle Informationen, die Sie mit der Kategorie verknüpfen, automatisch mit dem Ticket verknüpft.

So ändern Sie eine Kategorie

1. Wählen Sie auf der Registerkarte "Administration" die Option "Knowledge" > "Knowledge-Kategorien" aus.
Die Seite "Knowledge-Kategorien" wird angezeigt.
2. Klicken Sie mit der rechten Maustaste auf die Kategorie, die geändert werden soll, und wählen Sie dann im Kontextmenü "Bearbeiten".

In der Registerkarte "Inhalt" wird die Seite "Kategorie aktualisieren" geöffnet.

Hinweis: Die oberste Kategorie können Sie weder löschen noch ändern.

3. Aktualisieren Sie ein oder mehrere [Felder](#) (siehe Seite 1044) je nach Bedarf.
4. Klicken Sie auf "Berechtigungen".

Die Registerkarte "Berechtigungen" wird angezeigt.

5. Markieren Sie eine der folgenden Berechtigungsoptionen für die Kategorie:

Von übergeordnetem Element übernehmen

Legt fest, dass die neue Kategorie dieselben Berechtigungseinstellungen aufweist wie die übergeordnete Kategorie.

Hinweis: Die Option "Von übergeordnetem Element übernehmen" steht nicht zur Verfügung, wenn Sie die oberste Kategorie auswählen, bevor Sie das Fenster "Kategorie erstellen" öffnen.

Steuerung nach Gruppe

Gibt Kategorieberechtigungen für Gruppen an und gewährt Lese- oder Schreibzugriff auf die Kategorie.

Steuerung nach Rolle

Gibt Kategorieberechtigungen für Rollen an und gewährt Lese- oder Schreibzugriff auf die Kategorie. Wenn Sie "Alle" und "Steuerung nach Rolle" ausgewählt haben und die Berechtigungen speichern, wird "Steuerung nach Gruppe" markiert.

Hinweis: Wenn Sie die Steuerung der Kategorieberechtigung beispielsweise von Gruppe in Rolle ändern, wird eine Warnung angezeigt, die Sie darauf hinweist, dass die vorigen Berechtigungen für diese Kategorie gelöscht werden.

6. (Optional) Spezifizieren Sie die Lese-/Schreibberechtigungen für die Kategorie.

Mit dieser Option legen Sie fest, welche Gruppen oder Rollen über Lese- bzw. Schreibzugriff auf die Kategorie verfügen. Wenn Sie diese Option markieren, wird die Seite aktualisiert, um die [Kontrollkästchen](#) (siehe Seite 1049) "Allen Anwendern Schreibberechtigungen erteilen" und "Allen Anwendern Leseberechtigung erteilen" anzuzeigen.

7. Klicken Sie auf "Speichern".

Die geänderte Kategorie wird auf der Seite "Knowledge-Kategorie" angezeigt.

Löschen einer Kategorie

Sie können eine Kategorie aus der Knowledge-Kategorie-Struktur entfernen. Wenn Sie eine Kategorie löschen, können Sie spezifizieren, ob Sie die Unterkategorien der ausgewählten Kategorie und allen zugeordneten Dokumentverknüpfungen entfernen möchten.

Hinweis: Diese Funktion ist nur Systemadministratoren und Knowledge-Managern verfügbar.

So löschen Sie eine Kategorie

1. Wählen Sie auf der Registerkarte "Administration" die Option "Knowledge" > "Knowledge-Kategorien" aus.

Die Seite "Knowledge-Kategorien" wird angezeigt.

2. Klicken Sie mit der rechten Maustaste auf die zu löschende Kategorie und wählen Sie dann im Kontextmenü "Kategorie löschen".

Die Seite "Kategorie löschen" wird angezeigt.

Hinweis: Die oberste Kategorie können Sie weder löschen noch ändern.

3. (Optional) Führen Sie *einen* der folgenden Schritte durch:

- Markieren Sie das Kontrollkästchen "Einschließlich Unterkategorien", um alle Unterkategorien der markierten Kategorie zu löschen.
- Deaktivieren Sie das Kontrollkästchen "Einschließlich Unterkategorien", um all Unterverzeichnisse von der markierten Kategorie in die nächstgelegene übergeordnete Kategorie zu verschieben.

4. (Optional) Führen Sie *einen* der folgenden Schritte durch:

- Markieren Sie das Kontrollkästchen "Dokumente einschließen", um die in der markierten Kategorie verbliebenen Dokumente zu löschen. Wenn Sie das Kontrollkästchen "Dokumente einschließen" markieren, werden die folgenden Optionen angezeigt:
 - **Dokumente löschen, die nur über eine primäre Kategorie verknüpft sind** - Mit dieser Option werden Dokumente gelöscht, für welche die markierte Kategorie im Fenster "Knowledge-Kategorien" als primäre Kategorie des Dokuments gekennzeichnet ist.
 - **Alle Dokumente löschen, die mit dieser Kategorie verknüpft sind** Mit dieser Option werden alle Dokumente in der ausgewählten Kategorie gelöscht.
- Markieren Sie das Kontrollkästchen "Dokumente einschließen", um Dokumente von der markierten Kategorie in die nächstgelegene, übergeordnete Kategorie zu verlagern.

Klicken Sie auf "OK".

Die ausgewählte Kategorie wird gelöscht und der Fensterbereich "Knowledge-Kategorien" wird aktualisiert.

Verschieben von Kategorien

Sie können eine Kategorie, deren Unterkategorien und alle zugeordneten Dokumentverknüpfungen von ihrer aktuellen Position in eine andere Kategorie verschieben.

Hinweis: Diese Funktion ist nur verfügbar, wenn Knowledge Management installiert ist.

Ausschneiden und Einfügen einer Kategorie

1. Wählen Sie auf der Registerkarte "Administration" die Option "Knowledge" > "Knowledge-Kategorien" aus.

Die Seite "Knowledge-Kategorien" wird angezeigt.

2. Klicken Sie mit der rechten Maustaste auf die Kategorie, die verschoben werden soll, und wählen Sie im Menü die Option "Kategorie ausschneiden".

Die Software legt die markierte Kategorie, ihre Unterkategorien und alle zugeordneten Dokumentverknüpfungen im Arbeitsspeicher ab.

3. Klicken Sie mit der rechten Maustaste auf die Kategorie, in die Sie die kopierten Informationen einfügen möchten, und wählen Sie dann im Kontextmenü "Kategorie einfügen".

Die ausgeschnittene Kategorie wird von ihrem ursprünglichen Speicherort unter die ausgewählte Kategorie verschoben. Der Fensterbereich "Knowledge-Kategorien" wird aktualisiert und zeigt die neue Kategoriestructur an.

Kopieren von Kategorien mit Dokumentverknüpfungen

Sie können eine Kopie einer Kategorie, ihren Unterkategorien, und allen assoziierten Dokumentverknüpfungen in eine andere Kategorie einfügen, ohne diese vom ursprünglichen Speicherort zu löschen.

So kopieren Sie eine Kategorie mit Dokumentverknüpfungen und fügen diese ein

1. Wählen Sie auf der Registerkarte "Administration" die Option "Knowledge" > "Knowledge-Kategorien" aus.

Die Seite "Knowledge-Kategorien" wird angezeigt.

2. Klicken Sie mit der rechten Maustaste auf die zu kopierende Kategorie und wählen Sie "Kategorie mit Dokumentverknüpfungen kopieren".

Die Software legt die markierte Kategorie, ihre Unterkategorien und alle zugeordneten Dokumentverknüpfungen im Arbeitsspeicher ab.

3. Klicken Sie mit der rechten Maustaste auf die Kategorie, in die Sie die kopierten Informationen einfügen möchten, und wählen Sie dann "Kategorie einfügen" im Kontextmenü.

Die kopierten Informationen werden unter der ausgewählten Kategorie angezeigt. Der Fensterbereich "Knowledge-Kategorien" wird aktualisiert und zeigt die neue Kategoriestructur an.

Kopieren von Kategorien ohne Dokumentverknüpfungen

Sie können eine Kopie einer Kategorie und ihren Unterkategorien in eine andere Kategorie einordnen, ohne sie von ihrem ursprünglichen Speicherort zu entfernen oder die assoziierten Dokumentverknüpfungen zu kopieren.

So kopieren Sie eine Kategorie ohne Dokumentverknüpfungen und fügen diese ein

1. Wählen Sie auf der Registerkarte "Administration" die Option "Knowledge" > "Knowledge-Kategorien" aus.

Die Seite "Knowledge-Kategorien" wird angezeigt.

2. Klicken mit der rechten Maustaste auf die zu kopierende Kategorie und wählen Sie im Kontextmenü "Kategorie kopieren".

Die Software legt die markierte Kategorie und ihre Unterkategorien im Arbeitsspeicher ab.

3. Klicken Sie mit der rechten Maustaste auf die Kategorie, in die Sie die kopierten Informationen einfügen möchten, und wählen Sie dann "Kategorie einfügen" im Kontextmenü.

Die kopierten Informationen werden unter der ausgewählten Kategorie angezeigt. Der Fensterbereich "Knowledge-Kategorien" wird aktualisiert und zeigt die neue Kategoriestructur an.

Verwalten von Kategorieberechtigungen

Sie können Kategorieberechtigungen in Ihrer Knowledge Management-Umgebung verwalten, indem Sie bestimmte, auf Gruppe oder Rolle basierte, Lese-/Schreibberechtigungen gewähren. Sie können festlegen, wer Unterkategorien anzeigen, bearbeiten, löschen oder einer Kategorie hinzufügen kann.

Hinweis: Sie können leere Schreibberechtigungen für Dokumente und Kategorien verwenden. Wenn Sie keine Schreibberechtigung auswählen, werden leere Schreibberechtigungen festgelegt. Kategorien und Dokumente mit leeren Schreibberechtigungen können nur von berechtigten Anwendern geändert werden.

So verwalten Sie Kategorieberechtigungen:

1. Wählen Sie auf der Registerkarte "Administration" die Option "Knowledge" > "Knowledge-Kategorien" aus.

Die Seite "Knowledge-Kategorien" wird angezeigt.

2. Klicken Sie mit der rechten Maustaste auf die Kategorie, unter der Sie die Kategorie erstellen wollen, und wählen Sie aus dem Kontextmenü die Option "Neue Kategorie" aus, um die Berechtigungen der neuen Kategorie zu verwalten.

Auf der Registerkarte "Inhalt" wird die Seite "Neue Kategorie erstellen" angezeigt.

3. Klicken Sie auf "Berechtigungen".

Die Registerkarte "Berechtigungen" wird angezeigt.

4. Markieren Sie eine der folgenden Berechtigungsoptionen für die Kategorie:

Von übergeordnetem Element übernehmen

Legt fest, dass die neue Kategorie dieselben Berechtigungseinstellungen aufweist wie die übergeordnete Kategorie.

Hinweis: Wenn Sie die erste Kategorie auswählen, bevor Sie die Seite "Kategorie erstellen" öffnen, dann ist die Option "Vo. übergeordneten Element übernehmen" nicht verfügbar.

Steuerung nach Gruppe

Gibt Kategorieberechtigungen für Gruppen an und gewährt Lese- oder Schreibzugriff auf die Kategorie.

Steuerung nach Rolle

Gibt Kategorieberechtigungen für Rollen an und gewährt Lese- oder Schreibzugriff auf die Kategorie.

Hinweis: Wenn Sie die Steuerung der Kategorieberechtigung beispielsweise von "Gruppe" in "Rolle" ändern, wird eine Warnung angezeigt, die Sie darauf hinweist, dass die vorigen Berechtigungen für diese Kategorie gelöscht werden.

Allen Anwendern Schreibberechtigung erteilen

Gibt an, dass alle Anwender Schreibzugriff auf die Kategorie haben. Schreibzugriff bedeutet, dass Sie diese Kategorie bearbeiten oder löschen können.

Hinweis: Das Kontrollkästchen "Allen Anwendern Leseberechtigung erteilen" wird automatisch aktiviert, wenn Sie das Kontrollkästchen "Allen Anwendern Schreibberechtigung erteilen" aktivieren.

Allen Anwendern Leseberechtigung erteilen

Gibt an, dass alle Anwender Lesezugriff auf die Kategorie haben. Leseberechtigung bedeutet, dass Sie die Kategorie anzeigen, jedoch nicht bearbeiten oder löschen können. Anwender mit Administratorrechten können einen Ordner bearbeiten, selbst wenn die ihnen zugeordnete Gruppe dies nicht kann. Gehört ein Anwender zu mehreren Berechtigungsgruppen mit unterschiedlichen Zugriffsebenen auf die Kategorie, erhält er die höchste verfügbare Zugriffsebene (wenn zum Beispiel eine Gruppe nur Lesezugriff und die andere Schreibzugriff hat, erhält der Anwender Schreibzugriff).

Hinweis: Das Kontrollkästchen "Allen Anwendern Leseberechtigung erteilen" wird automatisch aktiviert, wenn Sie das Kontrollkästchen "Allen Anwendern Schreibberechtigung erteilen" aktivieren.

Wichtig: Wenn Sie die Berechtigung für "Alle" vergeben, ist der Zugriff nach Rolle oder nach Gruppe derselbe. Wenn Sie "Alle" und "Steuerung nach Rolle" ausgewählt haben und die Berechtigungen speichern, wird "Steuerung nach Gruppe" markiert.

5. Gewähren Sie in den Listen "Verfügbar" und "Ausgewählt" die geeigneten Lese-/Schreibberechtigungen bestimmten Gruppen oder Rollen.

In der Liste der verfügbaren Gruppen/Rollen können Sie eine oder mehrere Berechtigungsgruppen oder -rollen auswählen und diese mit den Schaltflächen "Hinzufügen" und "Entfernen" in die Listen der Gruppen/Rollen mit Schreibzugriff bzw. mit Lesezugriff übernehmen.

Hinweis: Alle Gruppen oder Rollen, die der Berechtigungsliste hinzugefügt wurden, werden automatisch der Leseberechtigung-Liste hinzugefügt. Wenn Sie das Kontrollkästchen "Allen Anwendern Leseberechtigung erteilen" aktivieren, dann brauchen Sie der Leseberechtigung-Liste keine Gruppen oder Rollen hinzuzufügen.

6. Klicken Sie auf "Speichern".
Die Seite "Change-Kategorie - Detail" wird angezeigt.
7. Klicken Sie auf "Fenster schließen".
Die veränderte Kategorie wird im Fenster "Knowledge-Kategorien" angezeigt.

Berichte und Indikatoren

Sie können die Effizienz der Knowledge Base mit den folgenden Berichterstellungs-Tools überwachen:

- Knowledge-Berichtskarte
- Vordefinierte webbasierte Berichte für Knowledge Management
- Rollenbasierte Webformulare

Mit diesen Tools können Sie Statistiken über den Nutzen Ihrer Dokumente und deren Wirksamkeit beim Lösen von Problemen anzeigen.

Weitere Informationen:

[Knowledge-Berichtskarte](#) (siehe Seite 1051)

[Webbasierte Berichte](#) (siehe Seite 1053)

[Rollenbasierte Berichts-Webformulare](#) (siehe Seite 1053)

Knowledge-Berichtskarte

Die Knowledge-Berichtskarte zeigt Informationen über den Wissensbeitrag jedes Endanwenders an und gibt an, welche der Knowledge-Dokumente am nützlichsten sind. Sie können diese Informationen verwenden, um die Prozesse für das Erstellen von Knowledge-Dokumenten zu optimieren und um Endanwendern in Ihrer Umgebung den bestmöglichen Support anzubieten.

Definieren der Knowledge-Berichtskartenstatistik

Verwenden Sie die Seite "Knowledge-Berichtskarte", um den Ablaufplan zur Berechnung und zum Senden von Knowledge-Berichtskarten-Benachrichtigungen und den Inhalt von Knowledge-Berichtskarten-E-Mail-Benachrichtigungen zu definieren.

Hinweis: Überarbeitungsversionen und deaktivierte Dokumente werden nicht angezeigt, wenn die Knowledge-Berichtskartenberechnung ausgeführt wird.

So definieren Sie eine Knowledge-Berichtskartenstatistik

1. Wählen Sie auf der Registerkarte "Administration" die Option "Knowledge" > "Knowledge-Berichtskarte" aus.

Die Seite "Berichtskarte" wird geöffnet.

2. Füllen Sie die nachstehenden Felder nach Bedarf aus.

Letzte Aktualisierung:

Führt die Berichtskartenberechnung aus.

Standard: Deaktiviert

Hinweis: Wenn die Berechnung nicht ausgeführt wurde und die Statistiken für die Daten nicht zusammengestellt wurden, wird die folgende Meldung angezeigt, wenn Sie auf der Registerkarte "Knowledge" im Menü "Anzeigen" den Befehl "Knowledge-Berichtskarte" auswählen: "Führen Sie eine Berichtskartenberechnung durch".

Ablaufplan

Plant den Ablauf der Berichtskarte aus.

- **Berichtskartenberechnung wird ausgeführt am xxx und wird ausgeführt alle xxx:** Gibt die Häufigkeit an, mit der die Berichtskartenstatistik neu berechnet wird.

- **E-Mail-Benachrichtigung zur Berichtskarte wird gesendet am xxx und wird gesendet alle xxx:** Gibt die Häufigkeit an, mit der Berichtskarten-Benachrichtigungen gesendet werden.

Standard: Nie

- **E-Mail zur Berichtskarte soll Statistiken enthalten für die letzten xxx:** Gibt den Zeitraum an, für den die Berichtskarten-Benachrichtigung Informationen enthalten soll. Dieses Feld ist nicht verfügbar, wenn Sie in der Liste "E-Mail-Benachrichtigung zur Berichtskarte wird gesendet alle xxx" den Wert "Nie" ausgewählt haben.

Standardeinstellung: 365 Tage

3. Klicken Sie auf "Speichern".

Die Knowledge-Berichtskartenstatistik ist definiert.

Webbasierte Berichte

CA Business Intelligence installiert diverse vordefinierte Knowledge Management-Berichte. Diese Berichte werden automatisch nach der CA SDM-Installation auf dem CA Business Intelligence bereitgestellt.

Sie werden entweder mit BusinessObjects Web Intelligence oder Crystal Reports entwickelt. Autorisierte Anwender können Berichte auf der CA SDM-Registerkarte "Berichte" anzeigen.

Rollenbasierte Berichts-Webformulare

Sie können die Berichts-Webformulare definieren, die angezeigt werden, wenn ein autorisierter Manager oder Analyst auf der Registerkarte "Berichte" auf das Symbol "Berichtsliste" klickt.

Berichts-Webformulare werden hier über die Rollenliste verwaltet: "Administration" > "Sicherheit und Rollenverwaltung" > "Rollenverwaltung".

Suchen

Die Suchfunktion ermöglicht Administratoren das Ausführen der folgenden Aufgaben:

- Verwalten der Knowledge Management-Suchmaschine und Definieren der Einstellungen für die Verwendung von Füllwörtern, Sonderbedingungen und Synonymen, die bei der Suche aus- oder eingeschlossen werden.
- Definieren der Einstellungen für die Analyse von Dokumenten.
- Definieren der Standardeinstellungen für die Suche.
- Erstellen von 'empfohlenen Dokumenten', die in den Suchergebnissen angezeigt werden. Verwenden einer dynamischen FAQ-Liste, um den Anwendern die empfohlenen Dokumente in der Liste ganz oben anzuzeigen.

Hinweis: Für ein Dokument können andere Berechtigungen vorhanden sein als für die damit verknüpften Anlagen.

Weitere Informationen:

[KT-Such-Engine](#) (siehe Seite 1054)

[Empfohlene Dokumente](#) (siehe Seite 1066)

[Einrichten von Standard-Sucheinstellungen](#) (siehe Seite 1070)

[Optionen zur Integration von CA SDM](#) (siehe Seite 1071)

KT-Such-Engine

Nachdem Sie CA SDM installiert haben, wird die KT-Such-Engine als Standard konfiguriert. Suchvorgänge in der Knowledge Base sind auf Knowledge-Dokumente begrenzt. Die Such-Engine befindet sich hier: Registerkarte "Administration", Knowledge, Suche, KT-Such-Engine-Knoten.

Über den KT-Such-Engine-Knoten können Sie folgende Optionen verwalten:

- Füllwörter
- Sonderbegriffe
- Synonyme

Weitere Informationen:

[Verwenden der Knowledge Management-Suche](#) (siehe Seite 1054)

Verwenden der Knowledge Management-Suche

Nachdem Sie CA SDM installiert haben, wird die Knowledge Management-Suchmaschine als die Standardsuch-Engine konfiguriert. Suchvorgänge in der Knowledge Base sind auf Knowledge-Dokumente begrenzt.

Sie können Zugänglichkeit und Vorgaben aller Knowledge-Quellen basierend auf Anwenderrollen festlegen. Standardmäßig sind Knowledge-Dokumente für alle Anwenderrollen zugänglich.

Gehen Sie wie folgt vor:

1. Klicken Sie auf die Registerkarte "Administration".
Die Admin-Konsole wird angezeigt.
2. Klicken Sie auf "Optionsmanager" > "Such-Engine".
Die Optionsliste wird angezeigt.
3. Klicken Sie auf "ebr_version".
Die Seite "Optionen – Detail" wird angezeigt.
Klicken Sie auf "Bearbeiten". Die Seite "Optionen aktualisieren" wird angezeigt.
4. Klicken Sie auf "KT-Such-Engine".
5. Klicken Sie auf "Speichern" und dann auf "Aktualisieren".
Die Seite "Optionen – Detail" wird gemäß Ihrer Auswahl aktualisiert.
6. Klicken Sie auf "Fenster schließen".
7. Starten Sie die CA SDM-Dienste neu.

Weitere Informationen:

[Füllwörter, Synonyme und Sonderbegriffe](#) (siehe Seite 1055)

[Erstellen von Füllwörtern](#) (siehe Seite 1056)

[Bearbeiten von Füllwörtern](#) (siehe Seite 1057)

[Anzeigen von Füllwörtern](#) (siehe Seite 1057)

[Erstellen von Sonderbegriffen](#) (siehe Seite 1058)

[Bearbeiten von Sonderbegriffen](#) (siehe Seite 1058)

[Anzeigen von Sonderbegriffen](#) (siehe Seite 1059)

[Erstellen von Synonymen](#) (siehe Seite 1060)

[Anzeigen von Synonymen](#) (siehe Seite 1060)

[Bearbeiten von Synonymen](#) (siehe Seite 1061)

[Einstellungen für Suchsyntax](#) (siehe Seite 1062)

Füllwörter, Synonyme und Sonderbegriffe

Sie können Wörter (Synonyme, Füllwörter, und besondere Termini) festlegen, die sich auf Freitext- und Schlüsselwortsuchen in CA SDM auswirken. Das Hinzufügen oder Entfernen der folgenden Begriffe hat eine drastische Auswirkung auf die Suchergebnisse, die dem Anwender zurückgegeben werden:

Füllwörter

Diese Wörter sind in der Regel nicht am Suchprozess beteiligt und können daher ignoriert werden. Zum Beispiel werden Präpositionen, wie zum Beispiel an, am, von, zu und bei, häufig als Füllwörter identifiziert. Verwenden Sie die Seite "Füllwörter – Liste", um die Wörter anzugeben, die ohne Auswirkung auf die Suchergebnisse in Dokumenten und Abfragen ignoriert werden können.

Sonderbegriffe

Spezifiziert einen Begriff, den Sie während des Suchvorgangs als ein Wort behandeln möchten, auch wenn es aus mehreren Wörtern besteht oder Sonderzeichen enthält. Hierzu zählen zum Beispiel Wörter, die ein nicht-alphanumerisches Zeichen enthalten, wie der Schrägstrich (/) in TCP/IP, der Bindestrich (-) in Wahlverbindungen oder der Unterstrich in LOCAL_SERVER. Bei Ihren Überlegungen, welche Wörter Sie als Sonderbegriffe definieren möchten, berücksichtigen Sie gültige Wörter, die während des Suchprozesses geteilt werden können, weil sie ein nicht-alphanumerisches Zeichen enthalten.

Synonyme

Spezifiziert ein Wort, das die gleiche Bedeutung wie ein anderes Wort hat. Sie können Synonyme hinzufügen, damit, wenn ein Anwender nach einem bestimmten Wort sucht, und wenn ein entsprechendes Synonym für dieses Wort in Ihrer Wissensbasis existiert, die Suche entsprechend ausgedehnt wird. Sie können mehrere Synonyme für das gleiche Wort definieren. Das System erstellt anhand der erstellten Schlüsselwörter automatisch Umkehrungen für bestehende Synonymbeziehungen. Wenn Sie beispielsweise Computer als ein Synonym für das Wort PC festlegen, ist PC automatisch auch ein Synonym für Computer. Verwenden Sie die Seite "Synonyme - Liste", um Schlüsselwort-/Synonympaare anzugeben, die bei der Analyse von Dokumenten und Abfragen als austauschbar angesehen werden. Durch diese Schlüsselwort-/Synonympaare können die Suchergebnisse verbessert werden.

Hinweis: Nachdem Sie Füllwörter, Sonderbegriffe, Synonyme oder Einstellungen für die Suchsyntax erstellt, geändert oder gelöscht haben, indizieren Sie die Knowledge Base mit dem mitgelieferten Dienstprogramm zur Knowledge-Neuindizierung.

Erstellen von Füllwörtern

Verwenden Sie das Fenster "Neues Füllwort erstellen", um ein neues Wort zur Liste der Wörter hinzuzufügen, welche das Produkt in Dokumenten und Abfragen ignorieren kann, ohne die Suchergebnisse zu beeinflussen.

So erstellen Sie ein Füllwort:

1. Wählen Sie auf der Registerkarte "Administration" die folgenden Optionen aus: "Knowledge" > "Suche" > "KT-Such-Engine" > "Füllwörter".

Die Seite "Füllwörter - Liste" wird angezeigt.

2. Klicken Sie auf "Neu erstellen".
3. Die Seite "Neues Füllwort erstellen" wird angezeigt.
4. Geben Sie in das Feld "Füllwort" das Wort ein, das Sie als Füllwort definieren möchten.

Hinweis: Sie können kein Füllwort definieren, das bereits als Synonym oder Schlüsselwort vorhanden ist.

5. Klicken Sie auf "Speichern".

Das neue Füllwort erscheint auf der Seite "Füllwörter - Liste". Sie können auf die Schaltfläche "Bearbeiten" klicken, um das neue Füllwort zu aktualisieren.

Hinweis: Nachdem Sie Füllwörter, Sonderbegriffe, Synonyme oder Einstellungen für die Suchsyntax erstellt, geändert oder gelöscht haben, indizieren Sie die Knowledge Base mit dem mitgelieferten Dienstprogramm zur Knowledge-Neuindizierung.

Bearbeiten von Füllwörtern

Sie können ein Füllwort bearbeiten, das bereits auf der Seite "Füllwörter - Liste" erstellt wurde.

Hinweis: Nachdem Sie Füllwörter, Sonderbegriffe, Synonyme oder Einstellungen für die Suchsyntax erstellt, geändert oder gelöscht haben, indizieren Sie die Knowledge Base mit dem mitgelieferten Dienstprogramm zur Knowledge-Neuindizierung.

So erstellen Sie ein Füllwort:

1. Klicken mit der rechten Maustaste auf das gewünschte Füllwort in der "Füllwörter - Liste" und wählen Sie im Kontextmenü "Eigenschaften" aus.

Die Seite "Füllwörter bearbeiten" wird angezeigt.

2. Geben Sie Ihre Änderungen in das Feld "Füllwort" ein.

Hinweis: Sie können kein Füllwort definieren, das bereits als Synonym oder Schlüsselwort vorhanden ist.

3. Klicken Sie auf "Speichern".

Das neue Füllwort erscheint auf der Seite "Füllwörter - Liste".

Hinweis: Nachdem Sie Füllwörter, Sonderbegriffe, Synonyme oder Einstellungen für die Suchsyntax definiert, geändert oder gelöscht haben, indizieren Sie die Knowledge Base mit dem mitgelieferten Dienstprogramm zur Knowledge-Neuindizierung.

Anzeigen von Füllwörtern

Sie können die Zusammenfassung für jedes Füllwort auf der Seite "Füllwörter - Liste" anzeigen.

Um eine Zusammenfassung für jedes Füllwort anzuzeigen, wählen Sie auf der Registerkarte "Administration" die folgenden Optionen aus: "Knowledge" > "Suche" > "KT-Such-Engine" > "Füllwörter".

Die Seite "Füllwörter - Liste" wird mit den folgenden Feldern angezeigt:

Füllwort

Definiert ein Füllwort, nach dem gesucht werden soll. Dieses Feld wird nur angezeigt, wenn Sie auf "Filter anzeigen" klicken.

Weitere Suchargumente

Definiert zusätzliche Kriterien für die Suche. Dieses Feld wird nur angezeigt, wenn Sie auf der Seite "Knowledge - Suche" auf die Verknüpfung "Weitere" klicken.

Füllwörter – Liste

Zeigt die Wörter an, die aus Suchanforderungen herausgefiltert werden sollen. Die Liste wird angezeigt, wenn Sie auf die Schaltfläche "Suche" klicken. Wenn Sie im Feld "Füllwort" ein Wort eingegeben haben, wird in der Liste nur das angegebene Wort angezeigt. Wenn Sie im Feld "Füllwort" keine Eingaben vorgenommen haben, werden alle systemdefinierten Füllwörter angezeigt.

Auf der Seite "Füllwörter - Liste" können Sie die folgenden Aufgaben ausführen:

- [Erstellen von Füllwörtern](#) (siehe Seite 1056)
- [Bearbeiten von Füllwörtern](#) (siehe Seite 1057)

Erstellen von Sonderbegriffen

Verwenden Sie die Seite "Neuen Sonderbegriff erstellen", um ein Wort oder eine Wortfolge festzulegen, die das Produkt als einzelne Schlüsselwörter betrachtet, wenn Dokumente und Abfragen analysiert werden.

Erstellen von Sonderbegriffen

1. Navigieren Sie auf der Registerkarte "Administration" zu "Knowledge" > "Suche" > "KT-Such-Engine" > "Sonderbegriffe".

Die Seite "Sonderbegriffe - Liste" wird angezeigt.

2. Klicken Sie auf "Neu erstellen".

Die Seite "Neuen Sonderbegriff erstellen" wird angezeigt.

3. Geben Sie in das Feld "Sonderbegriff" das Wort oder die Wortgruppe ein, das bzw. die Sie als Sonderbegriff definieren möchten.

4. Klicken Sie auf "Speichern".

Das Fenster "Sonderbegriff erstellen" wird geschlossen und die Seite "Sonderbegriff - Detail" geöffnet, so dass Sie das Wort oder die Wortfolge überprüfen können, das bzw. die Sie hinzugefügt haben. Sie können die Schaltfläche verwenden, um den neuen Begriff zu bearbeiten. Der neue Sonderbegriff erscheint auf der Seite "Sonderbegriffe - Liste".

Bearbeiten von Sonderbegriffen

Sie können einen Sonderbegriff bearbeiten.

Erstellen von Sonderbegriffen

1. Klicken Sie mit der rechten Maustaste auf den Begriff in der Liste, den Sie bearbeiten wollen und wählen Sie dann im Kontextmenü "Bearbeiten".

Die Seite "Sonderbegriff aktualisieren" wird angezeigt.

2. Geben Sie in das Feld "Sonderbegriff" das Wort oder die Wortgruppe ein, das bzw. die Sie als Sonderbegriff definieren möchten.
3. Klicken Sie auf "Speichern".

Das Fenster "Sonderbegriff aktualisieren" wird geschlossen und die Seite "Sonderbegriff - Detail" geöffnet, so dass Sie das Wort oder die Wortfolge überprüfen können, das bzw. die Sie hinzugefügt haben. Der aktualisierte Begriff erscheint auf der Seite "Sonderbegriffe - Liste".

Anzeigen von Sonderbegriffen

Sie können für jeden Sonderbegriff eine Zusammenfassung anzeigen.

Um Sonderbegriffe anzuzeigen, wählen Sie auf der Registerkarte "Administration" die folgenden Optionen aus: "Knowledge" > "Suche" > "KT-Such-Engine" > "Sonderbegriffe".

Die Seite "Sonderbegriffe - Liste" erscheint, und Sie können die folgenden Felder verwenden, um die vordefinierten Standardbegriffe zu ändern oder um Ihre eigenen Begriffe definieren:

Sonderbegriff

Definiert einen Sonderbegriff, nach dem gesucht werden soll. Dieses Feld wird nur angezeigt, wenn Sie auf "Filter anzeigen" klicken.

Weitere Suchargumente

Definiert zusätzliche Kriterien für die Suche. Dieses Feld wird nur angezeigt, wenn Sie im Feld "Knowledge – Suche" auf die Verknüpfung "Weitere" klicken.

Sonderbegriffe

Zeigt Wörter oder Wortfolgen an, die Leerstellen oder andere Zeichen (z. B. Bindestriche, Schrägstriche usw.) enthalten, die bei Abfrageanalysen als einzelne Schlüsselwörter angesehen werden sollen. Wenn Sie vor dem Klicken auf "Suche" im Feld "Sonderbegriff" ein Wort eingegeben haben, wird in der Liste nur das angegebene Wort angezeigt. Wenn Sie im Feld "Sonderbegriff" keine Eingaben vorgenommen haben, werden alle systemdefinierten Sonderbegriffe angezeigt.

Auf der Seite "Sonderbegriffe - Liste" können Sie die folgenden Aufgaben ausführen:

- [Erstellen von Sonderbegriffen](#) (siehe Seite 1058)
- [Bearbeiten von Sonderbegriffen](#) (siehe Seite 1058)

Erstellen von Synonymen

Synonyme sind Wörter oder Wortfolgen, die dieselbe oder annähernd dieselbe Bedeutung wie das Schlüsselwort haben, mit dem sie verknüpft sind.

Wenn Sie ein neues komplexes Synonym definieren (d. h. ein Synonym, das mehrere durch Leerzeichen oder andere Trennzeichen getrennte Wörter enthält) sollte hierfür auch ein identischer Sonderbegriff erstellt werden, damit das Synonym als eine Entität verarbeitet werden kann. Wenn Sie z. B. "Computer Associates" als Synonym für "CA" definieren, sollten Sie "Computer Associates" auch als Sonderbegriff definieren.

Hinweis: Es können keine Synonyme oder Schlüsselwörter definiert werden, die bereits als Füllwörter vorhanden sind.

So erstellen Sie ein Synonym:

1. Navigieren Sie auf der Registerkarte "Administration" zu "Knowledge" > "Suche" > "KT-Such-Engine" > "Synonyme".

Die Seite "Synonyme - Liste" wird angezeigt.

2. Klicken Sie auf "Neu erstellen".

Die Seite "Neue Synonyme erstellen" wird angezeigt.

3. Geben Sie in das Feld "Synonyme" das Wort oder die Wortfolge ein, das bzw. die Sie als Sonderbegriff definieren möchten.

4. Klicken Sie auf "Speichern".

Das Fenster zur Synonymerstellung wird geschlossen und die Seite "Synonym - Detail" geöffnet, so dass Sie das Wort oder die Wortfolge überprüfen können, das bzw. die Sie hinzugefügt haben. Das neue Synonym erscheint auf der Seite "Synonyme - Liste".

Anzeigen von Synonymen

Sie können für jedes Synonym eine Zusammenfassung anzeigen.

Um Synonyme anzusehen, wählen Sie auf der Registerkarte "Administration" die folgenden Optionen aus: "Knowledge" > "Suche" > "KT-Such-Engine" > "Synonyme".

Die Seite "Synonyme - Liste" wird angezeigt, und Sie können die standardmäßigen Schlüsselwörter anzeigen oder Ihre eigenen Schlüsselwörter definieren. Verwenden Sie dazu die folgenden Felder:

Schlüsselwort

Definiert ein Schlüsselwort, nach dem gesucht werden soll. Dieses Feld wird nur angezeigt, wenn Sie auf "Filter anzeigen" klicken.

Synonym

Definiert ein Synonym, nach dem gesucht werden soll. Dieses Feld wird nur angezeigt, wenn Sie auf "Filter anzeigen" klicken.

Weitere Suchargumente

Definiert zusätzliche Kriterien für die Suche. Dieses Feld wird nur angezeigt, wenn Sie im Feld "Knowledge – Suche" auf die Verknüpfung "Weitere" klicken.

Synonyme – Liste

Zeigt die Schlüsselwort-/Synonympaare an, die in der Anwendung definiert wurden. Für jedes in der Spalte "Schlüsselwort" enthaltene Schlüsselwort wird in der Spalte "Synonym" eines oder mehrere Synonyme angezeigt.

Auf der Seite "Synonyme - Liste" können Sie die folgenden Aufgaben ausführen:

- [Erstellen von Synonymen](#) (siehe Seite 1060)
- [Bearbeiten von Synonymen](#) (siehe Seite 1061)

Bearbeiten von Synonymen

Sie können ein Synonym bearbeiten.

So bearbeiten Sie ein Synonym:

1. Klicken Sie mit der rechten Maustaste auf den Begriff in der Liste, den Sie bearbeiten wollen und wählen Sie dann im Kontextmenü "Bearbeiten".
Die Seite "Synonym aktualisieren" wird angezeigt.
2. Geben Sie in das Feld "Synonym" das Wort oder die Wortgruppe ein, das bzw. die Sie als Sonderbegriff definieren möchten.
3. Klicken Sie auf "Speichern".

Das Fenster "Sonderbegriff erstellen" wird geschlossen und die Seite "Sonderbegriff - Detail" geöffnet, so dass Sie das Wort oder die Wortfolge überprüfen können, das bzw. die Sie hinzugefügt haben. Der neue Begriff erscheint auf der Seite "Synonyme - Liste".

Einstellungen für Suchsyntax

Bei der Veröffentlichung eines Dokuments in der Wissensdatenbank analysiert die Software die Informationen in den Feldern Titel, Zusammenfassung, Problem und Lösung vom Dokument und zerlegt diese Informationen in Schlüsselwörter. Durchsucht ein Anwender die Knowledge Base, vergleicht die Software die Schlüsselwörter aus der Abfrage des Anwenders mit den Schlüsselwörtern, die durch die Knowledge Base analysiert wurden, und generiert dann eine Ergebnisliste. Verwenden Sie die Seite "Einstellungen für Suchsyntax", um die Einstellungen für die Analyse der Dokumente in der Knowledge Base zu definieren.

Hinweis: Die Funktion "Einstellungen für Suchsyntax" ist nur mit der STANDARD-KT-Suchmaschine verfügbar.

Definieren von Einstellungen für Suchsyntax

Bei der Veröffentlichung eines Dokuments in der Wissensdatenbank analysiert die Software die Informationen in den Feldern Titel, Zusammenfassung, Problem und Lösung vom Dokument und zerlegt diese Informationen in Schlüsselwörter. Durchsucht ein Anwender die Knowledge Base, vergleicht die Software die Schlüsselwörter aus der Abfrage des Anwenders mit den Schlüsselwörtern, die durch die Knowledge Base analysiert wurden, und generiert dann eine Ergebnisliste.

Um die Einstellungen für die Suche von Dokumenten in der Knowledge Base zu definieren, navigieren Sie auf der Registerkarte "Administration" zu "Knowledge" > "Suche" > "Suchsyntax".

Die "Einstellungen für Suchsyntax" erscheinen, und Sie können die Einstellungen über die folgenden Felder näher bestimmen:

Maximale Anzahl von Schlüsselwörtern für die Suche

Definiert die maximale Anzahl der Schlüsselwörter, die bei der Suchtextanalyse extrahiert werden sollen.

Standard: 20

Hinweis: Es sind Werte von 1 bis 100 möglich, und der CA SDM-Knowledge-Administrator kann den Wert innerhalb dieses Bereichs auf Grundlage der Suchanfragen und Parameter einer bestimmten Knowledge-Datenbank ändern. Verwenden Sie eine geringere Anzahl von Schlüsselwörtern, um die Suche zu beschleunigen.

Sprache

Gibt den Sprachtyp an, der zur Verarbeitung der Analyse verwendet werden soll. Markieren Sie eine der folgenden Einstellungen:

Englisch

Führt während einer Suche bestimmte Verarbeitungstypen durch, die spezifisch für die englische Sprache sind (z. B. Verwendung der Suchbegriffe im Singular statt Plural).

Andere europäische Sprache

Verwendet während einer Suche nur Verarbeitungstypen, die für europäische Sprachen gelten.

Koreanisch

Verwendet während einer Suche nur Verarbeitungstypen, die für Koreanisch gelten.

Andere asiatische Sprache

Verwendet während einer Suche nur Verarbeitungstypen, die für andere asiatische Sprachen gelten.

Hinweis: Wenn Sie mit einem chinesischen, japanischen oder koreanischen Betriebssystem arbeiten, vergewissern Sie sich vor der Installation Ihres Knowledge Management-Systems, dass Sie die bestehenden Ansätze und Einschränkungen für die Suchsyntax von [Sprachen mit Multibyte Zeichensatz \(MBCS, Multi-Byte Character Set\)](#) (siehe Seite 1065) verstehen, damit Sie die Erwartungen der Anwender entsprechend steuern können.

Gültiger Zeichenbereich

Definiert den Bereich der alphanumerischen Zeichen, die bei der Analyse der Dokumentfelder "Titel", "Zusammenfassung", "Problem" und "Lösung" als gültig angesehen werden sollen. Alle anderen Zeichen werden vom System als Trennzeichen angesehen.

Hinweis: Wenn für "Sonderbegriffe erkennen" der Wert "Ja" festgelegt wurde, werden die als Sonderbegriffe definierten Wörter oder Wortfolgen von der Analyse ausgeschlossen.

Standard: "a-z". Gibt an, dass alphabetische Zeichen von a bis z bei der Analyse als gültige Zeichen angesehen werden.

Das Feld "Gültiger Zeichenbereich" enthält die entsprechenden Zeichen für die Suchsyntax. Die Buchstaben, die nicht im gültigen Zeichenbereich liegen, werden entfernt.

Für verschiedene Sprachen werden die folgenden Werte empfohlen:

Sprache	Gültiger Zeichenbereich
Deutsch	a-zäöüß
Spanisch	a-záéíóúüñ
Französisch	a-zàââçêëëëïîôùû
Brasilianisches Portugiesisch	a-zàáãäçêéíóúü
Italienisch	a-zàèéìîïù
Vereinfachtes Chinesisch	a-z
Japanisch	a-z
Traditionelles Chinesisch	a-z
Koreanisch	a-z

Hinweis: Japanisch enthält den Bereich "a-z" sowie eine Liste gültiger Katakana-Zeichen (ohne Satzzeichen).

Ähnliche Wörter entfernen

Gibt an, ob strukturell ähnliche Schlüsselwörter aus den für die Suche verwendeten Gruppen entfernt werden sollen. Sie können zwischen den folgenden Einstellungen wählen:

Ja

Entfernt strukturell ähnliche Schlüsselwörter aus den Suchkriterien.

Hinweis: Bei Auswahl von "Ja" werden ähnliche Wörter auch beim Speichern oder Veröffentlichen des Dokuments entfernt. Dies kann Auswirkungen darauf haben, ob ein Dokument durchsucht werden kann, wenn für "Ähnliche Wörter entfernen" der Wert "Ja" festgelegt wurde. Möglicherweise wurde das ähnliche Wort nicht indiziert und kann in späteren Such- und Abfragevorgängen für das Dokument nicht verwendet werden.

No

Behält strukturell ähnliche Schlüsselwörter in den Suchkriterien bei.

Standardwert: Nein

Füllwörter entfernen

Gibt an, ob Füllwörter bei der Analyse der Dokumentfelder "Titel", "Zusammenfassung", "Problem" und "Lösung" entfernt werden sollen. Sie können zwischen den folgenden Einstellungen wählen:

Ja

Entfernt Füllwörter aus den Suchkriterien.

No

Behält Füllwörter in den Suchkriterien bei.

Standard: Ja

Sonderbegriffe erkennen

Gibt an, ob Sonderbegriffe bei der Analyse der Dokumentfelder "Titel", "Zusammenfassung", "Problem" und "Lösung" als eine Einheit oder als mehrere Wörter angesehen werden sollen. Sie können zwischen den folgenden Einstellungen wählen:

Ja

Verarbeitet Sonderbegriffe in den Suchkriterien als eine Einheit.

No

Verarbeitet die einzelnen Wörter in den Suchkriterien, aus denen sich die Sonderbegriffe zusammensetzen, als separate Einheiten.

Standard: Ja

Suchbeschränkungen für Multibyte-Zeichensätze (MBCS, Multi-Byte Character Set)

Bevor Sie Ihr Knowledge Management-System implementieren, vergewissern Sie sich, dass Sie die bestehenden Ansätze und Einschränkungen für die Suchsyntax von MBCS-Sprachen verstehen, damit Sie die Erwartungen der Benutzer entsprechend steuern können. Diese Einschränkung des Produkts beeinträchtigt die Suchfunktionen für japanischen, chinesischen bzw. koreanischen Text innerhalb des Systems. Sie können die vom Suchmechanismus verwendete Suchsyntax auf der Seite "[Einstellungen für Suchsyntax](#) (siehe Seite 1062)" einstellen.

Bei Englisch, anderen europäischen Sprachen sowie bei Koreanisch geht das Produkt davon aus, dass Satzzeichen, Leerzeichen oder beides zwei Wörter voneinander trennen. Der Dokumenttext wird so in einzelne Wörter zerlegt, was die Grundlage dafür schafft, dass Füllwörter ignoriert und bekannte Synonyme bzw. Sonderbegriffe angewendet werden können, um Begriffe zu suchen.

Wenn jedoch die asiatischen Spracheinstellungen ausgewählt sind, greift die Routine für die Suchsyntax auf einen zeichenbasierten Ansatz zurück, da einige asiatische Sprachen einzelne Wörter nicht durch Leerzeichen voneinander trennen. Diese Einstellung signalisiert der Suchsyntax, dass jedes Zeichen als ein ganzes Wort betrachtet werden soll. Diese Einstellung gilt für jeden zu suchenden Text. Da die Spracheinstellungen den Modus der Suchsyntax beeinflussen, muss der gesamte Suchindex wiederhergestellt werden, wenn die Spracheinstellung in oder aus einer asiatischen Sprache geändert wird.

Empfohlene Dokumente

Hinweis: CA SDM-Anwender können Kriterien zum Suchbegriff eingeben. Die Suchmaschine sucht die passenden Knowledge-Dokumente und zeigt diese auf der Seite der Suchergebnisse als einen Satz von Verknüpfungen unter dem Titel "Empfohlene Dokumente" an. Die Suchanfrage kann als ein Schlüsselwort oder Satz von Wörtern (Wortfolge) ausgedrückt werden, der den Suchbegriff identifiziert, den ein oder mehr Dokumente enthalten können.

Die Liste von Dokumenten, die den Suchkriterien entsprechen, wird geordnet und (nach Priorität) eingestuft, damit in den Suchergebnissen die wichtigsten Dokumente ganz oben angezeigt werden. Mit Hilfe der empfohlenen Dokumente können die Anwender rascher zu den gewünschten Informationen gelangen.

Um einen Satz zutreffender Dokumente bereitzustellen, die entsprechend den angegebenen Kriterien schnell sortiert werden, sammelt die Suchmaschine Daten aufgrund des Bedingungstyps (Wortfolge, Schlüsselwörter oder Kategorie), den der Administrator auf der Seite für das Erstellen empfohlener Dokumente konfiguriert.

Weitere Informationen:

[Erstellen von empfohlenen Dokumenten](#) (siehe Seite 1066)

[Bearbeiten von Bedingungen für empfohlene Dokumente](#) (siehe Seite 1068)

[Anzeigen von empfohlenen Dokumenten](#) (siehe Seite 1068)

[Suchen empfohlener Dokumente](#) (siehe Seite 1069)

Erstellen von empfohlenen Dokumenten

Administratoren können empfohlene Dokumente erstellen, die Anwender finden können, wenn sie Kriterien für relevante Elemente spezifizieren.

Hinweis: Wenn die Mandantenfähigkeit installiert ist, wählen Sie in der Dropdown-Liste den entsprechenden Mandanten aus. Mit der Option "öffentlich (freigegeben)" wird das Objekt für alle Mandanten erstellt.

Erstellen eines Dokuments

1. Wählen Sie auf der Registerkarte "Administration" die Option "Knowledge" > "Suchen" > "Empfohlene Dokumente".

Das Fenster "Empfohlene Dokumente – Liste" wird angezeigt.

2. Klicken Sie auf "Neu erstellen".

Die Seite "Erstellen neuer empfohlener Dokumente" wird angezeigt.

3. Füllen Sie die nachstehenden Felder nach Bedarf aus.

Knowledge-Dokument

Spezifiziert ein Knowledge-Dokument, oder klicken Sie auf das Suchsymbol, um die Seite "Knowledge-Dokument suchen".

Bedienungstyp:

Spezifiziert einen [Bedingungstyp](#) (siehe Seite 1067) nach dem die Such-Engine die Dokumente sortiert und passende Ergebnisse findet.

- Wenn der Bedingungstyp "Genaue Übereinstimmung", "Genaue Wortfolge" oder "Schlüsselwörter" ist, wird ein Textfeld angezeigt. Sie können einen Satz oder ein Schlüsselwort eingeben, der/das ein Konzept identifiziert, das im Dokument enthalten sein soll.
- Wenn der Bedingungstyp "Knowledge-Kategorie" ist, wird die Knowledge-Kategorie-Verknüpfung angezeigt. Sie können eine Knowledge-Kategorie spezifizieren, die mit diesem Dokument assoziiert sein soll.

Status

Definiert den Status dieses Datensatzes als aktiv oder inaktiv.

Klicken Sie auf "Speichern".

Das neue empfohlene Dokument wird in der Knowledge Base gespeichert und auf der Seite "Liste empfohlener Dokumente" aufgeführt.

Feld "Bedingungstyp"

Die Such-Engine lokalisiert Dokumente mit den folgenden Bedingungstypen:

Genaue Übereinstimmung

Sucht nach Dokumenten gemäß der Zeichenfolge, die als Suchtext eingegeben wurde. Es wird nur dann ein Treffer angezeigt, wenn die Such-Engine genau die gleichen Wörter in einer Zeichenfolge findet.

Genaue Wortfolge

Sucht nach Dokumenten gemäß der exakten Zeichenfolge, die als Suchtext eingegeben wurde. Es wird nur dann ein Treffer angezeigt, wenn die Such-Engine genau die gleichen Zeichen oder Wörter in derselben Reihenfolge in einer Zeichenfolge findet.

Schlüsselwörter

Sucht nach Dokumenten gemäß der Stichwörter, die als Suchtext eingegeben wurden. Es wird nur dann ein Treffer angezeigt, wenn die Such-Engine alle Stichwörter findet.

Knowledge-Kategorie

Sucht nach Dokumenten gemäß Knowledge-Kategorie. Es wird nur dann ein Treffer angezeigt, wenn ein Anwender zu einer Kategorie navigiert, die für empfohlene Dokumente konfiguriert ist.

Bearbeiten von Bedingungen für empfohlene Dokumente

Sie können eine Bedingung für empfohlene Dokumente aktualisieren.

So bearbeiten Sie Bedingungen für empfohlene Dokumente

1. Wählen Sie auf der Registerkarte "Administration" die Option "Knowledge" > "Suchen" > "Empfohlene Dokumente".
Die Seite "Liste empfohlener Dokumente" wird angezeigt.
2. Um eine Bedingung zu bearbeiten, klicken mit der rechten Maustaste auf den Titel in der Spalte "Bedingung".
Die Seite "Empfohlenes Dokument aktualisieren" wird angezeigt.
3. Füllen Sie die Felder nach Bedarf aus.
4. Klicken Sie auf "Speichern".
Die aktualisierte Bedingung wird in der Liste "Empfohlene Dokumente" angezeigt.

Anzeigen von empfohlenen Dokumenten

Sie können zusammenfassende Informationen für jedes empfohlene Dokument ansehen.

Um empfohlene Dokumente anzusehen, wählen Sie "Suche" und dann auf der Registerkarte "Administration" die Option "Empfohlene Dokumente".

Die Seite "Liste empfohlener Dokumente" wird angezeigt; die folgenden Spalten werden aufgeführt:

Bedingung

Zeigt eine Bedingung, nach der die Such-Engines die Dokumente sortiert und passende Ergebnisse findet.

Knowledge-Dokument

Zeigt die Dokumente in der Ergebnisliste.

Author

Gibt den Autor des Knowledge-Dokuments an.

Änderungsdatum

Gibt das Datum der letzten Dokumentänderung an.

Auf der Seite "Liste empfohlener Dokumente" können Sie die folgenden Aufgaben ausführen:

- [Erstellen eines Knowledge-Dokuments](#) (siehe Seite 1066)
- [Bearbeiten von Bedingungen für empfohlene Dokumente](#) (siehe Seite 1068)
- [Suchen empfohlener Dokumente](#) (siehe Seite 1069)

Suchen empfohlener Dokumente

Mit der Suchfunktion können Sie die Liste der empfohlenen Dokumente filtern, so dass nur die gewünschten Elemente angezeigt werden.

Hinweis: Wenn die Mandantenfähigkeit installiert ist, zeigt die Listenseite die Einstellungen für Mandant und öffentliche Daten im Suchfilter an. Öffentliche Daten können in Mandantendaten eingeschlossen oder aus diesen ausgeschlossen werden. Es werden ausschließlich öffentliche Objekte gesucht. Wählen Sie auf Detailseiten den geeigneten Mandanten in der Liste aus. Wenn Sie <leer> wählen, ist das Objekt öffentlich.

So suchen Sie ein empfohlenes Dokument:

1. Wählen Sie auf der Registerkarte "Administration" die Option "Knowledge" > "Suchen" > "Empfohlene Dokumente" aus.
Das Fenster "Empfohlene Dokumente – Liste" wird angezeigt.
2. Klicken Sie auf "Filter anzeigen".
3. Füllen Sie die Felder nach Bedarf aus. Die nachstehenden Felder bedürfen einer näheren Erklärung.

Typ

Spezifiziert einen Bedingungstyp, mit dem das Dokument übereinstimmt und der als empfohlene Dokumentverknüpfung angezeigt wird.

Phrase/Keywords

Spezifiziert Informationen zu Suchanfragen, nach denen das gewünschte im Dokument enthaltene Konzept identifiziert wird.

Klicken Sie auf "Suche".

Die Seite "Empfohlene Dokumente – Liste" zeigt alle Elemente, die mit Ihren Suchkriterien übereinstimmen.

Einrichten von Standard-Sucheinstellungen

Sie können Suchoptionen einrichten, die als Standardoptionen verwendet werden sollen. Diese werden angezeigt, wenn Anwender über das Suchfeld nach Knowledge suchen.

Hinweis: Diese Suchoptionen werden von persönlichen Sucheinstellungen überschrieben, die von Anwendern im Fenster "Voreinstellungen" eingegeben werden, oder von zusätzlichen Suchoptionen im Fenster "Knowledge durchsuchen", oder im Fenster "Knowledge-Kategorien".

So richten Sie Standard-Sucheinstellungen ein:

1. Wählen Sie auf der Registerkarte "Administration" die Option "Knowledge" > "Suchen" > "Sucheinstellungen" aus.

Die Seite "Suchoptionen" wird angezeigt.

2. Wählen Sie nach Bedarf die folgenden Optionen aus:

Empfohlene Ergebnisse

Festlegen der Anzahl von Dokumenten, die in der Liste mit Suchergebnissen angezeigt werden.

Standardsuchfelder

Gibt an, welche Dokumentfelder standardmäßig in Schlüsselwortsuchen berücksichtigt werden sollen. Aktivieren Sie ein Kontrollkästchen, um das damit verknüpfte Feld bei Standardsuchen zu berücksichtigen. Deaktivieren Sie ein Kontrollkästchen, um das damit verknüpfte Feld bei Standardsuchen auszuschließen. Die folgenden Dokumentfelder sind für die Suche verfügbar:

- Titel
- Übersicht
- Problem
- Lösung
- Anhänge

Sucheinstellungen für alle Quellen

Spezifiziert ob Suchen alle Wissensquellen einschließen können. Beispiel: Knowledge-Kategorien und Request-Bereiche.

Sucheinstellungen für einen Ticket-Kontext

Gibt an, ob die Suchläufe alle Felder umfassen können, die in einem Service Desk-Ticket definiert werden (Incident, Problem, Issue, Change, Request).

- Wählen Sie für diese Optionen *einen* der folgenden Übereinstimmungstypen:
 - **Irgendeines der Wörter (ODER)**Fügt dem Ergebnissatz ein Dokument hinzu, wenn es eines oder mehrere der Wörter enthält, die im Feld "Suche" eingegeben wurden. Diese Option ist die Standardauswahl.
 - **Alle Wörter (UND)**Fügt dem Ergebnissatz nur ein Dokument hinzu, wenn es alle Wörter enthält, die im Feld "Suche" eingegeben wurden.

Klicken Sie auf "Speichern".

Die Standard-Sucheinstellungen sind jetzt definiert.

Optionen zur Integration von CA SDM

Die folgenden Konfigurationsoptionen sind für die CA SDM-Integration verfügbar:

Feldzuordnung

Gibt an, welche CA SDM-Felder mit Knowledge Management-Informationen aufgefüllt werden und ob vorhandene Informationen überschrieben werden sollen.

Issue – Suchkonfiguration

Wählt die Felder aus, in denen gesucht werden soll, wenn Sie auf die Schaltfläche 'Knowledge durchsuchen' auf einem Ticket klicken.

Definieren der Issue-Suchkonfiguration

Wählt die Felder aus, in denen gesucht werden soll, wenn Sie auf die Schaltfläche "Suchen" auf einem Ticket klicken.

Request/Incident/Problem – Suchkonfiguration

Wählt die Felder aus, in denen gesucht werden soll, wenn Sie auf die Schaltfläche "Suchen" auf einem Ticket klicken.

Knowledge vorschlagen

Wählt die Felder aus, in denen gesucht werden soll, wenn Sie auf die Schaltfläche 'Knowledge-Dokumente vor dem Speichern anzeigen' auf einem Ticket klicken.

Weitere Informationen:

[Definieren von Feldzuordnungen](#) (siehe Seite 1072)

[Definieren der Issue-Suchkonfiguration](#) (siehe Seite 1074)

[Definieren der Suchkonfiguration für Requests/Incidents/Probleme](#) (siehe Seite 1075)

[Knowledge-Vorschläge](#) (siehe Seite 1076)

[Definieren von Issue-Kategorien](#) (siehe Seite 1077)

[Definieren von Request-/Incident-/Problembereichen](#) (siehe Seite 1078)

[Konfigurieren von Self-Service-Richtlinien](#) (siehe Seite 1079)

Definieren von Feldzuordnungen

Administratoren geben auf der Seite "Feldzuordnung" an, welche Felder mit Informationen von Knowledge Management auszufüllen sind und ob vorhandene Informationen überschrieben werden sollen.

So definieren Sie Felder in Service Desk für Knowledge Management:

1. Wählen Sie auf der Registerkarte "Administration" die Option "Knowledge" > "Service Desk-Integration" > "Feldzuordnung" aus.

Die Seite "Feldzuordnung" wird angezeigt.

2. Füllen Sie die folgenden Felder nach Wunsch aus:

Ausfüllen mit Service Desk-Werten von Knowledge Management

Legt fest, ob Informationen aus Knowledge Management zum Ausfüllen von Feldern bei Service Desk-Issues oder -Requests zu verwenden sind.

- Aktivieren Sie das Kontrollkästchen, um Felder in den Spalten "Knowledge Management", "Service Desk-Werte über Knowledge Tools ausfüllen" und "Service Desk-Werte überschreiben" zugänglich zu machen, so dass Sie festlegen können, welche Informationen von Knowledge Management zum Ausfüllen von Feldern bei Service Desk-Issues oder -Requests zu verwenden sind.
- Deaktivieren Sie das Kontrollkästchen, um die Felder "Knowledge Management", "Leere Service Desk-Felder ausfüllen" und "Service Desk-Werte überschreiben" nicht zugänglich zu machen. In diesem Fall müssen die Anwender die von Knowledge Management erstellten Service Desk-Issues oder -Requests manuell ausfüllen.

Standard: Dieses Kontrollkästchen ist aktiviert.

Service Desk

Bezeichnet die Felder in Issues oder Requests, die den in der Spalte "Knowledge Management" aufgeführten Feldern entsprechen.

Bei jedem Kontrollkästchen, das in der Spalte "Leere Service Desk-Werte auffüllen" aktiviert ist, werden der Issue oder Request mit den Informationen aus dem entsprechenden Feld in der Spalte von "Knowledge Management" aufgefüllt.

Knowledge Management

Gibt die Knowledge Management-Felder an, die den in der Spalte "Service Desk" aufgeführten Service Desk-Feldern entsprechen.

Bei jedem Kontrollkästchen, das in der Spalte "Leere Service Desk-Werte auffüllen" aktiviert ist, werden der Issue oder Request mit den Informationen aus dem entsprechenden Feld in der Spalte von "Knowledge Management" aufgefüllt.

Die Spalte "Knowledge Management" enthält zwei Dropdown-Listen:

- Die erste Dropdownliste entspricht dem Feld "Zusammenfassung" in der Spalte "Service Desk" und legt das Knowledge Management-Feld fest (Titel, Zusammenfassung oder Problem), mit dem das Feld "Zusammenfassung" in einem Issue oder Request ausgefüllt werden soll.

Standard: Zusammenfassung

- Die zweite Dropdownliste entspricht dem Feld "Beschreibung" in der Spalte "Service Desk" und legt das Knowledge Management-Feld fest (Titel, Zusammenfassung oder Problem), mit dem das Feld "Beschreibung" in einem Issue oder Request ausgefüllt werden soll.
- **Standard:** Problem.

Leere Service Desk-Felder ausfüllen

Legt fest, welche leeren Felder in einem Service Desk-Issue oder -Request mit Informationen aus Knowledge Management ausgefüllt werden sollen.

- Aktivieren Sie ein Kontrollkästchen, um Informationen aus dem Knowledge Management-Feld dem entsprechenden Service Desk-Feld zuzuordnen, wenn dieses Feld gegenwärtig keine Informationen enthält.
- Deaktivieren Sie ein Kontrollkästchen, wenn Sie dem entsprechenden Service Desk-Feld keine Informationen aus dem Knowledge Management-Feld zuordnen möchten.

Standard: Die Kontrollkästchen, die den

Feldern "Zusammenfassung", "Beschreibung", "Produkt", "Asset" und "Request-Bereich" in Service Desk entsprechen, sind aktiviert.

Service Desk-Werte überschreiben

Legt fest, welche Felder in einem Service Desk-Issue oder -Request mit Informationen aus Knowledge Management überschrieben werden sollen.

- Aktivieren Sie ein Kontrollkästchen, um Informationen im Service Desk-Feld durch Informationen aus dem entsprechenden Knowledge Management-Feld zu ersetzen.
- Deaktivieren Sie ein Kontrollkästchen, wenn Sie die Informationen im Service Desk-Feld nicht durch Informationen aus dem Knowledge Management-Feld ersetzen möchten.

Diese Kontrollkästchen sind nur zugänglich, wenn die entsprechenden Kontrollkästchen in der Spalte "Leere Service Desk-Werte ausfüllen" markiert sind.

Standard: Alle Kontrollkästchen "Leere Service Desk-Werte überschreiben" sind deaktiviert.

Klicken Sie auf "Speichern".

Feldzuordnung wird definiert.

Definieren der Issue-Suchkonfiguration

Sie können die Felder innerhalb eines Issue definieren, die durchsucht werden sollen, wenn Sie auf einem Ticket auf die Schaltfläche "Knowledge durchsuchen" klicken. Die markierten Felder werden in die entsprechenden Felder im Suchfilter auf der Registerkarte "Knowledge" im Fenster "Issue – Detail" kopiert. Die Suchenfilterfelder werden aus dem Ticket ausgefüllt, wenn Sie die Registerkarte "Knowledge" markieren oder die Schaltfläche "Filter zurücksetzen" auf der Registerkarte "Knowledge" klicken.

So definieren Sie die Felder eines Issues, die für Knowledge Base-Suchläufe verwendet werden sollen:

1. Wählen Sie auf der Registerkarte "Administration" die Option "Knowledge" > "CA SDM-Integration" > "Issue – Suchkonfiguration" aus.

Die Seite "Integration von CA SDM" wird angezeigt.

2. Wählen Sie die Felder aus, die für Suchvorgänge in der Knowledge Base verfügbar sein sollen.

- Übersicht
- Beschreibung
- Configuration Item
- Priorität
- Kategorie
- Ursache
- Produkt

Hinweis: Die beiden Felder "Zusammenfassung" und "Beschreibung" können nicht gleichzeitig ausgewählt werden.

3. Wählen Sie die Option "Suche automatisch ausführen, wenn die Knowledge-Registerkarte eines Issue ausgewählt ist" aus, wenn die Knowledge Base automatisch durchsucht werden soll, sobald auf der Detailseite die Registerkarte "Knowledge" ausgewählt ist.
4. Klicken Sie auf "Speichern".
Issue-Suche wird konfiguriert.

Definieren der Suchkonfiguration für Requests/Incidents/Probleme

Sie können die Felder in Requests, Incidents oder Problemen definieren, die durchsucht werden sollen, wenn Sie auf einem Ticket auf die Schaltfläche "Knowledge durchsuchen" klicken. Die markierten Felder werden auf der Detailseite "Ticket" auf der Registerkarte "Knowledge" in die entsprechenden Felder des Suchfilters kopiert. Die Suchenfilterfelder werden aus dem Ticket ausgefüllt, wenn Sie die Registerkarte "Knowledge" markieren oder die Schaltfläche "Filter zurücksetzen" auf der Registerkarte "Knowledge" klicken.

So definieren Sie die Felder in einem Requests, Incident oder Problem, die für Knowledge Base-Suchläufe verwendet werden sollen:

1. Wählen Sie auf der Registerkarte "Administration" die Option "Knowledge" > "CA SDM-Integration" > "Request/Incident/Problem – Suchkonfiguration" aus.

Die Seite "Integration von CA SDM" wird angezeigt.

2. Wählen Sie die Felder aus, die für Suchvorgänge in der Knowledge Base verfügbar sein sollen.

- Übersicht
- Beschreibung
- Configuration Item
- Relevanz
- Impact
- Urgency
- Priorität
- Request-Bereich
- Ursache

Hinweis: Die beiden Felder "Zusammenfassung" und "Beschreibung" können nicht gleichzeitig ausgewählt werden.

3. Wählen Sie die Option "Suche automatisch ausführen, wenn die Knowledge-Registerkarte eines Issue ausgewählt ist" aus, wenn die Knowledge Base automatisch durchsucht werden soll, sobald auf der Detailseite die Registerkarte "Knowledge" ausgewählt ist.
4. Klicken Sie auf "Speichern".

Die Felder in einem Requests, Incident oder Problem, die für Knowledge Base-Suchläufe verwendet werden sollen, werden definiert.

Knowledge-Vorschläge

Mitarbeiter und Kunden können (mit entsprechender Berechtigung) eine Liste der Knowledge-Vorschläge abrufen, wenn sie ein neues Ticket in der Self-Service-Schnittstelle erstellen.

Wenn eine Lösung gefunden und das Ticket nicht gespeichert wird, können die vorgeschlagenen Dokumente durch ein Self-Service-Bewertungssystem im Dokumentformular verrechnet werden. Dieses Bewertungssystem hängt von den auf der Seite 'Sucheinstellungen' definierten Self-Service-Richtlinien ab.

Die abgerufenen Daten können für Berichte, Dashboards und bei der Suche in der Knowledge Base verwendet werden, in der die Anwender die Dokumente filtern können, die zu einer erfolgreichen Lösung ihrer Tickets geführt haben.

Self-Service hat den Vorteil, dass weniger Unterstützungsanrufe eingehen und weniger Tickets erstellt werden, was niedrigeren Betriebskosten gleichkommt.

Der Administrator muss diese Funktion aktivieren, bevor die entsprechenden Issue-Kategorien und Request-Bereiche genutzt und konfiguriert werden, für die Knowledge in der Self-Service-Schnittstelle vorgeschlagen wird.

Definieren von Issue-Kategorien

Sie können Issue-Kategorien definieren, für die den Kunden und Mitarbeitern Knowledge bei der Ticketerstellung vorgeschlagen wird.

Sie können die Funktion "Knowledge vorschlagen" aktivieren oder deaktivieren. Wenn Sie diese Funktion deaktivieren, ist sie für Kunden und Mitarbeiter nicht mehr verfügbar, verbleibt jedoch für die spätere Verwendung in der Datenbank. Wenn Sie diese Funktion zu einem späteren Zeitpunkt wieder nutzen möchten, können Sie sie erneut aktivieren.

So definieren Sie Issue-Kategorien für das Vorschlagen von Knowledge:

1. Wählen Sie auf der Registerkarte "Administration" die Option "Knowledge" > "Service Desk-Integration" > "Knowledge vorschlagen" > "Issue-Kategorien" aus.
Die Seite "Knowledge für Issue-Kategorien vorschlagen" wird angezeigt.
2. Wählen Sie die Option **Knowledge nicht vorschlagen**, um die Funktion "Knowledge vorschlagen" als aktiv zu markieren.

Standard: Inaktiv

Wenn Sie diese Funktion als aktiv markieren, werden die folgenden Optionen angezeigt:

Standardeinstellung für Knowledge:

Vorgeschlagen

Wählen Sie diese Option, wenn Knowledge für alle Issue-Kategorien vorgeschlagen werden *soll* (außer für die Kategorien, die in der Liste der Issue-Kategorien definiert sind).

Nicht vorgeschlagen

Wählen Sie diese Option, wenn *keine* Knowledge-Elemente für Issue-Kategorien vorgeschlagen werden sollen (außer für die Kategorien, die in der Liste der Issue-Kategorien definiert sind).

Dies gilt für alle Issue-Kategorien außer:

Zeigt die Liste der Request-Bereiche an, für die den Mitarbeitern und Kunden auf der Self-Service-Benutzeroberfläche Knowledge entweder vorgeschlagen oder nicht vorgeschlagen wird. Der Self-Service-Anwender darf die Request-Bereiche nicht bearbeiten, denn sie sind schreibgeschützt.

3. Klicken Sie auf *eine* der folgenden Schaltflächen:

Hinzufügen

Fügt der Liste den markierten Request-Bereich hinzu.

Entfernen

Entfernt den markierten Request-Bereich aus der Liste.

Alle entfernen

Entfernt alle Request-Bereiche aus der Liste.

Speichern

Speichert die Informationen zu den Request-Bereichen in der Knowledge Base.

Issue-Kategorien werden definiert.

Definieren von Request-/Incident-/Problembereichen

Sie können Request-, Incident- und Problembereiche definieren, für die den Kunden und Mitarbeitern Knowledge bei der Ticketerstellung vorgeschlagen wird.

Sie können die Funktion "Knowledge vorschlagen" aktivieren oder deaktivieren. Wenn Sie diese Funktion deaktivieren, ist sie für Kunden und Mitarbeiter nicht mehr verfügbar, verbleibt jedoch für die spätere Verwendung in der Datenbank. Wenn Sie diese Funktion zu einem späteren Zeitpunkt wieder nutzen möchten, können Sie sie erneut aktivieren.

So definieren Sie Request-/Incident-/Problembereiche:

1. Navigieren Sie auf der Registerkarte "Administration" zu "Knowledge" > "CA SDM-Integration" > "Knowledge vorschlagen" > "Request-/Incident-/Problembereiche".

Die Seite "Knowledge für Request-/Incident-/Problembereiche vorschlagen" wird angezeigt.

2. Wählen Sie die Option **Knowledge nicht vorschlagen**, um die Funktion "Knowledge vorschlagen" als aktiv zu markieren.

Standard: Inaktiv

Wenn Sie diese Funktion aktivieren, werden einige zusätzliche Optionen angezeigt:

Standardeinstellung für Knowledge:**Vorgeschlagen**

Wählen Sie diese Option aus, wenn Knowledge für alle Request-/Incident-/Problembereiche vorgeschlagen werden soll (außer für die Bereiche, die in der Liste der Request-Bereiche definiert sind).

Nicht vorgeschlagen

Wählen Sie diese Option aus, wenn *keine* Knowledge-Elemente für Request-/Incident-/Problembereiche vorgeschlagen werden sollen (außer für die Bereiche, die in der Liste der Request-Bereiche definiert sind).

Für alle Request-/Incident-/Problembereiche außer den folgenden:

Zeigt die Liste der Request-Bereiche an, für die den Mitarbeitern und Kunden auf der Self-Service-Benutzeroberfläche Knowledge entweder vorgeschlagen oder nicht vorgeschlagen wird. Der Self-Service-Anwender darf die Request-Bereiche nicht bearbeiten, denn sie sind schreibgeschützt.

Klicken Sie auf "Speichern".

Die Request-/Incident-/Problembereiche, für die Knowledge vorgeschlagen wird, werden definiert.

Konfigurieren von Self-Service-Richtlinien

Sie können Self-Service-Richtlinien konfigurieren, die sich auf Dokumente basierend auf einer Reihe von Anwenderszenarien auswirken.

So konfigurieren Sie Self-Service-Richtlinien:

1. Navigieren Sie auf der Registerkarte "Administration" zu "Knowledge" > "CA SDM-Integration" > "Knowledge vorschlagen" > "Self-Service-Konfiguration".

Die Seite "Sucheinstellungen" wird angezeigt.

2. Geben Sie die geeigneten Richtlinieneinstellungen für Dokumente an, und speichern Sie die vermiedenen Tickets basierend auf den folgenden Anwenderszenarien:
 - Anwender hat kein vorgeschlagenes Dokument geöffnet.
 - Anwender hat ein vorgeschlagenes Dokument geöffnet.
 - Anwender hat ein vorgeschlagenes Dokument als Lösung für sein Problem akzeptiert.
 - Anwender hat nach Knowledge-Inhalt gesucht, ein Dokument geöffnet und den Vorgang beendet.

Klicken Sie auf "Speichern".

Die Einstellungen der Self-Service-Richtlinien werden gespeichert.

Lösungsumfrage

Lösungsumfragen ermöglichen das Sammeln und Analysieren des Kundenfeedbacks zur Knowledge-Dokument-Leistung. Sie können die Umfrageeinstellungen durch Auswählen von 'Knowledge', 'Lösungsumfrage' auf der Admin-Oberfläche ändern. Die Umfrage bezieht sich auf ein veröffentlichtes Knowledge-Dokument und ermöglicht Kunden, Gästen und Angestellten die Bewertung des Knowledge-Dokuments.

Diese Funktion enthält die folgenden Komponenten:

- FAQ-Einstellungen
- Umfrageeinstellungen

Weitere Informationen:

[Festlegen der FAQ-Einstellungen](#) (siehe Seite 1080)

[Festlegen der Einstellungen für Lösungsumfragen](#) (siehe Seite 1082)

Festlegen der FAQ-Einstellungen

Verwenden Sie das Fenster "FAQ-Einstellungen", um Parameter festzulegen, mit deren Hilfe die Software die FAQ-Bewertung für jedes Dokument berechnet. Die Software ermittelt die FAQ-Einstufung anhand der folgenden Kriterien:

- Wie oft wurde in der Vergangenheit auf das Dokument zugegriffen
- Wie hilfreich war das Dokument den Anwendern
- Wie sehr hat die Nützlichkeit des Dokuments im Laufe der Zeit abgenommen

Standardmäßig werden im Fenster mit der Dokumentenliste die Dokumente nach der FAQ-Bewertung sortiert angezeigt (d. h., in der Reihenfolge der Nützlichkeit). Die nützlichsten Dokumente stehen in der Dokumentliste ganz oben. Im Laufe der Zeit wandern die Dokumente in der Dokumentliste abwärts, da die Anwender die Lösungen für die Probleme immer besser beherrschen.

So legen Sie die FAQ-Einstellungen fest:

1. Wählen Sie auf der Registerkarte "Administration" die Option "Knowledge" > "Lösungsumfrage" > "FAQ-Einstellungen".

Die Seite "FAQ-Einstellungen" wird angezeigt.

2. Füllen Sie die folgenden Felder nach Wunsch aus:

Letzte Aktualisierung:

Legt fest, ob der FAQ-Einstufungsdienst gestartet werden soll, und zeigt das Datum an, an dem die FAQ-Einstufungen zuletzt aktualisiert wurden.

- Markieren Sie das Kontrollkästchen "FAQ-Einstufungsdienst", um die FAQ-Kalkulation mit den Einstellungen dieses Fensters zu starten.
- Deaktivieren Sie das Kontrollkästchen "FAQ-Einstufungsdienst", um die FAQ-Kalkulation abzuschalten.

Ablauf

Legt die Häufigkeit fest, mit der die Software die FAQ-Einstufungen aktualisiert. Dieses Feld enthält die folgenden Komponenten:

Intervall für die Durchführung der FAQ-Kalkulation

Legt die Zeit fest, die bis zur nächsten Aktualisierung der FAQ-Einstufung für die Dokumente durch Software vergeht.

Standard: 1 Tag

Von:

Legt die Tageszeit fest, zu der die Software mit der Neuberechnung der FAQ-Einstufungen beginnt.

Standard: 00:00 (12:00 A.M.)

Bis

Legt die Tageszeit fest, zu der die Software die Neuberechnung der FAQ-Einstufungen beenden soll, unabhängig davon, ob die Berechnung fertig gestellt ist.

Standard: 07:00 (7:00 A.M.)

Hinweis: Diese Einstellung wird am Tag nach der Installation der Software wirksam. Wenn Sie die z. B. 19. April 2008 installiert haben, startet der FAQ-Server am 20. April 2008 zum ersten Mal.

Alterung:

Definiert, wie häufig die FAQ-Bewertung eines Dokuments neu berechnet wird, bevor der Wert 0 erreicht ist. Basierend auf diesem Wert sinkt die FAQ-Bewertung und erreicht schließlich den Wert 0. Daraufhin wird sie am unteren Ende der Liste der Dokumente angezeigt (wenn die Liste nach FAQ-Bewertung sortiert wird).

Standard: 180

Bei einem Alterungswert von beispielsweise 180 für ein Dokument mit einer Bewertung von 4 ("Sehr hilfreich") nimmt die FAQ-Bewertung den Wert 0 (null) an, wenn die Software die FAQ-Bewertung 180 Mal neu berechnet hat.

Hinweis: Standardmäßig erfordert die Berechnung der FAQ-Reihenfolge bu_trans-Daten für die letzten 180 Tage, wobei 180 der Alterungsfaktor ist. Wenn Sie den FAQ-Alterungsfaktor auf mehr als 365 Tage einstellen, müssen Sie die Archivregeln für die bu_trans-Tabelle ebenfalls dementsprechend erweitern.

Tagesangabe für neue Dokumente:

Legt die Anzahl von Tagen fest, die ein neu erstelltes oder importiertes Dokument im Ordner "Neue Dokumente" der Registerkarte "Knowledge" angezeigt wird.

Standard: 5 Tage

Einstufung

Legt die Standardeinstufung (überhaupt nicht hilfreich, etwas hilfreich oder sehr hilfreich) für Dokumente fest, die von Anwendern geöffnet, aber nicht eingestuft wurden.

Standard: Hilfreich

Klicken Sie auf "Speichern".

Die FAQ-Einstellungen werden festgelegt.

Festlegen der Einstellungen für Lösungsumfragen

Benutzen Sie die Seite "Umfrageeinstellungen", um zu konfigurieren, wie ein Knowledge-Dokument angezeigt werden soll, wenn man darauf zur Lösung eines Problems oder zur Beantwortung einer Frage zugreift.

So legen Sie die Einstellungen für Lösungsumfragen fest:

1. Wählen Sie auf der Registerkarte "Administration" die Option "Knowledge" > "Lösungsumfrage" > "Umfrageeinstellungen".

Die Seite "Umfrageeinstellungen" wird angezeigt.

2. Füllen Sie die nachstehenden Felder nach Bedarf aus. Klicken Sie auf "Speichern".

Die Einstellungen der Lösungsumfrage werden festgelegt.

Knowledge Management-Systemeinstellungen

Sie können die Standardinformationen so einstellen, dass auf der Registerkarte "Knowledge" (bei der Anmeldung) das Format, das die Kategorien im Fenster "Knowledge-Kategorien" auf der Registerkarte "Verwaltung" anzeigen, und die Anzahl der Dokumente angezeigt werden, die auf der Knowledge Management-Startseite in der Liste "Beste Lösungen" aufgeführt werden.

Weitere Informationen:

[Konfigurieren von allgemeinen Einstellungen](#) (siehe Seite 1083)

Konfigurieren von allgemeinen Einstellungen

Sie können festlegen, wie die Standardinformationen auf der Registerkarte "Knowledge" bei der Anmeldung angezeigt werden sollen, in welchem Format die Kategorien im Fenster "Knowledge-Kategorien" auf der Registerkarte "Administration" angezeigt werden sollen, und welche Anzahl an Dokumenten auf der Knowledge Management-Startseite in der Liste "Beste Lösungen" angezeigt werden sollen.

Gehen Sie wie folgt vor:

1. Wählen Sie Knowledge, System, Allgemeine Einstellungen auf der Registerkarte Administration aus.

Die Seite Allgemeine Einstellungen wird geöffnet.

2. Füllen Sie die folgenden Felder nach Wunsch aus:

Eröffnungsbildschirm für das Suchwerkzeug:

Gibt die Informationen an, die standardmäßig auf der Registerkarte Knowledge angezeigt werden. Sie können zwischen den folgenden Optionen wählen:

- Öffnen mit FAQ / Suche – Zeigt die Fenster Kategorie, Knowledge-Suche und Knowledge-Dokumente - Liste an.
- Öffnen mit Dokument-ID in der Knowledge-Struktur – Zeigt die Knowledge-Baumstruktur mit der Dokument-ID an, die im bereitgestellten Feld angegeben ist. Sie können zum Knowledge-Baumstrukturdokument selbst zurückkehren sowie dann zu den Fenstern Kategorie, Knowledge – Suche und Knowledge-Dokument – Liste. **Standard:** Öffnen mit FAQ/Suche

Kategorieansicht:

Legt das Format fest, in dem die Dokumentenkategorien im Fenster Knowledge-Kategorien der Registerkarte Administration angezeigt werden. Sie können zwischen den folgenden Optionen wählen:

- Kategorien als Struktur anzeigen – Zeigt im Fenster Knowledge-Kategorien Kategorien in einer hierarchischen Baumstruktur an. Sie können die Kategorien erweitern um zugehörige Unterkategorien anzuzeigen. Auf diese Weise können Sie alle Kategorien in der Baumstruktur gleichzeitig ansehen.
- Kategorien als Liste anzeigen – Zeigt im Fenster Knowledge-Kategorien Kategorien im Listenformat an. Wenn Sie eine Kategorie markieren, werden ihre Unterkategorien in einer Liste angezeigt. Sie können gleichzeitig nur die aktuelle Ebene von Kategorien oder Unterkategorien anzeigen. Verwenden Sie die Verknüpfung Eine Ebene nach oben, um auf die vorherige Kategorienebene zurückzukehren.

Hinweis: Bei mehr als 250 Kategorien unter der obersten Kategorie oder unter einer anderen Kategorie sollten Sie die Option Kategorien als Liste anzeigen und nicht die Strukturansicht verwenden.

Beste Lösungen

Gibt die Anzahl der Dokumente an, die in der Liste Beste Lösungen auf der CA SDM-Startseite aufgeführt werden.

Standard: 10

Pfad für EBR-Indexdateien

Definiert den Speicherort für das Speichern der EBR-Indexdateien. CA SDM erstellt EBR-Indexdateien, wenn Sie ein beliebiges Knowledge-Dokument speichern und veröffentlichen. Beachten Sie abhängig von Ihrem Konfigurationstyp die folgenden Punkte, wenn Sie den EBR-Indexdateipfad definieren:

- Konventionell: Wenn Sie ein Upgrade von CA SDM Version 12.9 von r11.2 oder r12.X durchführen, können Sie auswählen, den freigegebenen UNC-Pfad nicht zu verwenden. Wenn Sie keinen UNC-Pfad erstellt haben, verwendet CA SDM den standardmäßigen Pfad, um EBR-Indexdateien zu speichern. Wenn Sie ein freigegebenes UNC-Laufwerk verwenden, dann kopieren Sie den Ordner "ebr/ebr_ADM" manuell vom standardmäßigen Speicherort (\$NX_ROOT/site/) in den freigegebenen UNC-Pfad.
- Erweiterte Verfügbarkeit: Wenn Sie ein Upgrade auf eine Konfiguration für erweiterte Verfügbarkeit von CA SDM r11.2 oder r12.X durchführen, dann müssen Sie den freigegebenen UNC-Pfad erstellen und diesen verwenden, um EBR-Indexdateien zu speichern. Die UNC-Daten sind für den Standardpfad nicht erforderlich. Nachdem Sie ein UNC-Laufwerk erstellt haben, kopieren Sie den Ordner "ebr/ebr_ADM" manuell vom standardmäßigen Speicherort (\$NX_ROOT/site/) in den freigegebenen UNC-Pfad.

Wichtig! Der Pfad der EBR-Indexdateien und der KEIT-Dateien müssen sich auf die gleichen UNC-Daten beziehen, und der Pfad muss sich auf dem gleichen Server befinden, um dies zu unterstützen.

Standard: \$NX_ROOT/site/ebr

Pfad für Knowledge-Import-/Exportdateien

Definiert den Speicherort, in dem KEIT-Import-/Exportpakete während eines Import-/Exportvorgangs gespeichert werden. Beachten Sie abhängig von Ihrem Konfigurationstyp die folgenden Punkte, wenn Sie den KEIT-Dateipfad definieren:

- Konventionell: Wenn Sie ein Upgrade auf CA SDM Version 12.9 von r11.2 oder r12.X durchführen, können Sie auswählen, den freigegebenen UNC-Pfad nicht zu verwenden. Wenn Sie keinen UNC-Pfad erstellt haben, verwendet CA SDM den standardmäßigen Pfad, um die KEIT-Dateien zu speichern. Wenn Sie ein freigegebenes UNC-Laufwerk verwenden, dann kopieren Sie die Paketordner "Import/Export" manuell vom standardmäßigen Speicherort (\$NX_ROOT/site/keit) in den freigegebenen UNC-Pfad.
- Erweiterte Verfügbarkeit: Wenn Sie ein Upgrade auf eine Konfiguration für erweiterte Verfügbarkeit von CA SDM r11.2 oder r12.X durchführen, dann müssen Sie den freigegebenen UNC-Pfad erstellen und diesen verwenden, um KEIT-Dateien zu speichern. Die UNC-Daten sind für den Standardpfad nicht erforderlich. Nachdem Sie ein UNC-Laufwerk erstellt haben, kopieren Sie die Paketordner "Import/Export" manuell vom standardmäßigen Speicherort (\$NX_ROOT/site/keit) in den freigegebenen UNC-Pfad.

Wichtig! Der Pfad der EBR-Indexdateien und der KEIT-Dateien müssen sich auf die gleichen UNC-Daten beziehen, und der Pfad muss sich auf dem gleichen Server befinden, um dies zu unterstützen.

Standard: \$NX_ROOT/site/keit

UNC-Daten

Sie können diese Option verwenden, um UNC-Daten für den Zugriff auf das freigegebene Netzlaufwerk zu erstellen, um auf EBR-Indexdateien und Import-/Exportpakete zuzugreifen. Verwenden Sie die Verknüpfung "UNC-Daten", um die UNC-Daten zu erstellen.

Hinweis: UNC-Pfade und UNC-Daten sind bei der Konfiguration für erweiterte Verfügbarkeit erforderlich. Starten Sie den CA SDM-Service neu, wenn Sie die UNC-Details ändern (UNC-Pfade oder UNC-Daten).

Benachrichtigungen beim Indizieren der Dokumente

Legt einen Anwender fest, der E-Mail-Benachrichtigungen über den Status oder das Auftreten von Fehlern beim Indizieren von Dokumenten erhält. Die E-Mail-Adresse des Anwenders muss in der Tabelle "ca_contacts" vorhanden sein, damit er diese E-Mail-Benachrichtigungen empfangen kann. Verwenden Sie zur Festlegung der Benachrichtigungsmethoden die Seite "Benachrichtigung" des Kontaktdatensatzes für den Zuständigen.

Wichtig! Es ist unbedingt erforderlich, dass Sie im Abschnitt Benachrichtigungen beim Indizieren der Dokumente einen Verantwortlichen für den Erhalt von Benachrichtigungen festlegen. Eine gültige E-Mail-Adresse muss auf der Registerkarte Benachrichtigung dieses Kontakts definiert werden, um E-Mail-Benachrichtigungen zu aktivieren.

3. Klicken Sie auf "Speichern".

Die allgemeinen Einstellungen werden konfiguriert.

Hinweis: Wenn Sie eine Migration von einer älteren CA SDM-Version auf eine Konfiguration für erweiterte Verfügbarkeit durchführen, dann kopieren Sie manuell die Import-/Exportpakete in den freigegeben UNC-Speicherort (im Feld "Pfad für Knowledge-Import-/Exportdateien" angegeben). Für EBR-Indexdateien können Sie den Ordner "EBR/ebr_ADM" manuell in den freigegebenen UNC-Speicherort verschieben oder den Befehlspfad "pdm_k_reindex" ausführen.

Kapitel 24: Verwalten von Support-Automatisierung

Dieses Kapitel enthält folgende Themen:

[Automatisieren des Supports in Ihrer Umgebung](#) (siehe Seite 1087)
[Verwalten von Support-Automatisierung-Analysten](#) (siehe Seite 1090)
[Support-Automatisierung-Anwenderverwaltung](#) (siehe Seite 1105)
[Support-Automatisierung-Aktivitätsbenachrichtigungsverwaltung](#) (siehe Seite 1112)
[Support-Automatisierung-Seitenanpassungen](#) (siehe Seite 1113)
[Support-Automatisierung-Systemeigenschaften](#) (siehe Seite 1115)
[Support-Automatisierung-Warteschlangenverwaltung](#) (siehe Seite 1116)
[Verwaltung von Ticket-Vorlagen](#) (siehe Seite 1118)
[Administrationseinstellungen](#) (siehe Seite 1118)
[Anpassen von Support-Automatisierung-Tools](#) (siehe Seite 1121)
[Sitzungsprotokoll-Verwaltung](#) (siehe Seite 1129)
[Support-Automatisierung-Berichte](#) (siehe Seite 1130)
[Tickets mit Live-Unterstützung lösen](#) (siehe Seite 1130)

Automatisieren des Supports in Ihrer Umgebung

Sie können eine Supportstrategie implementieren, indem Sie Prozesse und Tools miteinander kombinieren. CA SDM stellt die Tools bereit, um die Live-Unterstützung zu verwalten, um automatische Tasks zu entwickeln und um diese durch die verschiedenen Support-Kanäle verfügbar zu machen.

Verwenden Sie die entsprechenden Prozesse, um eine Umgebung einzurichten, in der Folgendes möglich ist:

- Reduzieren der durchschnittlichen Dauer von Support-Aufrufen
- Reduzieren der allgemeinen Unterstützungskosten
- Steigern der behobenen Anfragen innerhalb eines Zeitraums
- Steigern der Zufriedenheit von Endbenutzern

Live-Unterstützung

Die Live-Unterstützung bietet Endbenutzern Unterstützung durch Verwendung von Tools, die zur Verbesserung der Remote-Interaktion zwischen Analysten und Endbenutzern beitragen. Sie können automatisierte vordefinierte Antworten verwenden, um mit dem Endbenutzer zu kommunizieren. Sie sammeln detaillierte Information über einen Endbenutzer-Computer und sind anschließend in der Lage, Support zu leisten.

Sie können Support für Endbenutzer in Echtzeit leisten, indem Sie die folgenden Schnittstellen verwenden:

Analystenschnittstelle von Support-Automatisierung

Ermöglicht Analysten, mit Endbenutzern zu interagieren und sie während dieser Sitzungen zu unterstützen.

Endbenutzer-Client

Ermöglicht dem Endbenutzer, mit dem Analysten zu sprechen, während der Computer des Endbenutzers unterstützt wird.

Support-Automatisierung-Konnektivität

Der Analyst und Endbenutzer kommunizieren niemals direkt miteinander. Sie benötigen keine direkte Peer-to-Peer-Konnektivität zwischen den beiden Benutzern. Jeder Datentransfer wird über den Server umgelenkt, und es wird sichergestellt, dass Sie kommunizieren können, auch wenn sich der Computer des Endbenutzers hinter einer einschränkenden Firewall befindet.

Sie können eine Verbindung mit dem Computer des Endbenutzers herstellen, indem Sie die folgenden Verbindungen verwenden:

Socket

Eine Socket-Verbindung ist die beste Verbindungsmöglichkeit. Socket-Verbindungen bieten die schnellste Art von Verbindung, mit dem geringsten Overhead, der niedrigsten Latenz und dem effizientesten Verbindungstyp.

HTTP (oder HTTPS)

Eine HTTP-Verbindung kann bessere Verbindungen bieten als eine direkte Socket-Verbindung, weil eine Firmenfirewall direkte Socket-Verbindungen blockieren kann. HTTP-Verbindungen generieren im Vergleich mit Socket-Verbindungen einen beachtlichen Overhead an Netzwerkverkehr. Aufgrund des HTTP-Overheads und der HTTP-Verarbeitung auf dem Server ist die Anzahl der gleichzeitigen Sitzungen viel niedriger, wenn die meisten Verbindungen mit dem Server über HTTP laufen.

Proxy

Socket-Proxy ist ein Betriebsmodus für den Support-Automatisierung-Server, damit einige der CPU-intensiven Vorgänge entlastet werden. Das betrifft zum Beispiel die Verschlüsselung/Dekodierung vom Hauptserver und das Bereitstellen einer Serverkomponente für die entmilitarisierte Zone (oder eine ähnliche Zone) innerhalb der logischen Netztopologie.

In der Regel wird versucht, über die direkte Socket-Verbindung zu verbinden und dann über HTTP zu verbinden, falls die direkte Socket-Verbindung fehlschlägt. Sie können jedoch benutzerdefinierte Verbindungseinstellungen auf dem Client-Computer angeben, um diese Abfolge zu ändern.

Hinweis: Weitere Informationen über das Konfigurieren von Kommunikationseinstellungen finden Sie in der *Online-Hilfe*.

Endanwender-Client

Der Endanwender-Client verbindet Endanwender mit Analysten in Live-Unterstützungssitzungen. Endanwender kommunizieren mit Analysten über Web-Chat. Wenn Sie jedoch die Tools in der Support-Automatisierung-Analystenschnittstelle verwenden müssen, startet CA SDM den Client auf dem Endanwender-Computer. Wenn der Client startet, werden browserspezifische Anweisungen für den Endanwender angezeigt.

Serverauslastung

In umfangreichen Bereitstellungen kann eine hohe Serverauslastung die Anwendungsleistung verschlechtern. Daher können Sie einen Teil der Verarbeitung folgendermaßen auf einen oder mehr Socket-Proxy-Server verlagern:

- Verlagern Sie die Verschlüsselung und Dekodierung der eingehenden und abgehenden Daten für alle Analysten oder Clients (verbunden entweder durch eine direkte Socket- oder eine HTTP-Verbindung).
- Verlagern Sie die Verarbeitung des HTTP-Verkehrs von und zu Clients, die über HTTP eine Verbindung zum Socket-Proxy herstellen.

Serverkomponente für die entmilitarisierte Zone (Demilitarized Zone, DMZ)

In einigen Netzwerkumgebungen kann es als ein Sicherheitsrisiko betrachtet werden, wenn Sie einen direkten Socketzugriff auf die Anwendungserver ermöglichen, die die Support-Automatisierung-Serveranwendung ausführen. In diesen Umgebungen können Sie Socket-Proxy innerhalb der DMZ verwenden, um einen Vermittler zwischen den Internetanwendern und den Anwendungsservern bereitzustellen. Das Verwenden eines Socket-Proxy in diesem Szenario sorgt für eine Verarbeitungsverlagerung vom Hauptserver.

Wie der Socket-Proxy arbeitet

Der Socket-Proxy arbeitet folgendermaßen:

1. Auf dem konfigurierten, externen Port überprüft der Socket-Proxy, ob Verbindungen mit Analysten oder Endanwendern eingehen.
2. Der Socket-Proxy stellt für jede Verbindung eine Peer-Verbindung mit dem Hauptserver auf dem konfigurierten internen Port her. Diese zwei Verbindungen werden Endanwenderverbindung und Serververbindung genannt.
3. Die Endanwenderverbindungen werden verschlüsselt, und der Socket-Proxy verschlüsselt/entschlüsselt alle Daten, die über die Endanwenderverbindung ein- oder ausgehen.

Hinweis: Die Serververbindungen werden nicht verschlüsselt.

4. Für jedes eingehende Datenpaket wird die Protokollstruktur überprüft und ein Prüfsummenwert bestätigt, bevor die Daten über die Serververbindung zum Hauptserver weitergeleitet werden.
5. Der Hauptserver entfernt den Verschlüsselungs- und Entschlüsselungsvorgang.
6. Der Socket-Proxy schließt die entsprechende Peer-Verbindung, sobald die Endanwender- oder Serververbindung getrennt wurde.

Verwalten von Support-Automatisierung-Analysten

Support-Automatisierung-Analysten überwachen und bewältigen in Live-Unterstützungssitzungen in Ihrer Umgebung mehrere Endanwender-Requests. Analysten verwenden Support-Automatisierung-Werkzeuge, um mit Endanwendern zu interagieren und eine Live-Unterstützung bereitzustellen.

Analysten greifen auf die Schnittstelle von einem CA SDM-Ticket, wie z. B. einem Incident, oder der Support-Automatisierung-Registerkarte zu. Durch das Verwalten von Zugriffsebenen können Sie Berechtigungen für Tools einrichten, die von Analysten verwendet werden können. Sie können Support-Automatisierung-Werkzeuge für bestimmte Mandanten aktivieren und deaktivieren. Wenn ein Tool für einen Mandanten deaktiviert wird, können Analysten dieses Tool in Unterstützungssitzungen nicht verwenden.

Wichtig! Die Support-Automatisierung-Analystenschnittstelle läuft nur auf Windows. Weitere Informationen zu unterstützten Betriebsumgebungen finden Sie in den *Versionshinweisen*.

Weitere Informationen:

[Einführung](#) (siehe Seite 1091)

[So konfigurieren Sie die Live-Unterstützung für Analysten](#) (siehe Seite 1092)

[Starten der Live-Unterstützung durch Analysten](#) (siehe Seite 1101)

[Konfigurieren von Live-Unterstützung für Analysten](#) (siehe Seite 1102)

[Verbinden von Endbenutzern mit Unterstützungssitzungen](#) (siehe Seite 1103)

[Wie Analysten die Unterstützung für Endbenutzer automatisieren](#) (siehe Seite 1104)

[Bereitstellen der Live-Unterstützung durch Analysten](#) (siehe Seite 1105)

Einführung

Produkt: CA SDM

Version: Version 12.9

BS: Windows und Linux

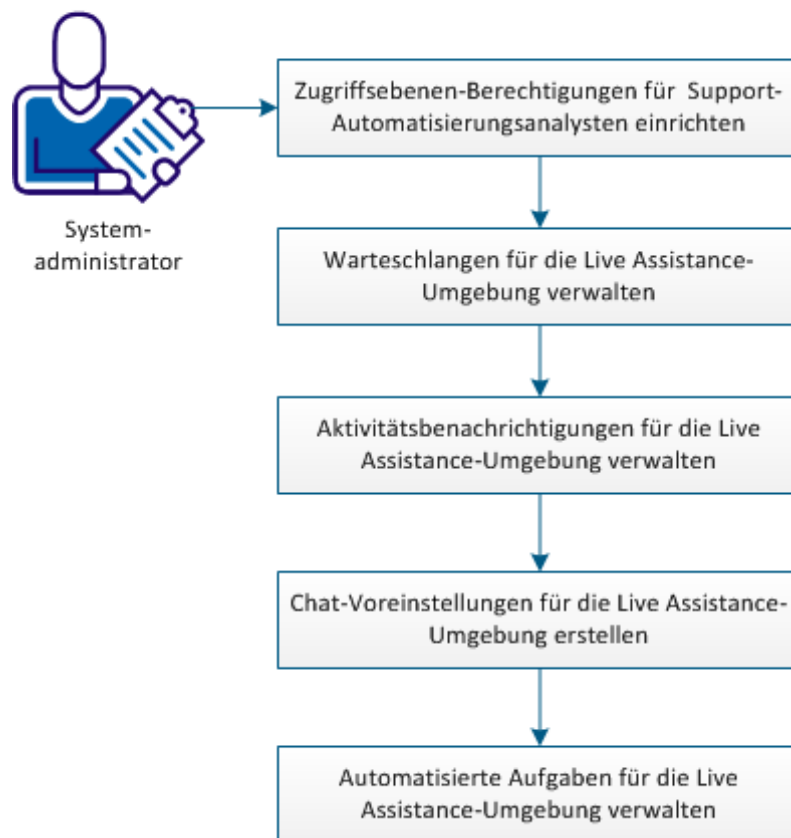
Dieses Szenario beschreibt, wie ein Systemadministrator die Live-Unterstützung für Support-Automatisierung-Analysten einrichtet.

So konfigurieren Sie die Live-Unterstützung für Analysten

Als Systemadministrator können Sie die Live-Unterstützung einrichten und Zugriffsebenen verwalten, um Berechtigungen für Tools festzulegen, die die Analysten verwenden können. Sie können Support-Automatisierung-Werkzeuge für bestimmte Mandanten aktivieren und deaktivieren. Wenn ein Tool für einen Mandanten deaktiviert wird, können Analysten dieses Tool in Unterstützungssitzungen nicht verwenden.

Folgendes Diagramm veranschaulicht, wie die Live-Unterstützung für Analysten eingerichtet wird:

Einrichten von Live Assistance für Analysten



Gehen Sie wie folgt vor:

1. [Festlegen der Berechtigungen auf Zugriffsebenen für Analysten der Support-Automatisierung](#) (siehe Seite 1093)
2. [Verwalten der Warteschlangen für die Umgebung der Live-Unterstützung](#) (siehe Seite 1095)

3. [Verwalten der Aktivitätsbenachrichtigungen für die Umgebung der Live-Unterstützung](#) (siehe Seite 1096)
4. [Erstellen von Chat-Voreinstellungen für die Umgebung der Live-Unterstützung](#) (siehe Seite 1098)
5. [Verwalten der automatisierten Aufgaben für die Umgebung der Live-Unterstützung](#) (siehe Seite 1099)

Festlegen der Berechtigungen auf Zugriffsebenen für Analysten der Support-Automatisierung

Sie können CA SDM-Rollen so konfigurieren, dass Support-Automatisierung möglich ist. Legen Sie Rollenberechtigungen in Ihrer Umgebung für Live-Unterstützung durch Konfigurieren von Support-Automatisierung-Zugriffsebenen für Analysten und Privatsphären-Ebenen für Endanwender fest.

Die folgenden Zugriffsebenen sind verfügbar:

Analyst

Gibt den Kontakttyp an, der in Ihrer Unterstützungsumgebung Live-Unterstützung für Endanwender bereitstellt. Eine Zugriffsebene definiert jeweils, welche Warteschlangen, automatisierten Aufgaben und Tools dem Analysten zur Verfügung stehen.

Endanwender

Gibt den Kontakttyp an, der Live-Unterstützung von Analysten erhält, z. B. "Mitarbeiter" und "Kunde".

Sie können die Support-Automatisierung-Zugriffsebenen auf der Registerkarte "Administration" verwalten.

Gehen Sie wie folgt vor:

1. Legen Sie die gewünschten Zugriffsebenen für Analysten in Ihrer Umgebung für Live-Unterstützung fest. Zum Beispiel "Analyst" oder "Endanwender".

Sie erstellen Zugriffsebenen für Analysten, um die Analystenberechtigungen in Ihrem System zu verwalten, wie beispielsweise Aktivieren und Deaktivieren von spezifischen Support-Automatisierung-Analysten-Schnittstellen-Tools.
2. Überprüfen Sie die Informationen, und wählen Sie die entsprechenden Privatsphären-Ebenen für die Endanwender in Ihrer Live-Unterstützungsumgebung aus.

Sie erstellen Privatsphären-Ebenen, um Endanwender-Zugriffsebenen in Ihrem System zu verwalten.
3. Zuweisen von Zugriffsebenen zu Rollen. Sie weisen Endanwender-Privatsphären-Ebenen und Analysten-Zugriffsebenen für Rollen in Ihrer Umgebung zu.
 - a. Wählen Sie auf der Registerkarte "Administration" > "Sicherheit und Rollenverwaltung" > "Rollenverwaltung" > "Rollenliste".

Die Seite "Rollenliste" wird angezeigt.
 - b. Klicken Sie auf die Rolle, der Sie eine Zugriffsebene zuweisen wollen, wie beispielsweise "Administrator".

Die Seite "Rolle - Detail" wird angezeigt.
 - c. Klicken Sie auf "Bearbeiten".

Die Seite "Rolle aktualisieren" wird angezeigt.
 - d. Wählen Sie auf der Registerkarte "Autorisierung" die von Ihnen erstellte Zugriffsebene aus der Drop-down-Liste "SA-Zugriff" aus, und klicken Sie auf "Speichern".

Die Seite "Rolle - Detail" wird angezeigt. Überprüfen Sie, ob der Support-Automatisierung-Zugang der Rolle zugewiesen ist.

Sie können Support-Automatisierung-Zugriffsebenen verwalten und sie innerhalb Ihrer Unterstützungsumgebung verschiedenen CA SDM-Rollen zuweisen. Unterstützungsumgebungen variieren in Größe und Struktur, d.h. die Implementierung von Zugriffsebenen richtet sich entsprechend danach.

In einer kleinen Unterstützungsumgebung darf es beispielsweise nicht mehr als einen oder zwei Analysten innerhalb einer Zugriffsebene geben. In einer größeren Unterstützungsumgebung kann der Mandantenadministrator mehrere Analysten-Zugriffsebenen einrichten, wobei jede Ebene unterschiedliche Zugriffs- und Unterstützungsprivilegien hat.

Wichtig! Wenn Sie in einer Umgebung für mehrere Mandanten arbeiten, haben Analysten, die nicht dem Service Provider angehören, nur auf ihre eigenen Mandanten und untergeordnete Mandanten Schreibzugriff. Sie können dem Analysten Schreibzugriff auf andere Mandanten und untergeordnete Mandanten geben. Dieser Zugriff ist möglich, indem Sie den Funktionszugriff des jeweiligen Mandanten so aktualisieren, dass auch Mandanten enthalten sein dürfen, die nicht zum Service Provider gehören.

Verwalten der Warteschlangen für die Umgebung der Live-Unterstützung

Sie können Warteschlangen verwenden, um Requests für Unterstützungssitzungen an den am besten geeigneten Analysten weiterzuleiten. Der Endanwender kann eine Kategorie oder eine Beschreibung des Computer-Problems auswählen, und das Ticket (z. B. ein Incident) wird dann in die entsprechende Warteschlange weitergeleitet.

Nach der Installation des Produkts ist der Name der Standardwarteschlange "Support". Sie können Warteschlangen einrichten, um verschiedene Support-Requests zu sortieren und nachzuverfolgen, je nachdem wie Ihre konkreten Geschäftsanforderungen sind. Sie können pro Mandant nur eine Standardwarteschlange zuweisen. Wenn Sie keine Standardwarteschlange zuweisen oder wenn die Standardwarteschlange nicht verfügbar ist, verwendet das System die öffentliche Standardwarteschlange. Sie können die Arbeitsstunden pro Warteschlange festlegen.

Das System platziert die Requests von Endanwendern automatisch, indem es Zuordnungen zwischen Warteschlangen und Incident-Bereichen herstellt. Wenn ein Bereich einer Warteschlange zugeordnet wird, wählt der Endanwender eine Kategorie aus und wird zu der entsprechenden Warteschlange weitergeleitet. Die Suchfunktionen werden auf die Beschreibungen von Incidents oder Issue-Kategorien angewandt, um relevante Warteschlangen zu finden. Der Anwender wird daraufhin an die Warteschlange weitergeleitet, die am besten auf seine Anfrage passt.

Gehen Sie wie folgt vor:

1. Passen Sie Warteschlangen für Analysten und Mandanten in Ihrer Live-Unterstützungsumgebung an. Um die Warteschlange anzupassen, ändern Sie den Standardwert des Felds, und passen Sie den Wert an.

Sie können Warteschlangen aktivieren oder deaktivieren, Chat-Voreinstellungen, Kategorien, Warteschlangen-Stunden, automatische Übertragungen festlegen und Mandanten- und Analystenberechtigungen angeben.

2. Aktivieren Sie ein Kontrollkästchen, um eine Standardwarteschlange zuzuweisen.

Sie können Endanwender an die Standardwarteschlange umleiten, wenn sie Abfragen eingeben, die nicht mit den in Ihrer Umgebung konfigurierten Warteschlangen übereinstimmen. Sie können auch Warteschlangen für Mandanten in Ihrer Umgebung anpassen.

Hinweis: Wenn die standardmäßige Mandantenwarteschlange fehlt oder nicht verfügbar ist, dann wird die öffentliche Warteschlange verwendet.

3. Geben Sie die Betriebsstunden für Ihre Warteschlangen ein.

Sie können Warteschlangen basierend auf der Verfügbarkeit von Anwendern in Ihrer Unterstützungsumgebung verwalten, z. B. indem Sie Support-Automatisierung-Services während der Geschäftszeiten aktivieren.

Wichtig! Sie können Schichten sowohl Support-Automatisierung-Zeiten als auch einzelnen Warteschlangen der Live-Unterstützung zuweisen. Wenn Sie Support-Automatisierung-Zeiten und einzelnen Warteschlangen verschiedene Schichten zuweisen, kann dies für Analysten und Endanwender in Ihrer Support-Umgebung zu Konflikten führen.

Verwalten der Aktivitätsbenachrichtigungen für die Umgebung der Live-Unterstützung

Als Systemadministrator können Sie anpassen, wie Endanwender und Analysten Benachrichtigungen verfolgen und empfangen können, wenn eine Aktivität auftritt. Zum Beispiel kann eine Benachrichtigung gesendet werden, wenn ein Analyst eine Unterstützungssitzung beendet. Sie erstellen E-Mail-Benachrichtigungen, um Analysten zu benachrichtigen, wenn eine Unterstützungssitzungsanfrage in ihre Warteschlange gestellt wurde.

Wählen Sie eine der folgenden Standardbenachrichtigungen (die inaktiv sind) entsprechend Ihrer Umgebung aus:

Benachrichtigung über Warteschlangeneintrag

Benachrichtigt den Analysten, wenn ein Endanwender sich mit einer Warteschlange der Unterstützungssitzung verbindet und wenn die Unterstützungssitzung auf eine andere Warteschlange übertragen wird.

Benachrichtigung des Analysten

Benachrichtigt den Analysten, wenn die Wartezeit der Endanwenderwarteschlange abgelaufen ist. Das Ablaufen der Zeit wird von einem Ereignis-Bedingungsmakro von CA SDM erkannt.

Endanwender zu einer Unterstützungssitzung einladen - Incident

Benachrichtigt den Endanwender, wenn der Analyst ihn zu einer Unterstützungssitzung über einen Issue oder einen Request einlädt.

Endanwender zu einer Unterstützungssitzung einladen - Issue

Benachrichtigt den Endanwender, wenn der Analyst ihn zu einer Unterstützungssitzung über einen Issue einlädt.

Benachrichtigung über Beendigung der Sitzung

Benachrichtigt das System, wenn die Unterstützungssitzung endet.

Wichtig! Wenn Sie die Support-Automatisierung-Funktionen mit einem externen System, wie Star, verwenden wollen, wird der Kontakt "System_SA_User" standardmäßig auf die Regel *Benachrichtigung über Beendigung der Sitzung* eingestellt.

Gehen Sie wie folgt vor:

1. Navigieren Sie zu "Administration", "Benachrichtigung", "Aktivitätsbenachrichtigungen"

Die Seite "Aktivitätsbenachrichtigungen" wird geöffnet.

2. Wählen Sie eine Benachrichtigung aus.

Die Benachrichtigung wird ausgewählt, und Sie können diese Benachrichtigung verwenden.

Erstellen von Chat-Voreinstellungen für die Umgebung der Live-Unterstützung

Sie können häufige Antworten auf häufig gestellte Fragen erstellen. So können sich wiederholende Antworten, die oft getippt werden, gespeichert und in anderen Chat-Sitzungen wieder verwendet werden. Diese gespeicherten Antworten werden Chat-Sitzungen genannt.

Sie können Endanwender am Anfang jeder Sitzung eine automatische Voreinstellung, wie z. B. einen Gruß, senden. Sie können die Voreinstellungen auch automatisch mit Informationen auffüllen, die sich spezifisch auf die aktuelle Sitzung beziehen, wie z. B. den Namen des Analysten.

Sie können in einer Live-Unterstützungssitzung folgende Voreinstellungstypen verwenden:

Chat-Voreinstellung

Identifiziert eine häufig verwendete Textantwort auf eine Endanwenderfrage.

URL-Voreinstellung

Identifiziert eine häufig verwendete URL, auf die der Endanwender zugreifen kann.

Sie können jede Chat-Voreinstellung lokalisieren. Die Chat-Voreinstellung wird mit der Endanwenderlokalisierung synchronisiert, so dass der Endanwender die korrekten lokalisierten Voreinstellungen erhält. Sie können vordefinierte Antworten auf häufig gestellte Fragen und bei oft auftretenden Problemsituationen verwenden.

Gehen Sie wie folgt vor:

1. Machen Sie sich kundig, wie die typischen Unterstützungssitzungen in Ihrer Organisation verlaufen.
2. Wählen Sie im Support-Automatisierung-Menü die Optionen "Extras" > "Chat-Voreinstellungen" > "Textvoreinstellungen – Liste".

Die Seite "Chat-Text-Voreinstellungen – Liste" wird angezeigt.

3. Klicken Sie auf "Neu erstellen".

Die Seite "Neue Chat-Text-Voreinstellung erstellen" wird angezeigt.

4. Füllen Sie die folgenden Felder aus:

Mandant

Gibt den Mandanten an.

Standard-Chat-Voreinstellung für Sitzungsteilnahme

Wählen Sie diese Option, um die Standard-Chat-Voreinstellung für die Sitzungsteilnahme festzulegen.

Textvoreinstellungen – Gruppe

Gibt die Gruppe der Textvoreinstellungen an.

Textvoreinstellungen – Name

Gibt den Namen der Textvoreinstellungen an.

Voreingestellter Text

Gibt den Text der Voreinstellung an.

Klicken Sie auf "Speichern".

Die Text-Chat-Voreinstellung wird erstellt.

5. (Optional) Klicken Sie auf "Bearbeiten", um die Liste der lokalisierten voreingestellten Chat-Texte zu ändern.

Die Seite "Chat-Text-Voreinstellung aktualisieren" wird angezeigt.

6. Klicken Sie auf eine Lokalisierungsverknüpfung.

Die Seite "Chat-Text - Voreinstellungen - Lokalisierungsdetails" wird angezeigt.

7. Klicken Sie auf "Bearbeiten".

Die Seite "Chat-Text-Voreinstellung aktualisieren: Lokalisierung" wird angezeigt.

8. Geben Sie den lokalisierten Namen und Text ein, und klicken Sie auf "Speichern".

Der lokalisierte Text für die Text-Chat-Voreinstellung wird hinzugefügt.

Verwalten der automatisierten Aufgaben für die Umgebung der Live-Unterstützung

Sie müssen den automatischen Aufgaben-Editor installieren und konfigurieren, um die automatischen Aufgaben zu verwalten, mit deren Hilfe Support-Automatisierung-Analysten Endanwender unterstützen. Der Endanwender kann eine automatische Aufgabe in einem Knowledge-Dokument und der Self-Service-Schnittstelle öffnen, oder ein Analyst führt während einer Unterstützungssitzung eine automatische Aufgabe aus. Die automatisierte Aufgaben bieten Analysten detaillierte Informationen über den Computer des Endanwenders. Sie erstellen automatische Self-Service-Aufgaben, die mit dem Endanwender interagieren und die Eingabe des Endanwenders bearbeiten. Diese Aufgaben können das Dateisystem und die Registrierung ändern, Installationssoftware herunterladen und so weiter.

Gehen Sie wie folgt vor:

1. Installieren Sie den automatischen Aufgaben-Editor.

Verwenden Sie folgenden Speicherort, und starten Sie das Installationsprogramm auf den Installationsdatenträgern von der DVD:

casd.nt\SAScriptWriter

Hinweis: In Ihrer Unterstützungsumgebung können Sie das Installationsprogramm auch kopieren und den entsprechenden Anwendern bereitstellen. Der Editor für automatisierte Aufgaben wird installiert, und es wird eine Verknüpfung auf Ihrem Desktop erstellt.

2. Doppelklicken Sie auf die Verknüpfung, um den Editor für automatisierte Aufgaben zu öffnen.

3. Klicken Sie auf 'Werkzeuge', 'Server'.

Das Dialogfeld 'Serverkonfiguration' wird angezeigt.

4. Geben Sie Hostnamen und Port an.

Standard: 8070

5. Geben Sie den Anwendernamen und das Kennwort eines Anwenders mit Lese-/Schreibzugriff auf den Editor für automatisierte Aufgaben an, z. B. die Anmeldedaten eines Support-Automatisierung-Analysten.

6. Klicken Sie auf "Test".

Das Tool versucht, auf die Service Desk-Anwendung zuzugreifen, indem der Aufruf der Webservices verwendet wird, und es wird überprüft, ob die Anwendung vorhanden und mithilfe der Anmeldeinformationen zugreifbar ist.

7. Klicken Sie auf "OK".

Die automatisierten Aufgaben werden erstellt und auf Ihren Server hochgeladen.

Sie können öffentliche Aufgaben exportieren oder sie bestimmten Mandanten und Untermandanten zuweisen.

Wichtig! Nur Rollen des Service Provider-Mandanten, bei denen der Flag "Öffentliche Daten aktualisieren" aktiviert ist, können Aufgaben und Bibliotheken auf den Server hochladen. Alle Inhalte der Aufgabenbibliothek und statischer Inhalt werden als öffentliche Daten gespeichert.

Das Setup wird abgeschlossen, und Analysten können dieses Setup verwenden, um den Anwendern zu helfen. Support-Automatisierung-Analysten überwachen und verwalten mehrere Endanwender-Requests in Live-Unterstützungssitzungen. Analysten verwenden Support-Automatisierung-Werkzeuge, um mit Endanwendern zu interagieren und eine Live-Unterstützung bereitzustellen. Analysten greifen auf die Schnittstelle von einem CA SDM-Ticket, wie z. B. einem Incident, oder der Support-Automatisierung-Registerkarte zu, und sie starten die Sitzung.

Starten der Live-Unterstützung durch Analysten

Analysten starten die Live-Unterstützung folgendermaßen:

1. Sie führen einen der beiden *folgenden* Schritte aus:
 - Sie melden sich bei CA SDM an und klicken auf die Registerkarte "Support-Automatisierung".
 - Sie öffnen ein CA SDM-Ticket und klicken auf die Registerkarte "Support-Automatisierung".
2. CA SDM fordert den Analysten auf, die 32-Bit-Version von Java Runtime Environment (JRE) 1.6 oder später zu installieren, falls sie nicht bereits installiert ist. Die Support-Automatisierung-Analystenoberfläche unterstützt 64-Bit-JRE nicht.

Hinweis: Der Safari-Browser benötigt 32-Bit-JRE 1.6.0_30 oder höher.

CA SDM startet die Analystenschnittstelle der Support-Automatisierung.

Hinweis: In der Tabelle "sa_login_session" wird jedes Mal ein Datensatz erstellt, wenn ein Analyst die Analystenschnittstelle der Support-Automatisierung startet, und wenn ein Endanwender den Web-Client startet. Weitere Informationen zur Tabelle "sa_login_session" finden Sie im technischen *CA SDM-Referenzhandbuch*.

Konfigurieren von Java-Verbindungsoptionen

Sie können Java-Verbindungsoptionen konfigurieren, um Probleme zu lösen, wenn die Support-Automatisierung-Analyst-Schnittstelle nicht mit dem Support-Automatisierung-Server verbunden werden kann. Ein solches Problem kann auftreten, wenn die Standard-Browser-Konfiguration des Analysten nicht korrekt für Ihre Umgebung eingerichtet ist und die Live-Unterstützung daher nicht gestartet wird. Sie können die Einstellungen für die Analyst-Verbindung von einem Browser oder dem Java-Systemsteuerung aus bearbeiten.

So konfigurieren Sie Verbindungsoptionen in Ihrem Browser

1. Öffnen Sie Ihrem Webbrowser, beispielsweise Internet Explorer.
Der Browser wird angezeigt.
2. Klicken Sie auf "Extras" > "Internetoptionen".
Das Dialogfeld "Internetoptionen" wird angezeigt.
3. Konfigurieren Sie die gewünschten Verbindungseinstellungen, wie eine Direktverbindung oder Proxy-Server.
4. Klicken Sie auf "OK".
Die Verbindungseinstellungen werden konfiguriert.

So konfigurieren Sie Verbindungseinstellungen in der Java-Systemsteuerung.

1. Öffnen Sie die Java-Systemsteuerung mit dem folgenden Befehl:
`javaws -viewer`
Die Java-Systemsteuerung wird angezeigt.
2. Klicken Sie auf der Registerkarte "Allgemein" auf "Netzwerkeinstellungen".
Das Dialogfeld "Netzwerkeinstellungen" wird angezeigt.
3. Konfigurieren Sie die gewünschten Einstellungen, wie eine Direktverbindung oder Proxy-Server.
Klicken Sie auf "OK".
Die Verbindungseinstellungen werden konfiguriert.

Konfigurieren von Live-Unterstützung für Analysten

Sie konfigurieren die Analystenschnittstelle der Support-Automatisierung, indem Sie die Rollen- und Sicherheitsrechte für Analysten in Ihrer Live-Unterstützungsumgebung folgendermaßen festlegen:

1. Erstellen oder bearbeiten Sie die geeigneten [Rollen](#) (siehe Seite 1106) und [Support-Automatisierung-Zugriffsebenen](#) (siehe Seite 1111) für Analysten in Ihrer Live-Unterstützungsumgebung.
Sie aktualisieren Rollen und Zugriffsebenen, um Analysten die Berechtigungen für bestimmte Tools zu gewähren, die diese in Unterstützungssitzungen verwenden können.
2. Definieren und verwalten Sie [Warteschlangen](#) (siehe Seite 1116) für Ihre Live-Unterstützungsumgebung.
Sie erstellen Warteschlangen, um eingehende Live-Unterstützungsanfragen angemessen weiterzuleiten.

3. Definieren und verwalten Sie [Aktivitätsbenachrichtigungen](#) (siehe Seite 1112) für Ihre Live-Unterstützungsumgebung.

Sie erstellen E-Mail-Benachrichtigungen, um Analysten zu benachrichtigen, wenn eine Unterstützungssitzungsanfrage in ihre Warteschlange gestellt wurde.

4. Definieren und verwalten Sie [Chat-Voreinstellungen](#) (siehe Seite 1128) für Ihre Live-Unterstützungsumgebung.

Sie erstellen Chat-Voreinstellungen, die Analysten verwenden, um vorkonfigurierte Antworten auf häufig gestellte Fragen und bei oft auftretenden Problemsituationen zu geben.

5. Definieren und verwalten Sie automatisierte Aufgaben für Ihre Live-Unterstützungsumgebung.

Sie erstellen automatisierte Aufgaben, um bestimmte Aktionen auf dem Endbenutzer-Computer auszuführen.

Hinweis: Sie können nur über den Editor für Automatisierte Aufgaben IDE Skripts erstellen und laden.

Verbinden von Endbenutzern mit Unterstützungssitzungen

Ein Endbenutzer fordert auf Ihrer CA SDM-Startseite Unterstützungssitzungen an oder wendet sich direkt, per Telefon oder E-Mail, an das Helpdesk. Der Support-Automatisierung-Analyst lädt den Endbenutzer vom CA SDM-Ticket aus zu einer Sitzung ein.

1. Der Endbenutzer führt *einen* der folgenden Schritte aus:

- Der Endbenutzer fordert von der CA SDM-Startseite aus einen Live-Chat an.

Die Live-Chat-Seite wird angezeigt, und der Endbenutzer wird aufgefordert, den Incident-Bereich und die Beschreibung anzugeben. Der Endbenutzer klickt auf 'Fortsetzen', die Sitzung wird geöffnet, und der Endbenutzer wird in die entsprechende Warteschlange eingereiht.

- Er klickt auf einen Link in einer E-Mail-Benachrichtigung und meldet sich bei der Unterstützungssitzung an, indem er seine Anmeldeinformationen und einen vom Analysten bereitgestellten Sitzungscode verwendet.

Wenn der Endbenutzer die Verbindung von der E-Mail-Benachrichtigung aus herstellt, wird die Warteschlange umgangen.

- Er klickt auf 'Analysten jetzt kontaktieren' und gibt den Sitzungscode an, um die Warteschlange zu umzugehen.

Hinweis: Wenn der Support-Automatisierung-Endanwender-Client startet, wird eine ausführbare Datei heruntergeladen, um das Programm zu auszuführen. Der Endanwender führt die Datei manuell aus. Aus Sicherheitsgründen besteht allerdings ein Zeitlimit für die Ausführung der Datei. Nachdem das Zeitlimit erreicht ist, erscheint eine Fehlermeldung auf dem Computer des Endanwenders, wenn dieser versucht, die Datei zu starten.

2. Der Analyst bietet dem Endbenutzer über Chat eine Live-Unterstützung. Der Endbenutzer benutzt seinen Webbrowser, um mit dem Analysten zu sprechen, oder er startet die Programmdatei.

Hinweis: Wenn der Analyst die Sitzung mit Hilfe von Web-Chat nicht lösen kann, kann er den Endbenutzer vom Sitzungsfenster aus auffordern, die vollständigen Werkzeuge in der Analystenschnittstelle der Supportautomatisierung zu verwenden. Der Endbenutzer muss die Aufforderung akzeptieren, damit der Client auf seinem Computer gestartet werden und der Analyst diese Werkzeuge verwenden kann.

Wie Analysten die Unterstützung für Endbenutzer automatisieren

Analysten verwenden Live-Unterstützungs-Tools, um die folgenden Aufgaben auf dem Computer des Endbenutzers auszuführen:

- Live-Chat-Sitzungen hosten
- Dateisysteme anzeigen
 - Dateien und Verzeichnisse erstellen, ändern, umbenennen oder löschen
 - Dateien und Verzeichnisse auf den Computer des Endbenutzers kopieren und übertragen
- Systemregistrierungen anzeigen
 - Registrierungsdatensätze erstellen, bearbeiten oder löschen
 - Registrierungswerte aus der Endbenutzerregistrierung exportieren oder importieren
- Endbenutzerscreenshots erstellen, wenn die Verbindungsqualität für die Remote-Control-Hilfe nicht ausreicht
- Computerdesktop des Endbenutzers anzeigen
- Computer des Endbenutzers fernsteuern
- Programme auf dem Computer des Endbenutzers starten
- Computer des Endbenutzers neu starten oder herunterfahren
- Automatischen Task ausführen

Hinweis: Weitere Informationen darüber, wie Analysten die Live-Unterstützungs-Tools verwenden, finden Sie in der *Online-Hilfe*.

Weitere Informationen:

[Verwalten der Support-Automatisierung-Zugriffsebenen](#) (siehe Seite 1111)

Bereitstellen der Live-Unterstützung durch Analysten

Analysten stellen Endbenutzern Live-Unterstützung über die Analystenschnittstelle der Support-Automatisierung bereit. Analysten verarbeiten Endbenutzer, die in ihre Warteschlangen weitergeleitet wurden, verwalten Unterstützungssitzungen und nehmen an Sitzungen teil, für die sie berechtigt sind.

1. Der Endbenutzer fordert eine Unterstützungssitzung auf der Startseite von CA SDM an, oder er fordert ein Ticket an, z. B. Incident, Anfrage oder Issue.
2. Der Endbenutzer wird in eine Warteschlange gestellt.

Hinweis: Wenn der Endbenutzer über die Verknüpfung der E-Mail-Einladung des Analysten an der Sitzung teilnimmt, dann wird die Warteschlange übersprungen.

Sie konfigurieren Anfragebereiche und Issue-Kategorien von CA SDM für die Warteschlangenweiterleitung.

3. Der Analyst wählt den Endbenutzer aus der Warteschlange aus.
4. Die Unterstützungssitzung beginnt und der Analyst stellt Live-Unterstützung bereit.

Hinweis: Wenn der Analyst auf der Registerkarte "Support-Automatisierung" die Analystenschnittstelle für Support-Automatisierung startet, wird kein CA SDM-Ticket mit der Unterstützungssitzung verknüpft.

5. Der Analyst erstellt das Ticket, wenn die Unterstützungssitzung beendet wird, und definiert den Status als *SA-Offen* oder *SA-Gelöst*; oder die Unterstützungssitzung wird in eine andere Warteschlange übertragen.
6. Der Analyst beendet die Sitzung, und der Endbenutzer erhält eine E-Mail-Benachrichtigung mit dem Sitzungsprotokoll.

Hinweis: Weitere Details darüber, wie Analysten Warteschlangen verarbeiten und Unterstützungssitzungen verwalten können, finden Sie in der *Online-Hilfe*.

Support-Automatisierung-Anwenderverwaltung

System- und Mandantenadministratoren konfigurieren CA SDM-Kontakte, Rollenberechtigungen, Zugriffs- und Datenschutzebenen, um Anwenderrechte zu definieren. Im Folgenden werden Anwender aufgelistet, die Support-Automatisierung verwenden.

Systemadministrator

Definiert den systemübergreifenden Zugriff, um alle Support-Automatisierung-Standardwerte und Funktionen in der Registerkarte 'Verwaltung' hinzuzufügen, zu bearbeiten und zu ändern. Der Systemadministrator richtet Mandanten und Analysten ein, passt die Support-Automatisierung-Systemeigenschaften an und ist für das Zurücksetzen des Systemkennworts zuständig.

Mandantenadministrator

Definiert die Administratorrechte auf der Mandantenebene und ist nicht berechtigt, Zugriffsrechte für das Erstellen oder Bearbeiten anderer Mandanten zu erteilen oder Anwenderkennwörter zurückzusetzen. Der Service Provider-Mandant legt die Berechtigungen fest.

Analyst

Definiert die Rechte für den Anwender, der EndAnwendern Live-Unterstützung in Ihrer Unterstützungsumgebung bereitstellt.

Endanwender

Definiert die Rechte für Anwender, die eine Live-Unterstützung durch Analysten in Ihrer Unterstützungsumgebung anfordern können, z. B. Angestellte und Kunden.

Konfigurieren von Rollenberechtigungen

Sie können CA SDM-Rollen so konfigurieren, dass Support-Automatisierung möglich ist. Sie können Rollenberechtigungen in Ihrer Umgebung für Live-Unterstützung wie folgt durch Konfigurieren von Support-Automatisierung-Zugriffsebenen für Analysten und Privatsphären-Ebenen für Endbenutzer festlegen.

1. Konfigurieren Sie die gewünschten Zugriffsebenen für Analysten in Ihrer Umgebung für Live-Unterstützung.

Sie erstellen Zugriffsebenen für Analysten, um die Analystenberechtigungen in Ihrem System zu verwalten, wie beispielsweise Aktivieren und Deaktivieren von spezifischen Support-Automatisierung-Analysten-Schnittstellen-Tools.

2. Konfigurieren Sie die gewünschten Privatsphären-Ebenen für Endbenutzer in Ihrer Umgebung für Live-Unterstützung.

Sie erstellen Privatsphären-Ebenen, um Endanwender-Zugriffsebenen in Ihrem System zu verwalten.

3. [Zuweisen](#) (siehe Seite 1112) von Zugriffsebenen zu Rollen.

Sie weisen Endanwender-Privatsphären-Ebenen und Analysten-Zugriffsebenen für Rollen in Ihrer Umgebung zu.

Hinweis: Weitere Informationen über Erstellen und Ändern von Support-Automatisierung-Zugriffsebenen für Analysten und Konfigurieren von Sicherheitsstufen für Endbenutzer finden Sie in der *Online-Hilfe*.

Support-Automatisierung anonyme und registrierte Benutzer

Der Support-Automatisierung-Server akzeptiert registrierte oder anonyme Benutzer je nach den in CA SDM vorhandenen Genehmigungen. Sofern dies erlaubt ist, gestattet der Gastbenutzer anonymen Benutzern, sich in CA SDM anzumelden. Sie können sich vom Server authentifizieren lassen, um Zugriff auf Folgendes zu bekommen:

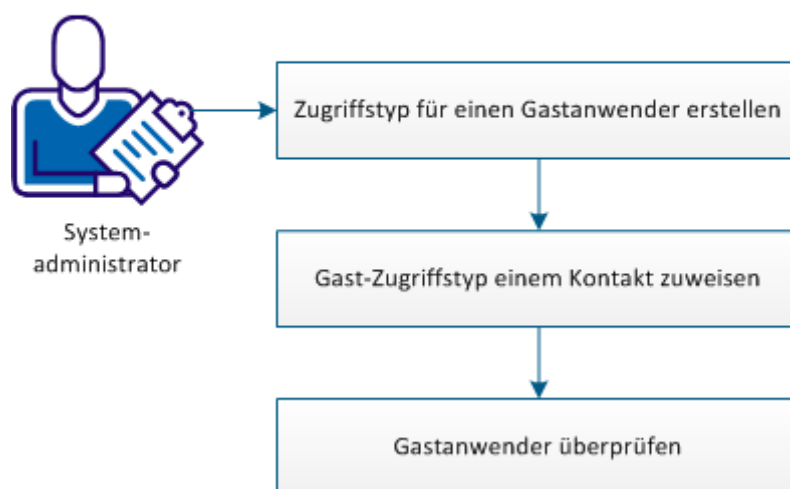
- Live-Unterstützung
- Self-Service
- Editor für automatisierte Aufgaben
- Endanwender-Client

So legen Sie die Support-Automatisierung für einen Gastanwender fest

Als Systemadministrator konfigurieren Sie Ihre Umgebung der Live-Unterstützung, um es Gastanwendern zu ermöglichen, mit den Analysten zu interagieren. Sie können einen Gastanwender für einen spezifischen Mandanten konfigurieren oder den Anwender für das gesamte System zur Verfügung stellen. Ein Mandant ist ein Anwender, der eine einzelne Instanz einer Softwareanwendung verwendet, die mehreren Kunden in einer Umgebung mit mehreren Mandanten dient.

Folgendes Diagramm veranschaulicht, wie ein Systemadministrator die Umgebung der Live-Unterstützung konfiguriert, um Gastanwendern Folgendes zu ermöglichen:

Einrichten der Support-Automatisierung für einen Gastanwender



Gehen Sie wie folgt vor:

1. [Erstellen Sie einen Zugriffstyp für einen Gastanwender](#) (siehe Seite 1109)
2. [Weisen Sie den Gast-Zugriffstyp einem Kontakt zu.](#) (siehe Seite 1110)
3. [Überprüfen Sie den Gastanwender](#) (siehe Seite 1110)

Erstellen Sie einen Zugriffstyp für einen Gastanwender

Damit sich die Gastanwender ohne Authentifizierung bei CA SDM anmelden können, erstellen Sie einen spezifischen Zugriffstyp in CA SDM. Wenn Sie der Service Provider sind, können Sie für jeden Mandanten in Ihrer Umgebung einen Gast-Zugriffstyp anlegen.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei CA SDM an.
2. Klicken Sie auf der Registerkarte "Administration" auf die Option "Sicherheits- und Rollenmanagement" > "Zugriffstypen".
Die Seite "Zugriffstypen - Liste" wird geöffnet.
3. Klicken Sie auf "Neu erstellen".
Die Seite "Neuen Zugriffstyp erstellen" wird geöffnet.
4. Füllen Sie die Felder nach Wunsch aus.
5. Klicken Sie auf die Registerkarte "Webauthentifizierung". Wählen Sie in der Drop-down-Liste "Validierungstyp" die Option "Geöffnet - Zugriff immer zulassen" aus.
6. Klicken Sie auf "Speichern".
Der Zugriffstyp für Gastanwender wird erstellt.
7. (Optional) Klicken Sie mit der rechten Maustaste auf die Seite "Zugriffstypen - Liste", und wählen Sie "Aktualisieren" aus.
Der Gast-Zugriffstyp erscheint in der Liste.

Weisen Sie den Gast-Zugriffstyp einem Kontakt zu.

Weisen Sie den Gast-Zugriffstyp einem Kontakt zu, nachdem Sie einen Zugriffstyp erstellt haben, sodass der Gast die Funktion der Support-Automatisierung-Live-Unterstützung verwenden kann. Der Gastanwender verwendet eine Webauthentifizierung, um sich bei CA SDM anzumelden. Ein Kontakt ist eine Person, die das System regelmäßig verwendet.

Gehen Sie wie folgt vor:

1. Klicken Sie auf der Registerkarte "Administration" auf die Option "Sicherheits- und Rollenmanagement" > "Kontakte".
Die Seite "Kontakt - Suche" wird geöffnet.
2. Klicken Sie auf "Neu erstellen".
Die Seite "Neuen Kontakt erstellen" wird geöffnet.
Hinweis: Sie können einen Kontakt auch ändern.
3. Wählen Sie in der Drop-down-Liste "Kontakttyp" die Option "Gast".
4. (Optional) Verknüpfen Sie den Kontakt mit einem Mandanten, und machen Sie den Kontakt öffentlich. Diese Verknüpfung hilft den Kontakten dabei, eine automatische Zuweisung eines Request zu akzeptieren.
5. Klicken Sie auf "Speichern".
Der Gast-Zugriffstyp wird dem Kontakt zugewiesen.

Überprüfen Sie den Gastanwender

Nachdem Sie den Zugriffstyp zugewiesen haben, können Sie die Existenz der entsprechenden Anwender in Ihrer Umgebung überprüfen.

Gehen Sie wie folgt vor:

1. Klicken Sie auf der Registerkarte "Administration" auf die Option "Sicherheits- und Rollenmanagement" > "Kontakte".
Die Seite "Kontakt - Suche" wird geöffnet.
2. Wählen Sie für "Kontakttyp" die Option "Gast" und "Zugriffstyp" aus, den Sie zugewiesen haben.
3. Klicken Sie auf "Suchen".
Die Seite "Kontaktliste" wird geöffnet.

Der Kontakttyp und der Zugriffstyp sind auf der Seite "Kontaktliste" verfügbar.

Dieser Schritt schließt das Support-Automatisierung-Setup für einen Gastanwender ab.

Verwalten der Support-Automatisierung-Zugriffsebenen

Sie können Support-Automatisierung-Zugriffsebenen verwalten und sie innerhalb Ihrer Unterstützungsumgebung verschiedenen CA SDM-Rollen zuweisen.

Unterstützungsumgebungen variieren in Größe und Struktur, d.h. die Implementierung von Zugriffsebenen richtet sich entsprechend danach.

In einer kleinen Unterstützungsumgebung darf es nicht mehr als einen oder zwei Analysten innerhalb einer Zugriffsebene (z. B. "Analyst") geben. In einer größeren Unterstützungsumgebung kann der Mandantenadministrator mehrere Analysten-Zugriffsebenen einrichten, wobei jede Ebene unterschiedliche Zugriffs- und Unterstützungsprivilegien hat.

Wichtig! Wenn Sie in einer Umgebung für mehrere Mandanten arbeiten, haben Analysten, die nicht dem Service Provider angehören, nur auf ihre eigenen Mandanten und untergeordnete Mandanten Schreibzugriff. Sie können diesem Analysten Schreibzugriff auf andere Mandanten und untergeordnete Mandanten zuweisen, indem Sie den Funktionszugriff des jeweiligen Mandanten so aktualisieren, dass auch Mandanten enthalten sein dürfen, die nicht zum Service Provider gehören.

Die folgenden Zugriffsebenen sind verfügbar:

Analyst

Kontakttyp, der in Ihrer Unterstützungsumgebung Live-Unterstützung für Endbenutzer bereitstellt. Zugriffsebenen definieren jeweils, welche Warteschlangen, automatisierten Aufgaben und Tools dem Analysten zur Verfügung stehen.

Endanwender

Kontakttyp, der Live-Unterstützung von Analysten erhält, z. B. "Mitarbeiter" und "Kunde".

Sie können die Support-Automatisierung-Zugriffsebenen auf der Registerkarte "Administration" verwalten.

Hinweis: Weitere Information über das Erstellen und Ändern von Support-Automatisierung-Zugriffsebenen für Analysten und Endbenutzer finden Sie in der *Online-Hilfe*.

Zuweisen einer Zugriffsebene für eine Rolle

Sie können Support-Automatisierung-Zugriffsebenen existierenden CA SDM-Rollen in Ihrer Umgebung zuweisen.

So weisen Sie einer Rolle eine Zugriffsebene zu

1. Wählen Sie auf der Registerkarte "Administration" > "Sicherheit und Rollenverwaltung" > "Rollenverwaltung" > "Rollenliste".
Die Seite "Rollenliste" wird angezeigt.
2. Klicken Sie auf die Rolle, der Sie eine Zugriffsebene zuweisen wollen, wie beispielsweise "Administrator".
Die Seite "Rolle - Detail" wird angezeigt.
3. Klicken Sie auf "Bearbeiten".
Die Seite "Rolle aktualisieren" wird angezeigt.
4. Wählen Sie auf der Registerkarte "Autorisierung" die von Ihnen erstellte Zugriffsebene aus der SA-Zugriffs-Dropdown-Liste aus und klicken Sie auf "Speichern".
Die Seite "Rolle - Detail" wird angezeigt. Überprüfen Sie, ob der Support-Automatisierung-Zugang der Rolle zugewiesen ist.

Support-Automatisierung-Aktivitätsbenachrichtigungsverwaltung

Sie können Aktivitätsbenachrichtigungen benutzen, um Support-Automatisierung-Aktivitäten zu verwalten. Sie können definieren, wie Endbenutzer, Analysten und Administratoren Benachrichtigungen überwachen und beim Auftreten einer Aktivität, z. B. dem Ende einer Unterstützungssitzung, empfangen sollen.

Konfigurieren Sie für Ihre Umgebung eine der folgenden Standardbenachrichtigungen:

Benachrichtigung über Warteschlangeneintrag

Benachrichtigt den Analysten, wenn ein Endbenutzer in die Warteschlange für eine Unterstützungssitzung gestellt wird.

Benachrichtigt den Analysten, wenn die Unterstützungssitzung in eine andere Warteschlange gestellt wird.

Benachrichtigung des Analysten

Benachrichtigt den Analysten, wenn die Wartezeit der Endanwenderwarteschlange abgelaufen ist. Das Ablaufen der Zeit wird von einem Ereignis-Bedingungsmakro von CA SDM erkannt.

Endanwender zu einer Unterstützungssitzung einladen - Incident

Benachrichtigt den Endbenutzer, wenn ihn der Analyst zu einer Unterstützungssitzung über einen Incident oder eine Anfrage einlädt.

Endanwender zu einer Unterstützungssitzung einladen - Issue

Benachrichtigt den Endbenutzer, wenn ihn der Analyst zu einer Unterstützungssitzung über ein Issue einlädt.

Benachrichtigung über Beendigung der Sitzung

Benachrichtigt das System, wenn die Unterstützungssitzung endet.

Wichtig! Wenn Sie die Support-Automatisierung-Funktionen mit einem externen System, wie Star, verwenden wollen, wird der Kontakt "System_SA_User" standardmäßig auf die Regel *Benachrichtigung über Beendigung der Sitzung* eingestellt.

Support-Automatisierung-Seitenanpassungen

Sie können Support-Automatisierung-Seiten für Ihre Endanwender entsprechend Ihren Geschäftsanforderungen konfigurieren. Über die folgenden Anpassungen können Sie kontrollieren, was dem Anwender angezeigt wird, bevor die Unterstützungssitzung beginnt und nachdem die Sitzung beendet wird:

- Passen Sie die Kopf- und Fußzeile aller Seiten an, die dem Endanwender angezeigt werden.

Sie können den HTML-Code der Kopf- und Fußzeile ändern, und Sie können auch den Standort der CSS-Datei ändern, die die Stildefinitionen enthält.
- Passen Sie die Lokalisierungsanforderungen Ihrer Umgebung an.

Sie können das Standardgebietsschema für alle Analysten und Endanwender festlegen.
- Passen Sie die Seitenlayouts an, die Endanwendern bei der Anmeldung und beim Warten auf die Teilnahme an Unterstützungssitzungen angezeigt werden.

Sie können die Seiten, durch die Ihre Endanwender geführt werden, den Anforderungen Ihres Unternehmens anpassen.

Hinweis: Weitere Informationen über das Konfigurieren von Support-Automatisierung-Seiten für Analysten und Endanwender finden Sie in der *Online-Hilfe*.

Branding-Verwaltung

Sie können die Kopfzeile und Fußzeile von Endanwender-Seiten, wie z. B. der Seite "Self-Service", anpassen. Sie können den HTML-Code im Header und in der Fußzeile verändern, und Sie können den Speicherort von CSS-Dateien verändern, in denen die Stildefinitionen hinterlegt sind.

Sie können eine Liste von Branding-Datensätzen anzeigen, jedoch höchstens einen Datensatz pro Mandant. Mandanten können ihr eigenes Branding erstellen. Falls für einen Mandanten kein Branding definiert ist, verwenden sie die Standardsystemeinstellungen. Sie können auch die Lokalisierung von Brandings ermöglichen und eine Liste aller lokalisierter Brandings für aktivierte Lokalisierungen anzeigen.

Wichtig! Branding-Anpassungen von CA Support-Automatisierung r6,0 SR1 eFix5 werden nicht automatisch nach CA SDM Version 12.9 migriert. Sie sollten Branding-Anpassungen überprüfen, um sicherzustellen, dass sie dem Branding von CA SDM entsprechen. Kopieren Sie bei Bedarf Kopf- und Fußzeilen sowie CSS URL-Daten jedes Organisationsbereichs, und fügen Sie diese in den entsprechenden Mandanten (oder in den öffentlichen Bereich) in CA SDM ein, um die Brandingdaten zu migrieren.

Verwalten der Lokalisierung

"Lokalisierung" bedeutet, dass Sie gleichzeitig mehrere Sprachen innerhalb derselben Installation unterstützen können. Dabei werden einzelne Elemente der Anwendung in eine bestimmte Sprache übersetzt. Zu diesen Elementen können Systemmeldungen, Symbole und Inhalt gehören. Endanwender können somit die entsprechenden Funktionen in ihrer Muttersprache effizient nutzen.

Lokalisierungen von Support-Automatisierung entsprechen den Bedürfnissen Ihrer globalen Umgebung. Jeder Mandant kann mehrere Sprachen beherrschen, und die Lokalisierungen werden über mehrere Mandanten hinweg unterstützt. Die Lokalisierung wird in Abhängigkeit von den Standardsystemeinstellungen eines Mandanten ausgeführt. Sie können die Sprache des Endanwenders und des Analysten einstellen und dann Live-Unterstützung von der Liste der aktivierten Sprachen aufrufen. In einer Unterstützungssitzung kann der Analyst eine andere Sprache verwenden als der Endanwender.

Sie können lokalisierten Text für Haftungsausschlüsse bearbeiten. Sie können Lokalisierungen nicht erstellen oder entfernen, Sie können sie jedoch aktivieren oder sperren.

Hinweis: Die Administratorschnittstelle ist nur in der standardmäßigen Server-Lokalisierung verfügbar.

Seitenlayoutkonfiguration

Wenn Endanwender sich bei "Live-Unterstützung" von CA SDM anmelden, dann wird eine Standard-Startseite angezeigt. Auch wenn der Endanwender zunächst in eine Warteschlange gestellt wird, dann wird eine Standardseite angezeigt.

Wenn für Mandanten keine besonderen Einstellungen festgelegt wurden, dann sind standardmäßig die öffentlichen Einstellungen festgelegt. Sie können die folgenden öffentlichen Einstellungen für Warteschlangen konfigurieren, die keine eigenen besonderen Einstellungen haben:

- Warteseite
- Endanwenderseite nach dem Start
- In Sitzung
- Seite Post-Logout
- Umfrageseite verlassen

Jede Seite hat ihre eigene Detailseite, die aus einem Textfeld zur Eingabe des URL und einem Kontrollkästchen für das Markieren dieser Seite als "extern" besteht.

Support-Automatisierung-Systemeigenschaften

Sie können viele der Methoden, die Support-Automatisierung zur Verarbeitung von Aktivitäten verwendet, so anpassen, dass sie von der Standardinstallation abweichen. Mit den Systemoptionsstandardeinstellungen können Sie das Verhalten von Support-Automatisierung anpassen. Zum Beispiel können Sie einige der folgenden Support-Automatisierung-Optionen anpassen:

- Aktivieren oder deaktivieren Sie den Link für Live-Chat von der Startseite für CA SDM-Angestellte und -Kunden.
- Aktivieren oder deaktivieren Sie den Link für die Teilnahme an einer Sitzung von der Startseite für CA SDM-Angestellte und -Kunden.
- Aktivieren oder deaktivieren Sie die Option, um einen CA SDM-Incident zu erstellen, wenn die Verbindung zum Endanwender getrennt wird, während er in einer Support-Automatisierung-Warteschlange darauf wartet, bedient zu werden.

System-Eigenschaften sind für Mandanten optional. Falls ein Mandant keine Eigenschaften definiert hat, verwendet Support-Automatisierung die öffentlichen (freigegebenen) Einstellungen. Die Produktinstallation erstellt die standardmäßigen öffentlichen Eigenschaften.

Hinweis: Weitere Informationen über das Konfigurieren von Support-Automatisierung-Systemeigenschaften finden Sie in der *Online-Hilfe*.

Support-Automatisierung-Warteschlangenverwaltung

Sie können Warteschlangen verwenden, um Requests für Unterstützungssitzungen an den am besten geeigneten Analysten weiterzuleiten. Der Endanwender kann eine Kategorie oder eine Beschreibung des Computer-Problems auswählen, und das Ticket (z. B. ein Incident) wird dann in die entsprechende Warteschlange weitergeleitet.

Nach der Installation des Produkts ist der Name der Standardwarteschlange "Support". Sie können Warteschlangen einrichten, um verschiedene Support-Requests zu sortieren und nachzuverfolgen, je nachdem wie Ihre konkreten Geschäftsanforderungen sind. Sie können pro Mandant nur eine Standardwarteschlange zuweisen. Wenn Sie keine Standardwarteschlange zuweisen oder wenn die Standardwarteschlange nicht verfügbar ist, verwendet das System die öffentliche Standardwarteschlange. Sie können die Arbeitsstunden pro Warteschlange festlegen.

Das System platziert die Requests von Endanwendern automatisch, indem es Zuordnungen zwischen Warteschlangen und Incident-Bereichen herstellt. Wenn ein Bereich einer Warteschlange zugeordnet wird, wählt der Endanwender eine Kategorie aus und wird zu der entsprechenden Warteschlange weitergeleitet. Suchfunktionen werden auf die Beschreibungen von Incidents oder Issue-Kategorien angewandt, um relevante Warteschlangen zu finden. Der Anwender wird daraufhin an die Warteschlange weitergeleitet, die am besten zu seinem Request passt.

Hinweis: Weitere Informationen über das Anpassen und Zuordnen von Support-Automatisierung-Warteschlangen finden Sie in der *Online-Hilfe*.

Warteschlangenverwaltung

Sie konfigurieren Warteschlangen, um Endbenutzern dabei zu helfen, die geeignete Live-Unterstützung zu erhalten. Sie verwalten Warteschlangen, um das Verfahren zu verbessern, wie Endbenutzer zu Unterstützungssitzungen weitergeleitet werden. Gehen Sie hierfür folgendermaßen vor:

- Passen Sie Warteschlangen für Analysten und Mandanten in Ihrer Live-Unterstützungsumgebung an.

Sie können Warteschlangen aktivieren und deaktivieren und Berechtigungen für Mandanten und Analysten festlegen.

- Weisen Sie Standardwarteschlangen zu.

Sie können Endanwender an die Standardwarteschlange umleiten, wenn sie Abfragen eingeben, die nicht mit den in Ihrer Umgebung konfigurierten Warteschlangen übereinstimmen. Sie können auch Warteschlangen für Mandanten in Ihrer Umgebung anpassen.

Hinweis: Wenn die standardmäßige Mandantenwarteschlange fehlt oder nicht verfügbar ist, dann wird die öffentliche Warteschlange verwendet.

- Weisen Sie Betriebsstunden für Ihre Warteschlangen zu.

Sie können Warteschlangen basierend auf der Verfügbarkeit von Benutzern in Ihrer Unterstützungsumgebung verwalten, z. B. indem Sie Support-Automatisierung-Services während der Geschäftszeiten aktivieren.

Wichtig! Sie können Schichten sowohl Support-Automatisierung-Zeiten als auch einzelnen Live Assistance-Warteschlangen zuweisen. Wenn Sie Support-Automatisierung-Zeiten und einzelnen Warteschlangen verschiedene Schichten zuweisen, kann dies für Analysten und Endbenutzer in Ihrer Unterstützungsumgebung zu Konflikten führen.

Verwalten von Warteschlangen-Zusammenfassungen

Sie können die Felder festlegen, die ein Analyst auf der Seite "Zusammenfassung der Warteschlange" anzeigen kann. Sie haben folgende Felder zur Auswahl, Sie können jedoch keine Felder erstellen:

- Warteschlange
- Frage
- Wartezeit
- E-Mail
- Unternehmen
- IP-Adresse
- Enthält Analysten
- Kategorie
- Sprache
- Mandant

Weitere Informationen:

[Warteschlangenverwaltung](#) (siehe Seite 1116)

[Verwalten der Warteschlangen-Stunden](#) (siehe Seite 1118)

Verwalten der Warteschlangen-Stunden

Sie können Support-Automatisierung für jede Warteschlange für bestimmte Uhrzeiten aktivieren, um sie so an die Arbeitszeiten der Analysten anzupassen. Gehen Sie dafür folgendermaßen vor:

- Erstellen Sie einen separaten Ablaufplan für jede Warteschlange und für alle automatisierten Support Services.

Hinweis: Diese Einstellungen beschränken nicht die Self-Service-Funktionen.

- Definieren Sie Unterstützungsstunden für den Support-Automatisierung-Server durch einen globalen offenen oder geschlossenen Status. Ein Eintrag für jede Stunde der Woche gibt einen Unterschied zum globalen Status des Servers an.
- Der Server verwendet den ersten Eintrag für jede Stunde, basierend auf den von Ihnen festgelegten Regeln.

Diese Aktion verbindet auf wirksame Weise die Definitionen der Unterstützungsstunden in den Einstellungen des übergeordneten Mandanten (oder öffentlichen Einstellungen). Diese Aktion kann zu unerwarteten Ergebnissen führen, wenn eine Kombination der Einstellungen "standardmäßig geschlossen" und "standardmäßig offen" in der Hierarchie verwendet wird.

Verwaltung von Ticket-Vorlagen

Sie können angeben, welche Ticket-Vorlagen für die Analystenbenutzeroberfläche zur Verfügung stehen. Sie können die Ticket-Vorlagen für Incident-, Anfrage und Issue-Ticket-Typen auswählen.

Sie können definieren, ob die Vorlage die Standardvorlage oder aktiv ist. Beim Erstellen einer Ticket-Vorlage können Sie eine Auswahl unter vorhandenen CA SDM-Vorlagen treffen. Die Standardvorlage muss aktiv sein.

Standardmäßig können Sie für jeden Mandanten nur eine Ticket-Vorlage haben.

Hinweis: Weitere Informationen über das Anpassen von Ticket-Vorlagen finden Sie in der *Online-Hilfe*.

Administrationseinstellungen

Sie können die folgenden Support-Automatisierung-Einstellungen definieren und konfigurieren:

- Routing-Server für Meldungen
- Endanwender-Berechtigungen (Privatsphären-Ebenen)
- Support-Automatisierung-Stunden

So konfigurieren Sie die Support-Automatisierung-Einstellungen:

Sie können die Support-Automatisierung-Einstellungen für Ihre Unterstützungsumgebung entsprechend Ihren Geschäftsanforderungen konfigurieren. Mit Hilfe der Einstellungen können Sie administrative Funktionen, wie Routing-Server für Meldungen, Privatsphären-Ebenen und Support-Automatisierung-Uhrzeiten steuern.

- Konfigurieren Sie Routing-Server für Meldungen, um die Leistung während Unterstützungssitzungen zu verbessern.

Sie können Endbenutzer mit dem bevorzugten lokalen Server des Analysten verbinden, oder Sie können bei einer fehlgeschlagenen Verbindung die Sitzung mit dem standardmäßigen Hauptserver verbinden.

- Definieren Sie die Privatsphären-Ebenen für Endbenutzer in Ihrer Umgebung.

Sie können, basierend auf den in Ihrer Umgebung verwendeten Privatsphären-Ebenen, bestimmte Tools von Support-Automatisierung-Analystenschnittstellen aktivieren.

- Legen Sie Ihre Support-Automatisierung-Uhrzeiten auf bestimmte Betriebszeiten oder auf eine durchgehende Betriebsbereitschaft fest.

Sie können Live-Unterstützungsanfragen durchführen, wenn das Support-Desk geschlossen ist, z. B. eine Webseite öffnen, um den Endbenutzer über die Support-Desk-Uhrzeiten und zusätzliche Supportoptionen zu informieren.

Hinweis: Weitere Informationen zum Konfigurieren von Support-Automatisierung-Einstellungen finden Sie in der *Online-Hilfe*.

Nachrichtenroutingserver

Mithilfe von Nachrichtenroutingservern (Message Routing Servers, MRS) können Sie je nach geografischem Standort des lokalen Servers mehrere Remote-Steuerungsserver verwalten. Der Einsatz von MRS trägt zur Optimierung der Leistung bei Unterstützungssitzungen bei. Wenn Sie die Nutzung von MRS (Message Routing Server) ermöglichen, versuchen sich die Support-Automatisierung-Analysten-Schnittstelle und der Endbenutzer-Client für eine gemeinsame Nutzung mit dem bevorzugten (lokalen) Server des Analysten zu verbinden. Falls keine Verbindung hergestellt werden kann, verwendet die Freigabesitzung den Hauptstandardserver. Im Live-Protokoll wird aufgezeichnet, welche MRS Sie während der Unterstützungssitzung verwenden.

Sie können ein Routing-Server-Objekt für Meldungen erstellen, aktualisieren, entfernen, aktivieren oder deaktivieren.

Hinweis: Weitere Informationen zum Konfigurieren von Routing-Servern für Meldungen finden Sie in der *Online-Hilfe*.

Support-Automatisierung-Datenschutzebenen

Mithilfe von Privatsphären-Ebenen können Sie festlegen, welche Aktionen für verschiedene Endanwender ausgeführt werden dürfen, um deren Privatsphäre zu schützen. Datenschutzebenen sind mit CA SDM-Rollen verknüpft. Es sind drei Standardberechtigungen vorhanden: "Hoch", "Mittel" und "Niedrig". Sie können jedoch ggf. weitere definieren. Sie können die Privatsphären-Ebenen, die für den Endanwender verfügbar sind, hinzufügen, aktualisieren und löschen.

Außerdem können Sie den Namen und die Beschreibung der betreffenden Privatsphären-Ebene festlegen. Sie können definieren, welche Funktionen für angegebene Werkzeuge (Datei-Explorer, Remote-Registrierung, Ausführungsprogramm und so weiter) für diese Datenschutzebene aktiviert werden.

Hinweis: Weitere Informationen über das Konfigurieren von Support-Automatisierung-Datenschutzebenen finden Sie in der *Online-Hilfe*.

Support-Automatisierung-Stunden

Sie können Support-Automatisierung so einstellen, dass es nur zu bestimmten Zeiten oder immer arbeitet. Sie verwalten diese Geschäftszeiten je nach den Bedürfnissen der Endanwender in Ihrer Support-Umgebung. Sobald die Support-Automatisierung-Funktion geschlossen ist, können Endanwender nicht mehr darauf zugreifen. Sie können in nur einem Schritt schnell Änderungen an mehreren Schichten vornehmen.

Wichtig! Sie können Schichten sowohl Support-Automatisierungs-Zeiten als auch einzelnen Live Assistance-Warteschlangen zuweisen. Wenn Sie Support-Automatisierungs-Zeiten und einzelnen Warteschlangen verschiedene Schichten zuweisen, kann dies für Analysten und Endanwender in Ihrer Support-Umgebung zu Konflikten führen.

Hinweis: Weitere Informationen zum Verwenden von Support-Automatisierungs-Stunden finden Sie in der *Online-Hilfe*.

Anpassen von Support-Automatisierung-Tools

Sie können die Support-Automatisierung-Tools für Ihre Unterstützungsumgebung entsprechend Ihren Geschäftsanforderungen konfigurieren. Mit Hilfe der Einstellungen können Sie administrative Funktionen, wie automatisierte Aufgaben, Chat-Voreinstellungen, Standardanmeldeinformationen und Disclaimer, steuern.

- Passen Sie die Liste und die Einstufungen der automatisierten Aufgaben an, die Support-Automatisierung-Analysten verwenden, um Endanwender zu unterstützen.
- Konfigurieren Sie Chat-Voreinstellungen für gängige Antworten auf häufig gestellte Fragen und bei oft auftretenden Problemsituationen.
- Konfigurieren Sie Standardanmeldeinformationen für den Zugriff auf einen Endanwender-Computer.
- Passen Sie die Disclaimer an, die Endanwendern vor dem Starten der Self-Service-Aufgaben angezeigt werden.

Hinweis: Weitere Informationen zum Konfigurieren von Support-Automatisierung-Tools finden Sie in der *Online-Hilfe*.

Automatisierte Aufgaben

Ein *automatischer Task* ist eine Sammlung von Schritten, die einen automatischen Prozess definieren, dem der Analyst oder Endbenutzer folgt. Automatische Task-Schritte werden in VBScript oder JavaScript geschrieben und führen bestimmte Aktionen auf dem Computer des Analysten oder des Endbenutzers aus. Sie können neue automatische Tasks und Task-Schritte mit dem Editor für automatisierte Tasks erstellen. Zu den allgemeinen Routinen zählen das Erfassen von Telemetriedaten, die Diagnose von Problemen und die Umsetzung von Lösungen.

Wenn Sie einen automatisierten Task ausführen, wird das Protokoll aktualisiert. Dieses Protokoll ist mit dem Sitzungsprotokoll verknüpft und wird von hier aus geöffnet. Die Einträge im Protokoll der automatisierten Aufgabe bestehen aus einer Reihe von Zeitstempel-Texteinträgen. Die Einträge werden durch das Abrufen von `Functions.LogMessage()` oder `WScript.Echo()` erstellt.

Weitere Informationen:

[Implementieren von automatisierten Aufgaben](#) (siehe Seite 1123)

Konfigurieren automatischer Aufgaben

Sie installieren und konfigurieren den automatischen Aufgaben-Editor, um automatische Aufgaben zu verwalten, mit deren Hilfe Support-Automatisierung-Analysten Endanwender unterstützen. Der Endanwender kann eine automatische Aufgabe in einem Knowledge-Dokument und der Self-Service-Schnittstelle öffnen, oder ein Analyst führt während einer Unterstützungssitzung eine automatische Aufgabe aus. Automatisierte Aufgaben bieten Analysten detaillierte Informationen über den Computer des Endanwenders. Sie erstellen automatische Self-Service-Aufgaben, die mit dem Endanwender interagieren und die Eingabe des Endanwenders bearbeiten. Diese Aufgaben können das Dateisystem und die Registrierung ändern, Installationssoftware herunterladen und so weiter. Sie konfigurieren automatische Aufgaben folgendermaßen:

1. Installieren Sie den automatischen Aufgaben-Editor.

Sie öffnen das Installationsprogramm vom folgenden Standort auf den Installationsdatenträgern:

casd.nt\SAScriptWriter

Hinweis: Sie können auch das Installationsprogramm kopieren und es den entsprechenden Anwendern in Ihrer Unterstützungsumgebung bereitstellen.

Der automatische Aufgaben-Editor wird installiert.

2. Öffnen Sie den automatischen Aufgaben-Editor.

Bei der Installation des automatischen Aufgaben-Editors wird eine Verknüpfung auf Ihrem Desktop erstellt.

3. Legen Sie die folgenden Verbindungsparameter fest:

- a. Klicken Sie auf Werkzeuge, Server.

Das Dialogfeld Serverkonfiguration wird angezeigt.

- b. Geben Sie Hostnamen und Port an.

Standard-Port: 8070

- c. Geben Sie den Anwendernamen und das Kennwort eines Anwenders mit Lese-/Schreibzugriff auf den automatischen Aufgaben-Editor an, z. B. die Anmeldedaten eines Support-Automatisierung-Analysten.

- d. Klicken Sie auf Test.

- e. Klicken Sie auf OK.

4. Erstellen Sie automatische Aufgaben, und laden Sie sie auf Ihren Server.

Sie können öffentliche Aufgaben exportieren oder sie bestimmten Mandanten und Untermantanten zuweisen.

Wichtig! Nur Rollen des Dienstleistermandanten, bei denen der Flag 'Öffentliche Daten aktualisieren' aktiviert ist, können Aufgaben und Bibliotheken auf den Server hochladen. Alle Inhalte der Aufgabenbibliothek und statischer Inhalt werden als öffentliche Daten gespeichert.

Implementieren von automatisierten Aufgaben

Sie können automatisierte Aufgaben verwenden, um Endbenutzer in Ihrer Unterstützungsumgebung zu unterstützen. Durch automatisierte Aufgaben werden bestimmte Aktionen auf dem Endbenutzercomputer ausgeführt, ohne dass der Analyst oder der Endbenutzer diesen Vorgang abschließen müssen. Diese Skripts können Ihnen dabei helfen, Fernmessungsinformationen zu erfassen, Computerprobleme zu diagnostizieren und Lösungen zu implementieren.

Um automatisierte Aufgaben zu implementieren, gehen Sie folgendermaßen vor:

1. Ermitteln Sie Möglichkeiten für eine Support-Automatisierung.

Sie ermitteln Probleme, die häufig bei Endbenutzern auftreten, und entscheiden, dass Sie bestimmte Lösungen automatisieren können, um Ihre Support-Kosten zu reduzieren.

2. Analysieren Sie die Automatisierung von möglichen Problemen.

Sie analysieren die Lösungen für häufig auftretende Probleme und erfassen Daten für die Diagnoseverfahren, die sie anwenden wollen.

3. Entwerfen Sie Aufgaben zur Automatisierung des Supports für Endbenutzer.

Sie entwerfen mit dem Editor für automatisierte Aufgaben für jede Aufgabe die Lösung, die Sie dem Endbenutzer anbieten wollen.

4. Implementieren und testen Sie die automatisierten Aufgaben.

Sie testen die automatisierten Aufgaben um zu überprüfen, dass sie Probleme lösen, die häufig in Ihrer Unterstützungsumgebung auftreten, und dass sie Supportkosten reduzieren helfen.

5. Stellen Sie automatisierte Aufgaben bereit und überwachen Sie sie.

Sie stellen die automatisierten Aufgaben für Endbenutzer in Ihrer Umgebung bereit, indem Sie Analysten deren Verwendung bei Unterstützungssitzungen ermöglichen. Sie können auch Skripts an Knowledge-Dokumente anhängen.

Wichtig! Wenn Sie sich in einer Umgebung mit mehreren Mandanten befinden und zulassen möchten, dass Analysten Aufgaben- und Bibliotheksinhalte hochladen können, muss für deren Rolle die Option "Öffentlich aktualisieren" aktiviert sein.

Hinweis: CA Technologies kann Schulung für das Erstellen von automatisierten Aufgaben und Komponenten, z. B. Vorlagen und Bibliotheken für automatisierte Aufgabenschritte, bereitstellen, die Sie in Ihrer Umgebung verwenden können. Für weitere Informationen über das Entwickeln von automatisierten Aufgaben wenden Sie sich an die *CA Technologies-Services*.

Verwalten automatisierter Aufgaben

Sie können automatische Aufgaben erstellen und sie mit dem Server verbinden. Für den automatischen Aufgaben-Editor benötigen Sie einen Lese-/Schreibzugriff auf alle automatischen aufgabenbezogenen Tabellen. Sie können mit der Anwendung Benutzerverwaltungsfunktionen ausführen, wie z. B. das Zuweisen automatischer Aufgaben an Rollen und Mandanten.

Hinweis: Wenn Sie ein Service Provider-Analyst sind und Zugriff auf mehrere Mandanten haben, können Sie den Mandantenkontext eines beliebigen Aufgabenaktualisierungsvorgangs für den Server auswählen. Sie können auch eine automatische Aufgabe als öffentlich zuweisen.

Automatische Aufgabenbereitstellung

Nachdem Sie eine automatische Aufgabe erstellt und im automatischen Aufgaben-Editor getestet haben, können Sie sie einer Klassifizierung auf dem CA SDM-Server für die Verwendung in Unterstützungssitzungen oder im Self-Service bereitstellen. Einige Einstellungen, die nicht Teil der automatisierten Aufgabendefinition sind, werden festgelegt, wenn Sie die Aufgabe bereitstellen.

Sie können automatische Aufgaben vom automatischen Aufgaben-Editor direkt auf den Server herauf- bzw. herunterladen. Sie wählen den entsprechenden Mandanten aus, wenn automatische Aufgabenklassifizierungen erstellt werden. Wenn Sie Skripts auf den Server hochladen, wählen Sie die Klassifizierung oder den Mandanten aus, auf die/den Sie einen Zugriff haben, oder legen Sie das Skript als öffentlich fest. Sie können auch automatische Aufgaben aus XSDF-Dateien importieren und sie in XSDF-Dateien exportieren.

Wichtig! Wenn Sie sich in einer Umgebung mit mehreren Mandanten befinden und zulassen möchten, dass Analysten Aufgaben- und Bibliotheksinhalte hochladen können, muss für deren Rolle die Option "Öffentlich aktualisieren" aktiviert sein.

Laden einer automatisierten Aufgabe

Sie können automatisierte Aufgaben laden, die Sie in der Anwendung erstellt haben. Wenn Sie eine Aufgabe wählen, wird automatisch der gesamte Inhalt geladen, wie Bibliotheken und statischer Inhalt.

So laden Sie eine automatisierte Aufgabe

1. Öffnen Sie den Editor für automatisierte Aufgaben.
Der Support-Automatisierung-Task-Editor wird angezeigt.
2. Wählen Sie die automatisierte Aufgabe aus, die Sie laden möchten.
3. Wählen Sie die Klassifikation aus, in die das Verzeichnis eingefügt werden soll.
Hinweis Wenn Sie ein privilegierter Benutzer in einer Umgebung mit mehreren Mandanten sind, wählen Sie den entsprechenden Mandanten aus, wenn Sie die automatisierte Aufgabe laden, oder machen Sie die Aufgabe öffentlich.
4. Wählen Sie in der Symbolleiste das Symbol zum Hochladen von automatisierten Aufgaben.
Der Support-Automatisierung-Task Editor lädt die Aufgabe auf den Server.

Bearbeiten von automatisierten Aufgaben

Sie können automatisierte Aufgaben vom Server herunterladen und diese im Editor für automatisierte Aufgaben bearbeiten. Der Inhalt einer neueren Version als der bestehende Inhalt auf dem Server wird in die Datenbank importiert und steht so den Administratoren dieses Mandanten zur Verfügung.

So bearbeiten Sie eine automatisierte Aufgabe

1. Öffnen Sie den Editor für automatisierte Aufgaben.
Der Support-Automatisierung-Editor wird angezeigt.
2. Wählen Sie in der Symbolleiste das Symbol zum Hochladen von automatisierten Aufgaben.
Im Fensterbereich "Server" wird die Option "Automatisierte Aufgabe öffnen".
3. Wählen Sie die automatisierte Aufgabe aus, die Sie herunterladen möchten.
Hinweis Wenn Sie ein privilegierter Benutzer in einer Umgebung für mehrere Mandanten sind, können Sie öffentliche oder mandantenspezifische automatisierte Aufgaben bearbeiten.
4. Klicken Sie auf "Aufgabe öffnen".
Der Support-Automatisierung-Task Editor lädt die Aufgabe auf den Client herunter. und öffnet sie in der Anwendung.
Durch das Herunterladen wird eine Textdatei auf dem Computer erstellt des Autors der automatisierten Aufgabe erzeugt, die den abhängigen Inhalt enthält.

Anmeldeinformationen für eine automatische Aufgabe

Sie können eine automatische Aufgabe, z. B. eine Softwareinstallation, für die Sie Administratorrechte benötigen, folgendermaßen ausführen:

- Definieren Sie die Standardanmeldeinformationen für den Mandanten, und konfigurieren Sie die automatische Aufgabe, um die Standardanmeldeinformationen bei der Verwaltung der automatischen Aufgaben zu verwenden.
- Definieren Sie die Standardanmeldeinformationen für den Mandanten, und geben Sie an, dass Sie das Dialogfeld 'Ausführen als' im Fenster der Unterstützungssitzung verwenden.
- Definieren Sie Anmeldeinformationen der automatischen Aufgabe, und geben Sie an, dass Sie das Dialogfeld 'Ausführen als' im Fenster der Unterstützungssitzung verwenden.
- Geben Sie die Anmeldeinformationen im Dialogfeld 'Ausführen als' im Fenster der Unterstützungssitzung an.

Rollenzuweisung

Sie weisen die angemessenen Rollen (z. B. Analyst, Administrator) zu, um die automatische Aufgabe zu verwenden. Sie weisen individuelle automatische Aufgaben ausgewählten Rollen zu, um die automatischen Aufgaben nur auf die Analysten in der zugewiesenen Rolle zu beschränken. Sie können die unterschiedlichen Kompetenzen oder Erfahrungsniveaus innerhalb der Unterstützungsorganisation verwalten.

Sie können die Rollen auf Aufgabenebene verwalten, indem Sie auswählen, dass bestimmte allgemeine Aufgaben, wie zum Beispiel Diagnostik, automatisch ausgeführt werden, wenn der Endbenutzer eine Sitzung beginnt.

Zuweisen einer Zugriffsebene für eine Rolle

Sie können Support-Automatisierung-Zugriffsebenen existierenden CA SDM-Rollen in Ihrer Umgebung zuweisen.

So weisen Sie einer Rolle eine Zugriffsebene zu

1. Wählen Sie auf der Registerkarte "Administration" > "Sicherheit und Rollenverwaltung" > "Rollenverwaltung" > "Rollenliste".
Die Seite "Rollenliste" wird angezeigt.
2. Klicken Sie auf die Rolle, der Sie eine Zugriffsebene zuweisen wollen, wie beispielsweise "Administrator".
Die Seite "Rolle - Detail" wird angezeigt.
3. Klicken Sie auf "Bearbeiten".
Die Seite "Rolle aktualisieren" wird angezeigt.
4. Wählen Sie auf der Registerkarte "Autorisierung" die von Ihnen erstellte Zugriffsebene aus der SA-Zugriffs-Dropdown-Liste aus und klicken Sie auf "Speichern".
Die Seite "Rolle - Detail" wird angezeigt. Überprüfen Sie, ob der Support-Automatisierung-Zugang der Rolle zugewiesen ist.

Verwalten von Chat-Voreinstellungen

Sie können häufige Antworten auf häufig gestellte Fragen und Situationen erstellen. So können sich wiederholende Informationen, die oft getippt werden, gespeichert und in anderen Chat-Sitzungen verwendet werden.

Sie können Endanwendern am Anfang jeder Sitzung automatisch Voreinstellungen, wie z. B. einen Gruß, senden. Sie können die Voreinstellungen auch automatisch mit Informationen auffüllen, die sich spezifisch auf die aktuelle Sitzung beziehen, wie z. B. den Namen des Analysten.

Sie können die folgenden Arten von Voreinstellungen in einer Unterstützungssitzung verwenden:

Chat-Voreinstellung

Identifiziert eine häufig verwendete Textantwort auf eine Endanwenderfrage.

URL-Voreinstellung

Identifiziert eine häufig verwendete URL, auf die der Endanwender zugreifen kann.

Sie können jede Chat-Voreinstellung lokalisieren. Die Chat-Voreinstellung wird mit der Endanwenderlokalisierung synchronisiert, so dass der Endanwender die korrekten lokalisierten Voreinstellungen erhält.

Verwalten von Chat-Voreinstellungen

Sie können vordefinierte Antworten auf häufig gestellte Fragen und bei oft auftretenden Problemsituationen verwenden.

1. Machen Sie sich kundig, wie die typischen Unterstützungssitzungen in Ihrer Organisation verlaufen.
2. Erstellen Sie Chat- und URL-Voreinstellungen gemäß den Anforderungen Ihrer Organisation.
3. Legen Sie fest, ob die Voreinstellungen mandantenspezifisch oder öffentlich verfügbar sein sollen.
4. (Optional) Duplizieren Sie die Baumstruktur der Voreinstellungen, um lokalisierte Umgebungen zu verwalten.
5. Senden Sie während einer Unterstützungssitzung Chat- und URL-Voreinstellungen.

Hinweis: Weitere Informationen zum Konfigurieren von Chat-Voreinstellungen finden Sie in der *Online-Hilfe*.

Standardanmeldeinformationen

Sie können auch dann automatisierte Aufgaben auf dem Computer eines Endanwenders ausführen, wenn der Endanwender gewöhnlich keine Zugriffsrechte für derartige Aktivitäten hat. Falls der aktuelle Endanwender keine Administratorrechte hat, um Systeminformationen zu seinem Computer anzuzeigen, können Sie eine beschränkte automatisierte Aufgabe ausführen, indem Sie sich mithilfe von Standardanmeldeinformationen Zugriff verschaffen.

Hinweis: Weitere Informationen zum Konfigurieren der Standardanmeldeinformationen finden Sie in der *Online-Hilfe*.

Disclaimer

Wenn der Endanwender Self-Service-Aufgaben startet, erscheint ein Disclaimer-Text, dem er zustimmen muss, bevor er fortfahren kann.

Sie können Disclaimer-Business-Objekte erstellen, aktualisieren und löschen.

Hinweis: Weitere Informationen zum Konfigurieren von Support-Automatisierung-Disclaimern finden Sie in der *Online-Hilfe*.

Sitzungsprotokoll-Verwaltung

Über das Sitzungsprotokoll können Sie alle Aktionen eines Analysten während einer Unterstützungssitzung einsehen, z. B. welche Tools verwendet wurden und welche Informationen im Chat ausgetauscht wurden (mit Ausnahme von Flüsternachrichten). Sie können das Sitzungsprotokoll drucken oder dem Endbenutzer per E-mail senden. Endbenutzer können das Protokoll auch anzeigen und speichern, Sie können es jedoch nicht ändern.

Anzeigen des Sitzungsprotokolls

Alle Aktionen, die Sie während der Unterstützungssitzung durchführen, wie Plauschdialog (ausgenommen Geflüster-Gespräche), automatisch aufgeführte Aufgabenergebnisse und das Verwenden eines Support-Automatisierung-Analystenschnittstellen-Tools, aktualisieren das Sitzungsprotokoll.

So zeigen Sie das Sitzungsprotokoll an:

1. Öffnen Sie die Ansicht der aktiven Sitzung.
Die Seite "Aktive Sitzung" wird angezeigt.
2. Wählen Sie das Sitzungsprotokoll von der Symbolleiste oder aus dem Menü "Sitzungen" aus.
Die Seite "Sitzungsprotokoll" wird angezeigt.
3. Klicken Sie auf "Jetzt aktualisieren".
Die Seite wird aktualisiert.
4. (Optional) Aktivieren Sie das Kontrollkästchen zur automatischen Aktualisierung.
5. (Optional) Klicken Sie auf "Protokoll auf Festplatte speichern".
Das Dialogfeld "Speichern" wird angezeigt. Sie können das Sitzungsprotokoll lokal als eine HTML-Datei speichern.

Support-Automatisierung-Berichte

CA Business Intelligence installiert diverse vordefinierte Support-Automatisierung-Berichte. Während der Installation stellt CA SDM diese Berichte automatisch auf dem BusinessObjects-Server zur Verfügung.

Der Support-Automatisierung-Administrator und Support-Automatisierung-Analystenrollen können BusinessObjects InfoView dazu verwenden, detaillierte und zusammengefasste Informationen über Folgendes anzuzeigen:

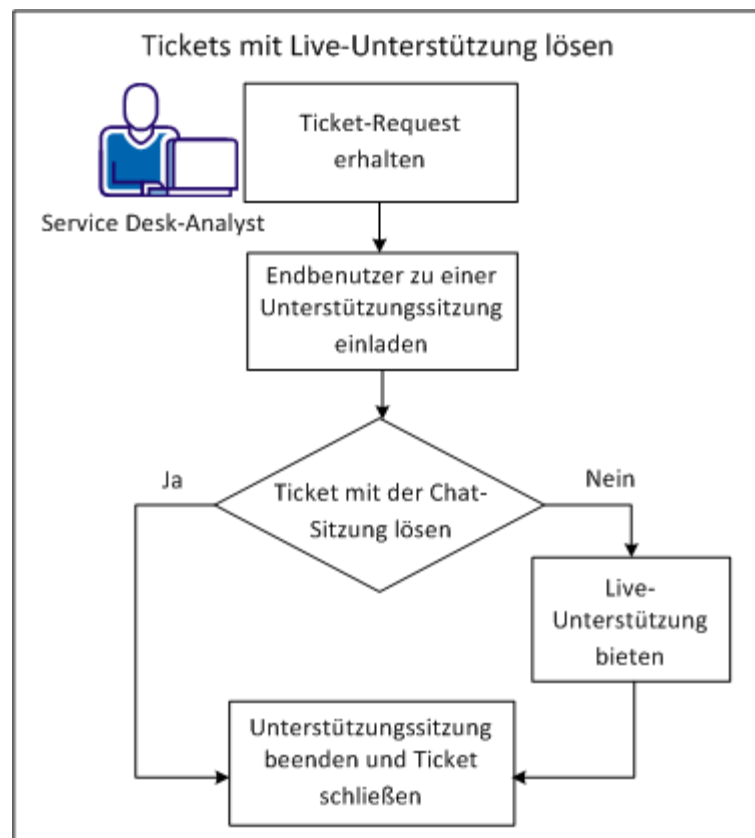
- Anmeldungsindikatoren für Analysten
- Indikatoren für Unterstützungssitzungen
- Indikatoren für Warteschlangeneinträge
- Indikatoren für die Ausführung automatisierter Aufgaben
- Verwendung von Tools pro Ticket-Kategorie
- Echtzeit-Daten über Benutzer in Warteschlangen, aktive Unterstützungssitzungen und aktive (angemeldete) Analysten.

Hinweis: Weitere Informationen über die Verwendung von BusinessObjects Infoview finden Sie unter "CA Business Intelligence" in der *Online-Hilfe*.

Tickets mit Live-Unterstützung lösen

In *Unterstützungssitzungen* können Service Desk-Analysten Endanwendern in CA SDM Live-Unterstützung bieten, um Tickets zu lösen. In einem CA SDM-Ticket sehen Sie Details zu einem Endanwender, der ein Computerproblem hat. Sie chatten mit dem Anwender und können ihn zu einer Unterstützungssitzung einladen. Verwenden Sie die Funktion zur Support-Automatisierung in CA SDM, um Tickets mit Live-Unterstützung zu lösen. Zum Beispiel erstellt der Endanwender ein Ticket zu einem Netzwerkverbindungsproblem mit einer Softwareanwendung.

Das folgende Diagramm erklärt, wie ein Service Desk-Analyst ein Ticket mit Live-Unterstützung löst:



Führen Sie diese Schritte aus, um ein CA SDM-Ticket mit Live-Unterstützung zu lösen:

1. [Ticket-Request empfangen](#) (siehe Seite 1132).
2. [Endanwender zu einer Unterstützungssitzung einladen](#) (siehe Seite 1132).
3. [Ticket in einer Chat-Sitzung lösen](#) (siehe Seite 1133) oder [Live-Unterstützung bieten](#) (siehe Seite 1134).
4. [Unterstützungssitzung beenden und Ticket schließen](#) (siehe Seite 1135).

Empfangen eines Ticket-Request

Ein Anwender sendet ein Ticket, das einen Issue mit seinem Computer beschreibt. Sie sehen die Ticketdetails in einem E-Mail-Alert oder auf dem CA SDM-Scoreboard. Zum Beispiel kann der Anwender eine Softwareanwendung, die er für die Synchronisierung mit seinem Netzwerk konfiguriert hat, nicht verwenden.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei CA SDM an, und wählen Sie "Scoreboard", "Eigene Warteschlange".
2. Öffnen Sie ein Ticket.
3. Überprüfen Sie die Ticketbeschreibung.
4. (Optional) Fügen Sie einen Kommentar zum Ticket hinzu, in dem der Anwender um weitere Informationen zur falsch konfigurierten Softwareanwendung gebeten wird.

Einladen des Endanwenders zu einer Unterstützungssitzung

Laden Sie den Anwender zu einer Unterstützungssitzung ein, um das Ticket zu lösen. Zum Beispiel benötigen Sie Informationen zu Netzwerkeinstellungen auf dem Endanwendercomputer.

Gehen Sie wie folgt vor:

1. Klicken Sie auf der Registerkarte "Support-Automatisierung" der Seite mit den Ticketdetails auf "Endanwender einladen".
2. Geben Sie eine Begrüßung für den Endanwender ein.
3. Klicken Sie auf "Starten".

Die Support-Automatisierung-Analystenoberfläche wird angezeigt. Warten Sie, dass der Anwender der Unterstützungssitzung beitrifft.

Lösen eines Tickets in einer Chat-Sitzung

Initiieren Sie eine Chat-Sitzung. Der Anwender erhält eine E-Mail-Benachrichtigung von CA SDM. Diese E-Mail enthält einen Link zur Unterstützungssitzung sowie die Ticketdetails. Die Verknüpfung öffnet den Support-Automatisierung-Endanwender-Client auf ihrem Computer. Chatten Sie mit dem Anwender, um zu entscheiden, wie Sie sein Ticket lösen können.

Hinweis: Wenn der Endanwender der Unterstützungssitzung nicht über die URL beitreten kann, bitten Sie ihn per E-Mail, auf der Self-Service-Startseite auf "Analysten jetzt kontaktieren" zu klicken.

Gehen Sie wie folgt vor:

1. Klicken Sie auf die Registerkarte "Chat" auf der Support-Automatisierung-Analystenoberfläche.
2. Führen Sie eine der folgenden Aktionen aus:
 - Wählen Sie eine Frage, Anweisung oder URL aus der Drop-down-Liste "Chat-Voreinstellungen" aus.
 - Geben Sie im Chat-Fenster einen Text ein, und klicken Sie auf "Senden".

Zum Beispiel fragen Sie den Endanwender nach den Netzwerkports, die sie bei der Konfiguration der Softwareanwendung angegeben haben.
 - Pushen Sie eine URL an den Endanwender.

Der Endanwender öffnet die Verknüpfung manuell in seinem Browser.

Live-Unterstützung

Verwenden Sie die Analystenschnittstelle der Support-Automatisierung, um Live-Unterstützung zu verwenden, um Aktionen auf dem Computer des Endanwenders durchzuführen. Führen Sie Aktionen wie das Ausführen von Diagnoseskripten, Durchsuchen des Dateisystems und Remote-Steuerung des Endanwenders durch. Zum Beispiel fällt im Chat mit dem Anwender die Entscheidung, dass Sie den Synchronisierungs-Issue der Softwareanwendung unter Verwendung von Live-Unterstützung lösen können.

Gehen Sie wie folgt vor:

1. Klicken Sie auf der Support-Automatisierung-Analystenoberfläche auf die Registerkarte des entsprechenden Tools, um das Ticket zu lösen:
 - **Automatisierte Aufgaben:** Wählen Sie im linken Bereich eine automatisierte Aufgabe aus, und klicken Sie auf "Ausführen". Führen Sie zum Beispiel ein Skript aus, das Netzwerkeinstellungen für die Softwareanwendung konfiguriert.
 - **Datei.Explorer:** Durchsuchen Sie das Dateisystem des Anwenders. Durchsuchen Sie zum Beispiel die Festplatte, um eine bestimmte Datei im Installationsverzeichnis der Softwareanwendung zu finden.
 - **Dateiübertragung:** Übertragen Sie eine Datei zwischen verschiedenen Computern. Übertragen Sie zum Beispiel eine Datei von Ihrem Computer, um eine beschädigte Datei im Installationsverzeichnis zu ersetzen.
 - **Remote-Registrierung:** Durchsuchen Sie die Endanwenderregistrierung, und ändern einen Registrierungseintrag. Ändern Sie zum Beispiel Registrierungswerte für die Softwareanwendung.
 - **Remote-System-Tools:** Führen Sie ein Programm auf dem Endanwendercomputer aus, oder erzwingen Sie einen Neustart des Computers. Führen Sie zum Beispiel die Konfigurationsoberfläche der Softwareanwendung aus.
 - **Remote-Steuerung.** Steuern Sie den Computer des Endanwenders per Remote-Zugriff. Übernehmen Sie beispielsweise die Steuerung des Endanwendercomputers, um die Softwareanwendung zu konfigurieren.
 - **Screenshots:** Erstellen Sie einen Screenshot des Endanwendercomputers. Wenn z. B. die Remote-Steuerung aufgrund von Verbindungsproblemen nicht erfolgreich ausgeführt werden kann, können Sie sich über Screenshots ein Bild machen, um den Anwender anzuleiten.
2. Wählen Sie "Remote-Steuerung" aus, und konfigurieren Sie die Softwareanwendung so, dass sie mit dem Unternehmensnetzwerk synchronisiert ist.
3. Stellen Sie gemeinsam mit dem Anwender sicher, dass die Softwareanwendung erfolgreich synchronisiert wurde und das Ticket gelöst ist.

Beenden der Unterstützungssitzung und Schließen des Tickets

Nachdem Sie sichergestellt haben, dass das Ticket gelöst ist, aktualisieren Sie das Ticket und schließen Sie die Unterstützungssitzung.

Gehen Sie wie folgt vor:

1. Klicken Sie auf der Support-Automatisierung-Analystenoberfläche auf "Ende", um die Sitzung zu schließen.

Der Anwender bekommt eine E-Mail-Benachrichtigung mit dem Sitzungsprotokoll.

2. (Optional) Klicken Sie auf "Sitzungsprotokoll", um Chat-Protokolle und Ergebnisse von Support-Automatisierung-Tools anzuzeigen.

3. Klicken Sie auf die Ticketnummer auf der Support-Automatisierung-Analystenoberfläche. Klicken Sie zum Beispiel auf Incident 40.

Die Detailseite zu Incident 40 wird in CA SDM geöffnet.

4. Klicken Sie auf "Bearbeiten".
5. Ändern Sie den Ticketstatus in "SA-Gelöst".
6. Klicken Sie auf "Speichern" und "Schließen".

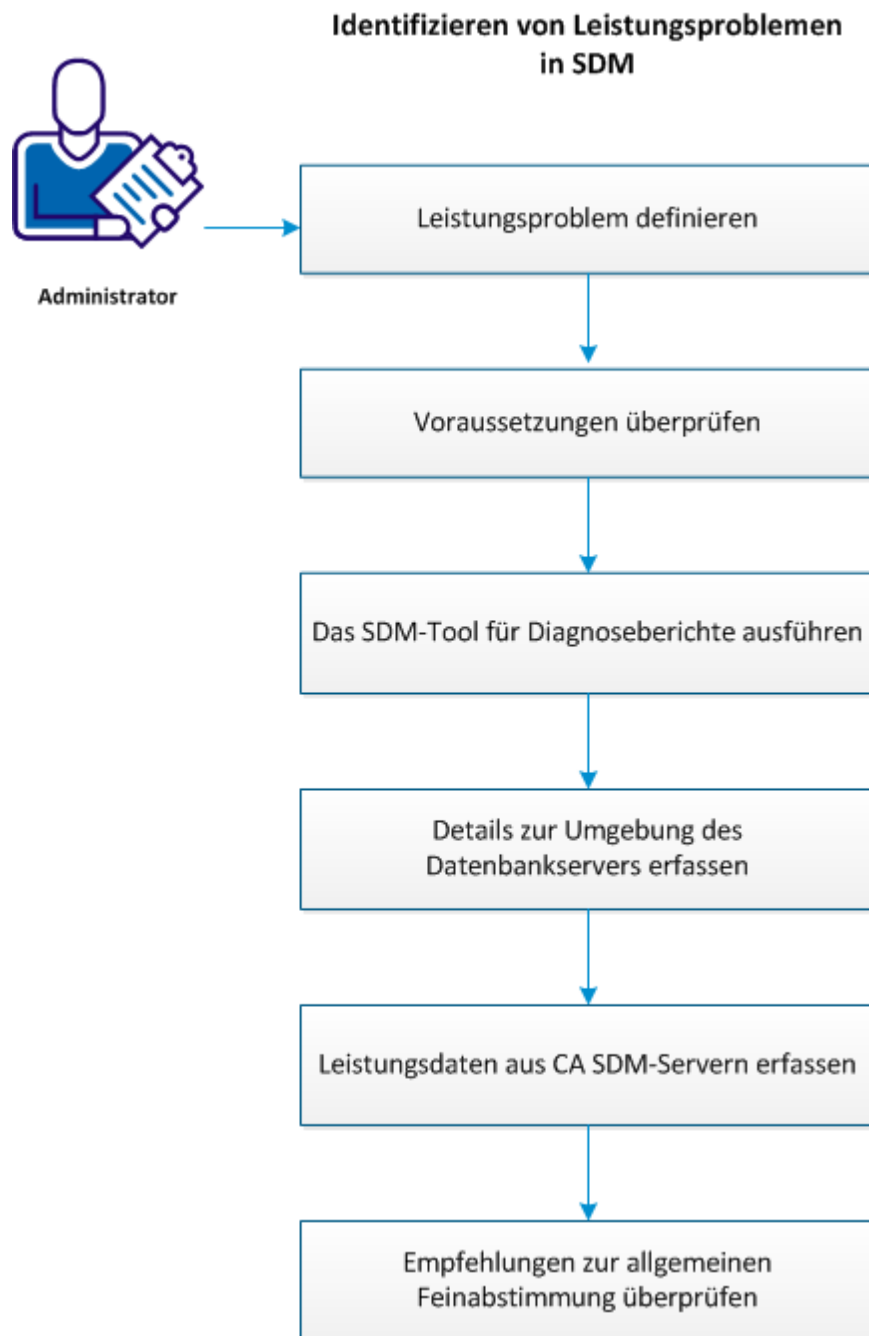
Das Aktivitätsprotokoll für das Ticket wird gespeichert, und der Prozess der Live-Unterstützung ist abgeschlossen.

Kapitel 25: So identifizieren Sie Leistungsprobleme in CA SDM

Als Systemadministrator sammeln Sie Informationen zu Ihrer Installationsumgebung, Ressourcenverwendung, Konfigurationsdetails und andere verfügbare Systemressourcen. Analysieren Sie zum Beispiel die Computerkonfiguration, um den Betriebssystemtyp, die Version und verfügbare Systemressourcen zu identifizieren. Diese Daten helfen Ihnen dabei, Issues in CA SDM, die mit der Leistung oder mit dem Arbeitsspeicher in Verbindung stehen, zu identifizieren und zu diagnostizieren. Verwenden Sie das Tool für Diagnoseberichte und das Hilfsprogramm für Intervallprotokollierung von CA, um Diagnoseinformationen zu Ihrer CA SDM-Umgebung zu erfassen.

Folgendes Diagramm beschreibt, wie Sie Diagnoseinformationen erfassen und Leistungsprobleme in CA SDM identifizieren können:

Equation 2: Identifizieren der Leistungsprobleme auf CA SDM-Servern



Gehen Sie folgendermaßen vor:

1. [Definieren Sie das Leistungsproblem](#) (siehe Seite 1138).
2. Überprüfen der Voraussetzungen
3. Führen Sie [das CA SDM-Tool für Diagnoseberichte aus](#) (siehe Seite 1140).
 - Überprüfen Sie die Windows-Berichte
 - Überprüfen Sie die UNIX-Berichte
 - Überprüfen Sie die gesammelten Diagnoseberichte
4. [Erfassen Sie Details zur Umgebung des Datenbankservers](#) (siehe Seite 1145).
5. Erfassen Sie Leistungsdaten von CA SDM-Servern
6. Lesen Sie [die allgemeinen Optimierungsempfehlungen](#) (siehe Seite 1150).

Definieren des Leistungsproblems

Sie können Ihr Leistungsproblem definieren, indem Sie zunächst Systeminformationen erfassen. Verwenden Sie folgende Liste mit Beispielfragen, und entscheiden Sie, ob sie für Ihren Issue relevant sind:

- Wie genau wurde die Anwendung für Anwender unterbrochen?
- Wann haben Anwender das Problem erstmals entdeckt?
- Wurde Ihre Umgebung sich vor Kurzem geändert, beispielsweise durch Hardware-Upgrades?
- Welche Funktionalität des Produkts ist von Issues betroffen?
- Auf wie viele und welche Typen von Anwendern hat der Issue Auswirkungen?
- Auf welche Anwender hat er keine Auswirkungen?
- Was ist der geografische Standort der Anwender, die das Problem haben?
- Was ist die Zugriffsebene der betroffenen Anwender?
- Hosten Sie CA SDM auf einem VMware ESX-Server oder einer anderen virtualisierten Umgebung?
- Welche andere Software wird auf dem ESX-Server bzw. Hostrechner ausgeführt?
- Was sind die Spezifikationen dieser Umgebung?
- Wie viele CPUs haben Sie auf den einzelnen Computern?
- Wie viel Speicherplatz ist für die einzelnen Computer konfiguriert?

Überprüfen der Voraussetzungen

1. Installieren Sie unter Windows das Tool "pslist.exe", und fügen Sie die zugehörige Verzeichnispfadvariable auf allen CA SDM-Servern hinzu.
2. Installieren und konfigurieren Sie den CA SDM-Server, bevor Sie das Diagnose-Tool ausführen.

Hinweis: Wir empfehlen, dass Sie sich mit CA Support Online in Verbindung setzen, bevor Sie das Diagnose-Tool verwenden.

Installieren der Ps-Tools für Windows

Installieren Sie unter Windows das Tool "pslist.exe", und fügen Sie die zugehörige Verzeichnispfadvariable der Systempfadvariablen hinzu.

Gehen Sie folgendermaßen vor:

1. Laden Sie die PsTools-Suite von Microsoft herunter.
2. Extrahieren Sie pstools.zip in ein Verzeichnis Ihrer Wahl und fügen Sie das Verzeichnis zur Umgebungsvariablen Windows-%PATH% hinzu.
3. Führen Sie pslist.exe einmal manuell über die Eingabeaufforderung als Anwender des lokalen Systems aus und akzeptieren Sie die Lizenzvereinbarung. Um pslist.exe als Anwender des lokalen Systems auszuführen, führen Sie folgenden Befehl aus:
`psexec.exe -s -i pslist.exe`

Hinweis: Sie können den CA SDM-Windows-Dienst unter einem anderen Anwenderkonto als dem lokalen Systemkonto starten. Führen Sie für diesen Dienst pslist.exe unter diesem Konto aus und akzeptieren Sie die Lizenzvereinbarung. Wenn pslist.exe hinzugefügt wird, nachdem CA SDM installiert und konfiguriert wurde, starten Sie die CA SDM-Dienste neu, nachdem Sie die Lizenzvereinbarung von pslist akzeptiert haben.

Erfassen der Informationen über das CA-Tool für Diagnoseberichte

Der CA SDM-Installationsdatenträger enthält das Tool für Diagnoseberichte, um Informationen zu erfassen, die bei der Diagnose von Leistungsproblemen hilfreich sind. Sie können das Diagnoseprogramm verwenden, um Informationen unter Berücksichtigung des Betriebssystemtyps zu erfassen, und zu entscheiden, welche Befehle Sie für die Datenerfassung von der CA SDM-Installation verwenden.

Konfigurieren Sie den CA SDM-Server, bevor Sie das Diagnose-Tool ausführen.

Gehen Sie folgendermaßen vor:

Windows

1. Legen Sie `$NX_ROOT` als Ihr Stammverzeichnis für die CA SDM-Installation fest.
Der Standard für `$NX_ROOT` ist das `C:\Programme\CA\Service Desk\` unter Windows. Wenn gewünscht, können Sie den Standard während des Installationsprozesses ändern.
2. Stellen Sie sicher, dass die Systempfadvariable "`$NX_ROOT\bin`" enthält.

UNIX/Linux

1. Legen Sie `$NX_ROOT` als Ihr Stammverzeichnis für die CA SDM-Installation fest.
Der Standard für `$NX_ROOT` ist — `/opt/CAisd/` auf UNIX- und Linux-Betriebssystemen. Wenn gewünscht, können Sie den Standard während des Installationsprozesses ändern.
2. Stellen Sie sicher, dass Ihr "`$PATH`" "`$NX_ROOT/bin`" enthält.

Ausführen des CA-Tools für Diagnoseberichte

Das CA-Tool erstellt unter Windows eine ".CAZ"-Datei bzw. unter UNIX eine ".tar.gz"-Datei im Verzeichnis "`$NX_ROOT\diag\rpt`", in der Sie Ihren Issue zu <http://support.ca.com> hochladen.

Gehen Sie folgendermaßen vor:

1. Führen Sie unter Windows `supp_diag.cmd` und unter UNIX `supp_diag.sh` aus.
Die Ausführung des Diagnose-Tools kann fünf bis zehn Minuten in Anspruch nehmen.

2. Wenn der Datenerfassungsprozess nicht abschließt, lesen Sie die Protokolldatei `$NX_ROOT\diag\<Hostname>_supp_diag.log`, um die Fehler zu identifizieren, die bei der Erfassung der Diagnoseinformationen aufgetreten sind.

Hinweis: Wenn Sie den im Hintergrund ausgeführten Batch-Job abbrechen möchten, verwenden Sie STRG-C, um die Batch-Datei abzubrechen. Bestimmte Prozesse wie MSINFO32.exe werden weiterhin im Hintergrund ausgeführt. Wenn Sie Fragen zur Verwendung des Diagnose-Tools haben, setzen Sie sich mit CA Support Online in Verbindung.

3. Die Skriptverzeichnisstruktur zeigt den Speicherort der Skriptdateien, Diagnose-ZIP-Dateien und Protokolldateien an:
 - Das Verzeichnis `$NX_ROOT\diag\bin` enthält Skriptdateien.
 - Das Verzeichnis `$NX_ROOT\diag\rpt` enthält die Diagnose-ZIP-Datei (in Windows-Systemen im Format `.caz` und in UNIX-Systemen im Format `.tar.gz`).
 - Das Verzeichnis `$NX_ROOT\diag\misc_logs` enthält die Protokolldateien, die automatisch in die ZIP-Datei aufgenommen werden können.
4. Führen Sie die entsprechenden Schritte aus, um die basierend auf Ihrem Betriebssystem erfassten Dateien zu öffnen:

Windows

- Öffnen Sie eine Eingabeaufforderung.
- Navigieren Sie per `cd` zu `$NX_ROOT\diag\rpt` bzw. einem Verzeichnis, in dem sich die `.CAZ`-Datei befindet.
- Führen Sie den folgenden Befehl aus.

```
$NX_ROOT\diag\bin\cazipxp -u <Paketname>.CAZ
```

UNIX

- Öffnen Sie eine Eingabeaufforderung.
- Navigieren Sie per `cd` zu `$NX_ROOT/diag/rpt` bzw. einem Verzeichnis, in dem sich die `.TAR`- oder `-TAR-GZ`-Datei befindet.
- Dekomprimieren und entpacken Sie die Datei:

```
gunzip -d <Paketname>.tar.gz  
tar -xvf <Paketname>.tar
```

Überprüfen der Windows-Berichte

Die folgende Liste beschreibt die Windows-Berichtsdateien, die erstellt und ins CAZ\tar-Dateipaket eingeschlossen werden.

Ca.olf

Enthält die CA-Lizenzierungsinformation aus dem Verzeichnis ca_lic.

Lic98.log

Gibt die Protokolldatei mit Bezug zur CA-Lizenzierung im Verzeichnis ca_lic an.

Lic98version.log

Gibt die Protokolldatei mit Bezug zur CA-Lizenzierung im Verzeichnis ca_lic an.

Licdebug.log log

Gibt die Datei mit Bezug zur CA-Lizenzierung im Verzeichnis ca_lic an.

Drwatsoninfo.txt

Gibt die Dr. Watson-Konfiguration des Computers an.

<Hostname>_env.txt

Gibt die Umgebungsvariablen an, die auf dem Computer festgelegt sind.

<Hostname>_slstat.txt

Gibt die Ausgabe des slstat-Befehls an.

<Hostname>_pdm_status.txt

Gibt die Ausgabe des slstat-Befehls an.

<Hostname>_dir_listing.txt

Listet die Service Desk-Installationsverzeichnisse auf.

<Hostname>_pslist.txt

Listet die Prozesse bei installiertem pslist-Microsoft-Tool auf.

<Hostname>_MSINFO32.NFO

Enthält die MSINFO-Ausgabe mit erfassten Systeminformationen.

<Hostname>_SYSTEMINFO.TXT

Enthält die Systeminformationen.

<Hostname>_appevents.csv

Enthält die Protokolle zu Anwendungs-Events, die in den letzten sieben Tagen erstellt wurden.

<Hostname>_sysevents.csv

Enthält die Protokolle zu Anwendungs-Events, die in den letzten sieben Tagen erstellt wurden.

<Hostname>_hostinfo.txt

Enthält die Computerinformationen.

<Hostname>_prodinstallinfo.txt

Enthält Informationen zur CA-Produktinstallation.

<Hostname>_caprod_registry.txt

Enthält die Registrierungsinformationen von installierten CA-Produkten.

<Hostname>_softfeatures.txt

Enthält eine Liste von Softwarefunktionen, die für Service Desk installiert sind.

<Hostname>_ipconfig.txt

Enthält die IP-Konfigurationsinformationen an.

<Hostname>_supp_diag.log

Gibt das Protokoll an, das für die Ausführung des supp_diag-Tools erstellt wurde.

Überprüfen der UNIX-Berichte

Die folgende Liste beschreibt die UNIX-Berichtsdateien, die erstellt und in die CAZ\tar-Datei eingeschlossen werden.

Ca.olf

Enthält die CA-Lizenzierungsinformation aus dem Verzeichnis ca_lic.

Lic98.log

Gibt die Protokolldatei mit Bezug zur CA-Lizenzierung im Verzeichnis "ca_lic" an.

<Hostname>_env.txt

Gibt die Umgebungsvariablen an, die auf dem Computer festgelegt sind.

<Hostname>_slstat.txt

Gibt die Ausgabe des slstat-Befehls an.

<Hostname>_pdm_status.txt

Gibt die Ausgabe des slstat-Befehls an.

<Hostname>_dir_listing.txt

Listet die Service Desk-Installationsverzeichnisse auf.

<Hostname>_pslist.txt

Listet die Prozesse bei installiertem pslist-Microsoft-Tool auf.

<Hostname>_uname.txt

Enthält die Ausgabe des Betriebssystembefehls "uname".

<Hostname>_diskinfo.txt

Enthält die Ausgabe des Betriebssystembefehls "df".

<Hostname>_freemem.txt

Enthält die Ausgabe von Speicherinformationen.

<Hostname>_supp_diag.log

Gibt das Protokoll an, das für die Ausführung des supp_diag-Tools erstellt wurde.

<Hostname>_prtconf.txt

Gibt die Ausgabe des Betriebssystembefehls "prtconf" für Solaris- und AIX-Computer an.

<Hostname>_solrev.txt

Enthält die BS-Version und Informationen zu Patches für Solaris-Computer an.

<Hostname>_netconf.txt

Enthält die IP-Konfigurationsinformationen für AIX-Computer.

Überprüfen der gesammelten Diagnoseberichte

Die Liste der CA SDM-Dokumentationsdateien und -Verzeichnissen schließt die folgenden Berichte aus der CAZ\tar-Datei. Fügen Sie zusätzliche Dateien oder Verzeichnisse hinzu, die Sie in die "CAZ\tar"-Datei aufnehmen können, indem Sie sie in das Verzeichnis "\$NX_ROOT\diag\misc_logs" einfügen.

- \$NX_ROOT/GENLEVEL oder \$NX_ROOT/.GENLEVEL
- \$NX_ROOT/<COMPUTERNAME>.his
- \$NX_ROOT/NX.env
- \$NX_ROOT/NX.env.last
- \$NX_ROOT/log\
- \$NX_ROOT/pdmconf\
- \$NX_ROOT/pdmconf\version
- \$NX_ROOT/bopcfg\www*.cfg
- \$NX_ROOT/site\mods\
- \$NX_ROOT/site\ddict.sch
- \$NX_ROOT/site\eh\
- \$NX_ROOT/bopcfg\www\CATALINA_BASE\logs\
- \$NX_ROOT/bopcfg\www\CATALINA_BASE\webapps\CAisd\WEB-INF\web.xml
- \$NX_ROOT/bopcfg\www\CATALINA_BASE\webapps*.xml

Erfassen von Details zur Umgebung des Datenbankservers

Sie können Details über Ihren Datenbankserver erfassen, um Leistungsprobleme in CA SDM zu identifizieren.

Gehen Sie wie folgt vor:

1. Bestimmen Sie den Speicherort Ihres Datenbankservers, wie lokal oder Remote.
2. Bestimmen Sie DBMS-Version, Betriebssystemversion und Patch-Ebene.
3. Führen Sie die entsprechenden Schritte für Ihren Datenbanktyp aus:
 - Führen Sie die folgenden Abfragen für SQL Server aus, und notieren Sie die Ergebnisse:

```
select @@version  
SELECT SERVERPROPERTY('productversion'), SERVERPROPERTY ('productlevel')
```
 - Führen Sie die folgende Abfrage für Oracle aus:

```
select * from v$version where banner like 'Oracle%';
```
4. Stellen Sie die Version des Datenbank-Client, den Sie auf dem Anwendungsserver installiert haben, fest.
5. Wenn verfügbar, erfassen Sie Zusatzinformationen zu Umgebungsdaten, wie z. B. das Betriebssystem und andere Datenbanken.
6. Erfassen Sie die Netzwerktopologie und Topologieinformationen bzw. andere Produkte, die Sie mit CA SDM integrieren.

Durchsuchen Sie zum Beispiel verfügbare PDF-Dateien oder Diagrammen nach Informationen zu den Produkten.

Erfassen Sie Leistungsdaten von CA SDM-Servern

Sie können Ressourcennutzungsdaten auf den verschiedenen CA SDM-Servern in einer mehrfachen Serverkonfiguration erfassen, um die Probleme zu ermitteln, die auf jedem Server aufgetreten sind. Die erfassten Datensätze werden verwendet, um Issues auf CA SDM-Servern, die mit der Leistung oder mit dem Arbeitsspeicher in Verbindung stehen, zu analysieren und zu beheben. Das Skript für Intervallprotokollierung ermöglicht es Ihnen, die diagnostische Datenerfassung mithilfe der CA SDM-Weboberfläche zu starten oder anzuhalten. Sie können den erfassten Datensatz mit "CA Support Online" freigeben, um die CA SDM-Serverprobleme zu identifizieren und zu lösen.

Das Hilfsprogramm für die Intervallprotokollierung wird auf dem Daemon "pdm_intrvlog_nxd" ausgeführt, der Protokolldaten von einem Server erfasst. Der Daemon wird automatisch gestartet, wenn ein Service Desk-Server startet.

- Um den Daemon für die Intervallprotokollierung manuell anzuhalten, entfernen Sie den Eintrag des Hilfsprogramms für die Intervallprotokollierung aus "pdm_startup"
- Um den Daemon für die Intervallprotokollierung manuell zu starten, doppelklicken Sie auf die Datei "pdm_intrvlog_nxd.bat" im Ordner "\$NX_ROOT/bin"

Erfassen von Nutzungsdaten mithilfe der Intervallprotokollierung

Um die Ressourcennutzungsdaten auf den CA SDM-Servern zu erfassen, konfigurieren Sie den Server für die Intervallprotokollierung. Sie können den Datentyp auswählen, den Sie von jedem Server erfassen möchten, und Sie können auch die Protokollierungsoptionen für die Server zu einem beliebigen Zeitpunkt ändern.

Wenn Sie zum Beispiel nur die CPU-Auslastungsoption für einen bestimmten Server aktivieren, wird das Hilfsprogramm nur die CPU-Auslastungsdaten auf dem Server erfassen.

Gehen Sie folgendermaßen vor:

1. Melden Sie sich bei CA SDM an.
2. Wählen Sie auf der Registerkarte "Administration" die Optionen "Systeme", "Intervallprotokollierung" aus.

Die Konfigurationsliste der Intervallprotokollierung wird geöffnet.

3. Klicken Sie auf "Neu erstellen", um eine Intervallprotokoll-Konfiguration hinzuzufügen.

Die Seite "Neue Intervallprotokoll-Konfiguration erstellen" wird geöffnet.

4. Füllen Sie die folgenden Felder aus:

Servername

Gibt den Server an, für den Sie die Protokolldaten erfassen möchten. Verwenden Sie das Suchsymbol, um die Liste der Server anzuzeigen, die Sie für die Intervallprotokollierung konfigurieren können.

Rekurrenzintervall

Gibt das Zeitintervall an, in dem die Protokolldaten für den Server erfasst werden. Wenn das Wiederholungsintervall zum Beispiel auf 3 Minuten festgelegt ist, dann wird das Protokoll alle 3 Minuten erfasst.

Standard: 3 Minuten

Minimum: 2 Minuten

Aktiviert

Zeigt an, ob die Intervallprotokollierung für den Server aktiviert oder deaktiviert ist. Bei Aktivierung wird das Intervallprotokoll für den Server erfasst.

Hinweis: Um die Intervallprotokollierung vor dem geplanten Enddatum anzuhalten, ändern Sie den Status "Aktiviert" auf "NEIN".

Datensatzstatus

Zeigt an, ob die Intervallprotokoll-Konfiguration aktiv oder inaktiv ist.

Geplantes Startdatum

Gibt das Startdatum und die Startzeit für das Erfassen der Protokolldaten an. Wenn Sie kein Startdatum eingeben, dann wird die Intervallprotokollierung bis die Konfiguration aktiv und aktiviert ist oder bis zum geplanten Enddatum sofort gestartet.

Geplantes Enddatum

Gibt das Enddatum und die Endzeit für das Erfassen der Protokolldaten an. Wenn Sie kein Enddatum eingeben, dann wird Intervallprotokollierung weiter ausgeführt, bis die Konfiguration aktiv und aktiviert ist.

5. Wählen Sie die entsprechenden Protokolloptionen aus, die Sie vom Server erfassen möchten.

Wählen Sie zum Beispiel "CPU-Verwendung" aus, wenn Sie das Protokoll für CPU-Auslastungsdaten erfassen möchten.

CPU-Nutzung

Erfasst CPU-Auslastungsstatistiken für den Server, indem "pslist -x" unter Windows oder "ps" unter Unix ausgeführt wird. Je nach Konfigurationstyp können Sie die Diagnosedaten auf folgenden Servern erfassen:

- Konventionell: Primärserver.
- Erweiterte Verfügbarkeit: Alle Server.

Speicherauslastung

Erfasst die Speicherauslastung für den Server, indem "pslist -m" unter Windows oder "ps" unter Unix ausgeführt wird. Je nach Konfigurationstyp können Sie die Diagnosedaten auf folgenden Servern erfassen:

- Konventionell: Primärserver.
- Erweiterte Verfügbarkeit: Alle Server.

Netzwerkstatus

Erfasst Informationen aller aktiven Verbindungen und Netzwerkstatistiken, indem "netstat /b" oder "/a" über das Betriebssystem ausgeführt wird. Je nach Konfigurationstyp können Sie die Diagnosedaten auf folgenden Servern erfassen:

- Konventionell: Primärserver.
- Erweiterte Verfügbarkeit: Alle Server.

Aufgabenliste

Erfasst Informationen der Anwendungen und Services für alle Aufgaben, die auf dem Server ausgeführt werden. Je nach Konfigurationstyp können Sie die Diagnosedaten auf folgenden Servern erfassen:

- Konventionell: Primärserver.
- Erweiterte Verfügbarkeit: Alle Server.

Anzahl der Websitzungen

Erfasst CA SDM-Sitzungen und Anwenderstatistiken für die Web-Engine-Prozesse, indem der Befehl "pdm_webstat" ausgeführt wird. Sie können die Daten für einen beliebigen CA SDM-Server erfassen.

Server Status

Erfasst Informationen zu allen CA SDM-Daemons oder -Prozessen auf dem Server, indem der Befehl "pdm_status" ausgeführt wird. Sie können die Daten für einen beliebigen CA SDM-Server erfassen.

DB-Bericht

Erfasst Informationen von Datenbanksatztypen, indem der Befehl "db_report" ausgeführt wird. Sie können die Daten für einen beliebigen CA SDM-Server erfassen.

Virtuelle DB - Info

Erfasst verknüpfte Informationen, die mit den Datenbank-Requests in der Warteschlange verbunden sind, indem der Befehl "pdm_vdbinfo" ausgeführt wird. Sie können die Daten für einen beliebigen CA SDM-Server erfassen.

Serververbindungen auflisten

Erfasst Informationen auf aktiven Verbindungen für den Server, indem der Befehl "pdm_listconn" ausgeführt wird. Sie können die Daten für einen beliebigen CA SDM-Server erfassen.

Slump-Prozesse auflisten

Erfasst Informationen zu Slump-Verbindungen und -Prozesse, indem der Befehl "slstat" ausgeführt wird. Sie können die Daten für einen beliebigen CA SDM-Server erfassen.

6. Klicken Sie auf "Speichern".

Der Server wird für die Intervallprotokollierung konfiguriert.

7. (Optional) Wiederholen Sie die Schritte 1 - 5, um weitere Intervallprotokoll-Konfigurationen zu erstellen.
8. Navigieren Sie in das Verzeichnis "\$NX_ROOT\log", und überprüfen Sie die generierten Protokolldateien. Je nach den von Ihnen ausgewählten Optionen der Intervallprotokollierung werden folgende Ausgabedateien generiert:

- cpu_usage_hostname
- db_report_hostname
- memory_usage_hostname
- netstat_hostname
- pdm_listconn_hostname
- pdm_vdbinfo_hostname
- server_status_hostname
- session_counts_hostname

- tasklist_hostname

Wichtig! Die maximale Größe der Ausgabedatei ist standardmäßig auf 30 KB festgelegt. Sie können die Dateigröße ändern, indem Sie den Wert "@NX_LOGFILE_LIMIT" in der NX_env-Datei ändern. Wenn die generierte Ausgabedatei die maximale Größe der Datei überschreitet, dann wird eine neue Datei mit dem Suffix "1" erstellt. Dateien, die nachfolgend generiert werden, haben das Suffix der inkrementellen Zahl.

Sie können die erfassten Protokolldaten über CA Support freigeben, um Leistungsprobleme in Ihrer SDM-Installation zu identifizieren.

Lesen der allgemeinen Optimierungsempfehlungen

Als Best Practice empfehlen wir Ihnen, die Leistungsschlüsselindikatoren und den Ressourcenverbrauch regelmäßig zu überwachen. Routinemäßige durchgeführte Wartungsvorgänge können ebenfalls dabei helfen, kleine Probleme zu identifizieren, bevor sie kritisch werden.

Wenn Sie einen Issue vermuten oder wenn sich Anwender über einen Leistungsabfall beklagen, können Sie online einen Issue öffnen und die Daten der Intervallprotokollierung, des CA SDM-Tools für Diagnoseberichte, der CA SDM-Standardprotokolle sowie Informationen über das Problem an "CA Support Online" senden. Senden Sie die Informationen über jeden CA SDM-Server an den CA Support.

Die folgende Liste beschreibt Gemeinsamkeitszeichen von Leistungsproblemen:

- Lange Meldungen in den CA SDM-Standardprotokollen (stdlog.x-Dateien)
- Durchsuchen von stdlog-Dateien nach Meldungen, die Text der folgenden Art enthalten: "The following query took ##### milliseconds...".
- Warteschlangen in Datenbank-Agents in der Ausgabe von pdm_vdbinfo
- Suche nach *Requests in der Warteschlange* in der Ausgabe von pdm_vdbinfo. Sie können diesen Befehl in der BS-Eingabeaufforderung manuell ausführen. Das Skript für Intervallprotokollierung führt diesen Befehl ebenfalls aus.
- Große Anzahl von mit Web-Engines verbundenen Anwendern. Zum Beispiel mehr als 200 Anwender.

Hinweis: Führen Sie pdm_webstat aus, um die Anzahl von gleichzeitigen Anwendern pro Web-Engine anzuzeigen. Sie können diesen Befehl in der BS-Eingabeaufforderung manuell ausführen. Das Skript für Intervallprotokollierung führt diesen Befehl ebenfalls aus.

- Anwenderbeschwerden

Anhang A: Referenzbefehle

Dieser Anhang enthält ausführliche Informationen zu den Referenzbefehlen, die für CA SDM verfügbar sind.

Dieses Kapitel enthält folgende Themen:

[bop_sinfo – Systeminformationen anzeigen](#) (siehe Seite 1152)
[dbmonitor_nxd – Daemon zur Überwachung von Datenbanken](#) (siehe Seite 1153)
[pdm_backup – Exportieren der Datenbank in eine ASCII-Datei](#) (siehe Seite 1155)
[pdm_cache_refresh – Aktualisieren der Datenbank](#) (siehe Seite 1156)
[pdm_configure – Öffnen des Konfigurationsfensters](#) (siehe Seite 1158)
[pdm_d_refresh – Starten fehlgeschlagener Daemons](#) (siehe Seite 1158)
[pdm_deref – Dereferenzieren von ASCII-Daten](#) (siehe Seite 1159)
[pdm_discimp – Importieren ermittelter Assets](#) (siehe Seite 1163)
[pdm_discupd – Asset-Aktualisierung ermittelt](#) (siehe Seite 1165)
[pdm_extract – Extrahieren von Daten aus der Datenbank](#) (siehe Seite 1165)
[pdm_halt – Beenden von Daemons oder Anhalten von Diensten](#) (siehe Seite 1169)
[pdm_init – Starten von Daemons](#) (siehe Seite 1169)
[pdm_key_refresh – Aktualisieren von im Cache gespeicherten Schlüsselinformationen](#) (siehe Seite 1170)
["pdm_lexutil" – CA SDM-Lexika ändern](#) (siehe Seite 1170)
["pdm_k_reindex" – Dienstprogramm zur Knowledge-Neuindizierung](#) (siehe Seite 1172)
[pdm_listconn – Auflisten der aktiven Verbindungen](#) (siehe Seite 1176)
[pdm_load – Hinzufügen, Aktualisieren und Löschen von Datenbank-Datensätzen](#) (siehe Seite 1178)
[pdm_logfile – Ändern der Cutover-Größe von STDLog](#) (siehe Seite 1180)
[pdm_log4j_config-Hilfsprogramm: Ändern der log4j-Eigenschaftsdatei](#) (siehe Seite 1181)
[pdm_proctor_init – Starten von Proctor auf sekundären Servern](#) (siehe Seite 1186)
[pdm_replace – Ersetzen einer Datenbanktabelle](#) (siehe Seite 1186)
[pdm_rest_util: Verwalten der CA SDM-Webservices-Anwendung RESTful](#) (siehe Seite 1188)
[pdm_restore – Wiederherstellen einer Datenbank](#) (siehe Seite 1189)
[pdm_status – Anzeigen des Status von Daemons oder Prozessen](#) (siehe Seite 1191)
[pdm_task – Einstellen der Umgebungsvariablen](#) (siehe Seite 1192)
[pdm_text_cmd – Befehlszeilenschnittstelle für Text-API](#) (siehe Seite 1192)
[pdm_uconv – Konvertiert den lokalen Zeichensatz in UTF-8](#) (siehe Seite 1196)
[pdm_userload – Hinzufügen, Aktualisieren und Löschen von Datenbank-Datensätzen](#) (siehe Seite 1199)
[pdm_webstat – Zurückgeben von Webnutzungsstatistiken](#) (siehe Seite 1201)
[report – Generieren von Berichten](#) (siehe Seite 1205)
[rpt_srv – Generieren von Berichten](#) (siehe Seite 1206)
[uniconv – Starten des UNIX CA NSM-Event Converter-Daemons](#) (siehe Seite 1208)
[Dienstprogramm "pdm_mail" - Senden von E-Mail-Informationen](#) (siehe Seite 1209)
[pdm_server_control Utility--Identify Servers](#) (siehe Seite 1211)

bop_sinfo – Systeminformationen anzeigen

Das Hilfsprogramm "bop_sinfo" zeigt Information über ein einzelnes Majic-definiertes Objekt an. Sie können dieses Dienstprogramm für die im *Technischen Referenzhandbuch* genannten Objekte ausführen.

Syntax

Dieser Befehl hat das folgende Format:

```
bop_sinfo [-s server] [-p] [-l] [-d] [f] [-q] [-t] [-m] [-a] object [-h]
```

-s server

Gibt den Server an, der abgefragt werden soll.

-p

Zeigt Informationen über den Produzenten an.

-l

Zeigt die Domsetliste an.

-d

Zeigt Datenbankobjektinformation an, einschließlich des Namens und des Typs aller Attribute.

-f

Zeigt Factoryinformationen an, einschließlich "rel_attr" und "common_name".

-q

Zeigt den Schemanamen der zugeordneten Tabelle an.

-t

Zeigt Auslöser des Objekts an.

-m

Zeigt die vom Objekt benutzten Methoden an.

-a

Zeigt Attributdetails an.

Objekt

Der Name des abzufragenden Objects

-h

(Optional) Zeigt Hilfe zum Dienstprogramm an.

Beispiel: Anzeigen von Systeminformationen für das dmn-Objekt

```
bop_sinfo -d dmn
```

```
Factory dmn
```

```
Attribute
```

```
  id                INTEGER
  producer_id LOCAL STRING(20)
  persistent_id     STRING(30)
  sym               STRING(60) REQUIRED
  delete_flag SREL -> actbool.enum REQUIRED
  desc              STRING(40)
  tables            BREL <- dcon.dom_id {dom_id = ?}
  last_mod          DATE
  last_mod_by SREL -> cnt.id
  audit_useridLOCAL SREL -> cnt.id
```

dbmonitor_nxd – Daemon zur Überwachung von Datenbanken

Der Daemon zur Überwachung von Datenbanken (dbmonitor_nxd) stellt einen Mechanismus bereit, um CA SDM die Cache-Speicherung solcher Datenbanktabellen zu erlauben, die aktualisiert werden sollen, wenn Änderungen außerhalb von CA SDM gemacht werden.

Die Hauptfunktion von "dbmonitor_nxd" besteht darin, CHANGE-Benachrichtigungen für Änderungen in den angegebenen Tabellen zu generieren, die nicht durch CA SDM verursacht wurden. Dazu fragt der Daemon in periodischen Abständen die Datenbank ab, registriert, welche externen Änderungen gemacht wurden und schickt dann CHANGE-Benachrichtigungen an den bpvirtb_nxd-Server. Der bpvirtb_nxd-Server informiert alle Domsrvr-Server über die Änderung, was dazu führt, dass jeder domsrvr-Server seinen Cache an bestimmten Datenbankobjekten aktualisiert und dann alle anderen Prozesse benachrichtigt, die Änderungen in den angegebenen Tabellen abonniert haben.

Dieser Mechanismus funktioniert gut, wenn nur gelegentlich externe Änderungen in überwachten Tabellen gemacht werden. Wenn es jedoch zu externen Massenaktualisierungen kommt, wird eine Vielzahl von CHANGE-Benachrichtigungen generiert. Dies hat eine Vielzahl von Datenbankabfragen verschiedener CA SDM-Prozesse zur Folge und beeinträchtigt die Leistung von CA SDM erheblich.

Um dieser Leistungsbeeinträchtigung von CA SDM entgegenzuwirken, wurde dbmonitor_nxd für diesen Release des Produkts aktualisiert. Die Überwachung unterstützt eine Befehlszeilenschnittstelle, die es dem Anwender erlaubt, die Überwachung bestimmter Tabellen zu starten und zu stoppen.

Syntax

Dieser Befehl hat das folgende Format:

```
dbmonitor_nxd -c <command> -t <tables>
```

<command>

Geben Sie "start" oder "stop" ein.

<tables>

Gibt einen Tabellennamen oder eine CSV-Liste (Comma Separated Values) von Tabellennamen an, die mit einer oder mehreren Tabellen übereinstimmen müssen, die in der Umgebungsvariable NX_DBMONITOR_TABLES festgelegt sind.

Jede Anfrage wird an den dbmonitor_nxd-Daemon geschickt. Der Daemon führt die entsprechenden Aktionen durch und gibt eine Meldung an den Anwender zurück, die besagt, dass die Aktion erledigt wurde.

- Wenn eine Startanfrage für eine Tabelle aufgerufen wird, die bereits gestartet wurde, erfolgt keine Aktion.
- Wenn eine Beendigungsanfrage für eine Tabelle aufgerufen wird, die bereits beendet wurde, erfolgt keine Aktion.
- Wenn die Überwachung für eine Tabelle erfolgreich stoppt oder startet, wird eine Protokollmeldung in "stdlog" geschrieben.

Hinweis: Wenn die Überwachung für eine Tabelle angehalten wird, veralten alle CA SDM-Prozesse, die Daten aus diesen Tabellen in den Cache-Speicher laden. In dem Fall ist für eine Aktualisierung dieses Cache-Speichers nicht gesorgt.

Beispielsweise lädt BOPLGIN Kontaktdatensätze (aus den Tabellen "ca_contact" und "usp_contact") in den Cache-Speicher. Eine Aktualisierung dieses Cache-Speichers würde nicht erfolgen, wenn die Überwachung an der Tabelle "ca_contact" anhalten würde, während externe Aktualisierungen in die Datenbank geladen werden. Im Fall von BOPLGIN hat dies fast keine Auswirkungen, weil die wesentlichen in BOPLGIN zwischengespeicherten Kontaktattribute aus der Tabelle "usp_contact" und nicht aus der Tabelle "ca_contact" stammen.

Hinweis: Wenn die Überwachung an einer Tabelle anhält, sind Web-Anwender nicht in der Lage, Änderungen in der Tabelle zu sehen. Sie sehen dann ein Detailformular, das extern erstellt wurde während die Überwachung anhält.

pdm_backup – Exportieren der Datenbank in eine ASCII-Datei

pdm_backup hält CA SDM an und schreibt dann eine oder mehrere Tabellen von einer CA SDM-Datenbank in eine ASCII-Datei. Sie können diese Ausgabedatei als Eingabedatei für "pdm_restore" verwenden. Neben dem Inhalt der Datenbank sichert "pdm_backup" auch die Anwendungskonfigurationsdateien.

Wenn Sie betriebsumgebungsspezifische Sicherungswerkzeuge einsetzen, wird empfohlen, diese anstelle von "pdm_backup" zu verwenden. Da "pdm_backup" ein allgemeines Werkzeug ist, kann es auf einigen Betriebsumgebungskombinationen sehr langsam sein.

Hinweis: Als Teil der Verarbeitung schließt "pdm_backup" zunächst die Daemons (UNIX) oder Dienste (Windows).

Syntax

Dieser Befehl hat das folgende Format:

```
pdm_backup [-d] [-g] [-v] -f filename [ALL | table1...tableN]
```

-d

Gibt an, dass nur die Datenbankdaten gesichert werden sollen.

-g

Gibt an, dass nur Nicht-Datenbankdaten gesichert werden. Dies bedeutet, dass nur Windows-Daten (Formulare) und andere Nicht-Datenbankdaten gesichert werden.

-v

Gibt den Verbose-Modus an, der Kommentare zum Befehlsablauf zu stdout hinzufügt.

-f filename

Gibt eine Ausgabedatei an

ALL|table1...tableN

Gibt alle Dateien (ALL) oder die Tabelle(n) an, die exportiert werden. Wenn Sie mehrere Tabellen angeben, trennen Sie diese jeweils durch Leerzeichen.

- Sie können Tabellennamen in der CA SDM-Datenbankschema-Datei (ddict.sch) finden, die sich in Verzeichnis \$NX_ROOT/site (UNIX) oder *installation-directory\site* (Windows) befindet. \$NX_ROOT bzw. *installation-directory* bezieht sich auf das Verzeichnis, in dem Sie CA SDM installiert haben.
- Wenn keine Tabelle angegeben ist, wird die gesamte CA SDM-Datenbank exportiert, einschließlich Fenstergruppen und Menüregistrierungsdateien.

Einschränkungen

pdm_backup kann nicht ausgeführt werden, während CA SDM aktiv ist.

Wichtig! Bei UNIX muss der LIBPATH vor der Ausführung mehrerer CA SDM-Dienstprogramme festgelegt werden. Verwenden Sie *pdm_task*, um den LIBPATH vor der Ausführung eines Dienstprogramms festzulegen. Geben Sie zum Beispiel "pdm_task pdm_clean_attachments ..." ein.

Weitere Informationen:

[pdm_restore – Wiederherstellen einer Datenbank](#) (siehe Seite 1189)

pdm_cache_refresh – Aktualisieren der Datenbank

pdm_cache_refresh bewirkt, dass CA SDM-Daemons oder -Prozesse Daten verwenden, die mit pdm_userload oder anderen Datenbankdienstprogrammen, einschließlich CA SDM-fremden Datenbank-Tools, in die Datenbank geladen wurden.

Die meisten Daemons und ausführbaren Dateien von CA SDM unterhalten im dynamischen Speicher einen Cache mit Datenbank-Datensätzen. Dieser Cache-Speicher verbessert die Leistung, indem Zugriffe auf die Datenbank vermieden werden, wenn die erforderlichen Daten bereits verfügbar sind. Die ausführbaren Dateien von CA SDM benachrichtigen einander über Datenbankaktualisierungen, damit der Cache stets aktuell ist. Jedoch gibt es keine Benachrichtigung von Aktualisierungen durch externe Dienstprogramme, wie zum Beispiel "pdm_userload" oder Datenbank-Dienstprogramme von Drittanbietern. Wenn neue Daten von einer dieser externen Quellen in die Datenbank geladen werden, muss das Dienstprogramm "pdm_cache_refresh" verwendet werden, um die ausgeführten Module darüber zu informieren, dass ihr Cache über die Datenbank aktualisiert werden muss.

Syntax

Dieser Befehl hat das folgende Format:

```
pdm_cache_refresh [-f filename] [-t tablenamelist] [-d] [-v]
```

-f filename

Gibt eine Textdatei an, die eine Liste der Datenbanktabellen enthält, die extern geändert wurden. Die Textdatei besteht aus einer oder mehreren Zeilen, wobei jede Zeile einen oder mehrere Tabellennamen enthält, die durch Leerzeichen getrennt sind.

-t tablename

Gibt eine oder mehrere Tabellen an, die extern geändert wurden. Wenn die Liste mehr als eine Tabelle enthält, müssen die Tabellennamen durch Semikola getrennt sein, und die ganze Liste muss durch Anführungszeichen eingeschlossen sein. Die Tabellen sind im Anhang "Datenelementverzeichnis" im *Technischen Referenzhandbuch* aufgeführt.

Angenommen, Sie haben Daten für Positionen (Locations) und Standorte (Sites) mit dem Dienstprogramm eines Drittanbieters in die <USKD>-Datenbank geladen. Um CA SDM-Daemons mitzuteilen, dass sie ihren Cache für diese Tabellen aktualisieren sollen, geben Sie den folgenden Befehl aus:

```
pdm_cache_refresh -t "Location;Site"
```

-d

Sendet eine Meldung an den domsrvr, den Domänenserver von CA SDM. Der Domänenserver lädt dann alle Auswahllisten neu. Dies bewirkt, dass alle auf einem Client angezeigten Listenfenster aufleuchten.

-v

Gibt den Verbose-Modus an. Der Wert 1 ist der Kurzmodus. Mit dem Wert 2 drucken Sie die Fortschrittsmeldungen der Protokolldatei aus.

Wichtig! Bei UNIX muss der LIBPATH vor der Ausführung mehrerer CA SDM-Dienstprogramme festgelegt werden. Verwenden Sie *pdm_task*, um den LIBPATH vor der Ausführung eines Dienstprogramms festzulegen. Geben Sie zum Beispiel "pdm_task pdm_clean_attachments ..." ein.

pdm_configure – Öffnen des Konfigurationsfensters

pdm_configure öffnet ein Fenster, das das CA SDM-Konfigurationsfenster enthält. In diesem Fenster können Sie die CA SDM-Konfiguration nach der Installation von CA SDM festlegen oder die CA SDM-Konfiguration ändern, nachdem CA SDM läuft. Es folgen mögliche Gründe für die Änderung der CA SDM-Konfiguration:

- Änderung des Datenbanktyps oder -servers
- Neuladen der Standarddaten
- Ändern der Kennwörter für CA SDM-Systemkonten
- Wiederherstellen der Schemadateien zur Integration von Änderungen
- Konfigurieren Sie abhängig von Ihrer CA SDM-Konfiguration den folgenden Server neu:
 - Konventionell: Primärserver oder Sekundärserver
 - Erweiterte Verfügbarkeit: Anwendungsserver oder Hintergrundserver

Syntax

Dieser Befehl hat das folgende Format:

```
pdm_configure
```

Einschränkungen

"pdm_configure" kann auf einem beliebigen CA SDM-Server oder auf einem CA SDM-Linux-Client ausgeführt werden. Zur Ausführung von "pdm_configure" müssen Sie der privilegierte Anwender oder der Root sein.

pdm_d_refresh – Starten fehlgeschlagener Daemons

Das Befehlszeilenhilfsprogramm "pdm_d_refresh" wird hauptsächlich für Remote-Daemon-Konfigurationen verwendet. Dem Daemon-Manager wird mitgeteilt, dass versucht werden soll, Daemons zu starten, die zehn Mal nicht gestartet werden konnten und die der Daemon-Manager als "Nicht ausführbar" markiert hat. Bei der Ausführung dieses Hilfsprogramms werden alle Daemons als ausführbar gekennzeichnet, und der Neustartzähler wird zurückgesetzt. Anschließend versucht der Daemon Manager, alle angehaltenen Daemons zu starten.

Syntax

Dieser Befehl hat das folgende Format:

```
pdm_d_refresh
```

Wichtig! Bei UNIX muss der LIBPATH vor der Ausführung mehrerer CA SDM-Dienstprogramme festgelegt werden. Verwenden Sie *pdm_task*, um den LIBPATH vor der Ausführung eines Dienstprogramms festzulegen. Geben Sie zum Beispiel "pdm_task pdm_clean_attachments ..." ein.

pdm_deref – Dereferenzieren von ASCII-Daten

pdm_deref verarbeitet ASCII-formatierte Eingaben, um in einer Datenbanktabelle gefundene Daten gegen Daten auszutauschen, die in einer anderen Datenbanktabelle gefunden werden. Dieses Programm kann verwendet werden, um Dateien zu erstellen, die mit pdm_userload von einer Nicht-CA SDM-Datenbank oder Tabellenkalkulation kompatibel sind. Es kann außerdem verwendet werden, um Berichte oder Ausgabedateien für eine Nicht-CA SDM-Datenbank oder Tabellenkalkulation zu erstellen.

Wichtig! Verwenden Sie pdm_deref nicht, wenn Sie mit SQL nicht vertraut sind. Die Verzeichnisse „export“ und „import“ in \$NX_ROOT/samples (UNIX) oder installation-directory\samples (Windows) enthalten ein Standardset von specfiles, die Sie ansehen können.

Syntax

Dieser Befehl hat das folgende Format:

```
name pdm_deref -s specfile [-c|-e|-r] [-d] [-h] [-n] [-u] [-v] <filename
```

-s specfile

(Erforderlich) Gibt eine Datei an, in der definiert ist, welche Daten ausgetauscht werden und unter welchen Bedingungen der Austausch erfolgen soll.

Specfile enthält eine Liste von SQL-Befehlen im folgenden Format (beachten Sie, dass „att“ Attribut und „atts“ Attribute bedeutet) :

Deref

```
{  
input = <list of "from" atts from input file>  
output = <list of "to" atts for output file>  
rule = "SELECT <atts used to fill output atts> \  
      FROM <table name> \  
      WHERE <att from table name to match input 1> =?\ \  
      AND <att from table name to match input 2> = ? \  
      OR <att from table name to match input 3> =?"  
}
```

-c

Erstellt eine CSV-Ausgabe (durch Kommata getrennte Werte) wie zum Beispiel:

"field1","field2","field3"

Die Ausgabe-Formatoptionen „-c“, „-e“ und „-r“ sind gegeneinander austauschbar.

-e

Führt zu einer CSV-Ausgabe (comma separated value) mit eingebetteten Anführungszeichen, denen ein weiteres doppeltes Anführungszeichen vorangestellt ist. Beispiel:

"Text with a "quoted string" in it".

Die Ausgabe-Formatoptionen „-c“, „-e“ und „-r“ sind gegeneinander austauschbar.

-r

Führt bei den Formaten zu einer linksbündigen Ausgabe, wenn die Spaltenbeschriftungen nicht in der Eingabedatei enthalten sind:

"label": "value"

oder

"value"

Diese Option ist für Gebrauch mit Line-Printers vorgesehen, z. B.:

Field_Name: Wert des Feldes

Die Ausgabe-Formatoptionen „-c“, „-e“ und „-r“ sind gegeneinander austauschbar.

-d

Erstellt diagnostische Informationen

-h

Zeigt Hilfe und Anwenderinformationen an.

-n

Gibt an, dass Sie Fremdschlüssel mit dem Wert 0 nicht als NULL behandeln möchten. Dieses Argument sollte nur unter besonderen Umständen bei der Wiederherstellung einer beschädigten Datenbank verwendet werden.

-u

Führt zu einer Ausgabe ohne Überschriften.

-v [1|2]

Gibt den Verbose-Modus an. Der Wert 1 ist der Kurzmodus. Mit dem Wert 2 drucken Sie die Fortschrittmeldungen der Protokolldatei aus.

filename (Dateiname)

(Optional) Gibt die zu verarbeitende ASCII-Eingabedatei an. Wenn keine Angabe erfolgt, wird stdin verwendet.

Einschränkung: Nur gültig für UNIX.

Vor der Verwendung von `pdm_deref` unter UNIX muss die Umgebungsvariable `$NX_ROOT` auf den Pfad des CA SDM-Installationsverzeichnis eingestellt werden, und die Umgebungsvariable `PATH` muss `$NX_ROOT/bin` einschließen.

Beispiel: Verwenden von "pdm_deref", um Daten für die Eingabe vorzubereiten

Dieses Beispiel zeigt, wie Sie "pdm_deref" verwenden können, um Daten für die Eingabe vorzubereiten.

Angenommen, die Tabelle "ca_location" enthält die folgenden Daten:

```
id      location_name_name
86873FA40BA4234A8CF7A418D7C8B2DB    "Boulder NCC"
```

würde folgende Anweisung in der specfile:

```
Deref
{
input = place
output = location_uuid
rule = "SELECT id FROM ca_location WHERE location_name=?"
}
```

die folgende Eingabe ändern:

```
last_name, first_name, place
{"Potts", "Elmore", "Boulder NCC"}
```

in die folgende Ausgabe, die mit pdm_userload in die Tabelle „ca.contact“ geladen werden kann:

```
last_name, first_name, location_uuid
{"Potts", "Elmore", "86873FA40BA4234A8CF7A418D7C8B2DB"}
```

Beispiel: Verwenden von "pdm_deref", um Daten für die Ausgabe vorzubereiten

Dieses Beispiel zeigt, wie Sie "pdm_deref" verwenden können, um Daten für die Ausgabe vorzubereiten.

Angenommen, die Tabelle „ca_contact“ enthält die folgenden Daten:

```
id last_name first_name
"69499D5A2424884887E62EC9823F5E47" "Potts" "Elmore"
```

würde folgende Anweisung in der specfile:

```
Deref
{
input = primary_contact_uuid
output = firstname, lastname
rule = "SELECT first_name, last_name FROM ca_contact
WHERE id=?"
}
```

die folgende Eingabe ändern:

```
location_name, primary_contact_uuid
{"Boulder NCC", "69499D5A2424884887E62EC9823F5E47"}
```

in die folgende Ausgabe, die gedruckt oder an eine Tabellenkalkulation gesendet werden kann:

```
location_name, firstname, lastname
{"Boulder NCC", "Elmore", "Potts"}
```

Weitere Informationen:

[pdm_extract – Extrahieren von Daten aus der Datenbank](#) (siehe Seite 1165)

pdm_discimp – Importieren ermittelter Assets

Batch-Registrierung ermittelter Nicht-CA SDM-Anlagen. Dieses Dienstprogramm kann verwendet werden, um die MDB nach Anlagen zu durchsuchen, die von anderen Softwareprodukten registriert wurden und diese als CA SDM-Anlagen zu registrieren, so dass sie in CA SDM verwendet werden können.

Die Logik ist ähnlich dem Dialogfenster „Ermittelte Anlagen“, das Sie im Webformular „Anlage – Suche/Liste“ aufrufen können. Hierbei handelt es sich um einen interaktiven Prozess und einen Batch-Prozess.

Dieses Programm durchsucht mithilfe verschiedener Parameter die Tabellen „ca_logical_asset“, „ca_asset“ und „ca_logical_asset_property“ und registriert anhand der gefundenen Werte neue CA SDM-Anlagen.

Syntax

```
pdm_discimp [-l label] [-s serial number] [-t asset tag] [-n hostname] [-d dns name]
[-m mac address] [-c asset class] [-v] [-r] [-o object manager]
```

Anlagenauswahlkriterien (verwenden Sie % als Platzhalter):

l

Diese Anlagenbeschriftung vergleichen.

s

Diese Seriennummer vergleichen.

t

Dieses Anlagenetikett vergleichen.

n

Diesen Hostnamen vergleichen.

Auswahlkriterien für Anlageneigenschaften (verwenden Sie % als Platzhalter):

d

Diesen DNS-Namen vergleichen.

m

Diese MAC-Adresse vergleichen.

Weitere Optionen:

c

Anlagenklasse, die beim Registrieren neuer Anlagen zuzuweisen ist. Standardwert ist „Entdeckte Hardware“.

v

Verbose-Modus/Diagnosemodus.

o

Anlagen registrieren, andernfalls im Simulationsmodus ausführen.

h

Zeigt diese Informationen an.

o

Für die Verarbeitung zu verwendender Objektmanager (domsrvr).

Hinweis: Wenn die Verarbeitung eine leere Asset-Beschriftung als Ergebnis hat, wird der für den Hostnamen oder den DNS-Namen gefundene Wert als Asset-Beschriftung verwendet. Anlagen müssen zumindest eine Benennung und eine Anlagenklasse aufweisen, um für die Verwendung in CA SDM registriert zu werden.

Um die entsprechenden Datensätze für die Verarbeitung herauszufinden, werden aufgrund der Struktur der MDB und der CA SDM-Architektur zwei Abfragen durchgeführt. Es ist wichtig, dies zu verstehen, da dadurch die Leistung beeinflusst werden kann. Die erste Abfrage ruft Zeilen aus einer Verbindung der Tabellen „ca_logical_asset“ und „ca_asset“ ab, bei der Beschriftung, Seriennummer, Etikett und Hostname verglichen werden. Anschließend wird für jede resultierende Zeile eine Abfrage für „ca_logical_asset_property“ durchgeführt, um „dns_name“ und „mac_address“ zu vergleichen. Die Anlage aus der ersten Abfrage wird für die Registrierung ausgewählt, wenn bei der zweiten Abfrage Zeilen zurückgegeben werden.

Wichtig! Bei UNIX muss der LIBPATH vor der Ausführung mehrerer CA SDM-Dienstprogramme festgelegt werden. Verwenden Sie *pdm_task*, um den LIBPATH vor der Ausführung eines Dienstprogramms festzulegen. Geben Sie zum Beispiel "pdm_task pdm_clean_attachments ..." ein.

pdm_discupd – Asset-Aktualisierung ermittelt

Batch-Aktualisierung ermittelter Nicht-CA SDM-Assets. Verwenden Sie dieses Hilfsprogramm, um Assets zu aktualisieren, die vom Befehl "pdm_discimp" importiert wurden.

Syntax

```
pdm_discupd [-t] [-v] [-d domsrvr]
```

Wo

t

Test

v

Verbose-Modus/Diagnosemodus.

d

Für die Verarbeitung zu verwendender Objektmanager (domsrvr).

Wichtig! Bei UNIX muss der LIBPATH vor der Ausführung mehrerer CA SDM-Dienstprogramme festgelegt werden. Verwenden Sie *pdm_task*, um den LIBPATH vor der Ausführung eines Dienstprogramms festzulegen. Geben Sie zum Beispiel "pdm_task pdm_clean_attachments ..." ein.

pdm_extract – Extrahieren von Daten aus der Datenbank

Der Befehl `pdm_extract` extrahiert Daten aus den angegebenen Datenbanktabellen von CA SDM oder die gesamte CA SDM-Datenbank und gibt sie als ASCII-formatierten Text aus.

Syntax

Dieser Befehl hat das folgende Format:

```
pdm_extract [-c|-e|-r] [-d] [-h] [-u] [-v] [-C] --B] [-f formatstring| ALL | table1  
. . . TableN]
```

-c

Erstellt eine CSV-Ausgabe (durch Kommata getrennte Werte) wie zum Beispiel:

```
"field1","field2","field3"
```

Die Ausgabe-Formatoptionen „-c“, „-e“ und „-r“ sind gegeneinander austauschbar.

-e

Führt zu einer CSV-Ausgabe (comma separated value) mit eingebetteten Anführungszeichen, denen ein weiteres doppeltes Anführungszeichen vorangestellt ist. Beispiel:

"Text with a "quoted string" in it"

Die Ausgabe-Formatoptionen „-c“, „-e“ und „-r“ sind gegeneinander austauschbar.

-r

Führt bei den Formaten zu einer linksbündigen Ausgabe, wenn die Spaltenbeschriftungen nicht in der Eingabedatei enthalten sind:

"label": "value"

oder

"value"

Diese Option ist für Gebrauch mit Line-Printers vorgesehen, z. B.:

Field_Name: Wert des Feldes

Die Ausgabe-Formatoptionen „-c“, „-e“ und „-r“ sind gegeneinander austauschbar.

-d

Verwendet das Datumsformat, das in der Datei

"\$NX_ROOT/fig/english/cfg/dataent.fmt" (UNIX) oder

"Installationsverzeichnis\fig\english\cfg\dataent.fmt" (Windows) gefunden wird. Dieses können Sie bearbeiten, um es an Ihre Anforderungen anzupassen.

-h

Zeigt Hilfe und Anwenderinformationen an.

-u

Führt zu einer Ausgabe ohne Überschriften.

-v

Gibt den Verbose-Modus an, der Kommentare zum Befehlsablauf zu stdout hinzufügt.

-C

Ändert die Codierung von UTF-8 in einen anderen Zeichensatz. Die Standardausgabe ist UTF-8.

Beispiel: Um die Ausgabe nach JIS zu konvertieren, würden Sie den Befehl "-C iso-2022-jp" ausführen.

Beispiel: Um den systemeigenen Zeichensatz zu kodieren, verwenden Sie "DEFAULT" oder "NATIVE".

-B

Unterdrückt die Bytereihenfolge-Markierung, wenn die Variable NX_ADD_UTF8_BYTE_ORDER_MARK gesetzt ist.

Die Option NX_ADD_UTF8_BYTE_ORDER_MARK ist eine Signatur für eine Datei. Sie ermöglicht Editoren, die UTF-8 unterstützen, die UTF-8-Integrität der Datei zu bewahren.

Hinweis: Die Option ist nur für Nicht-ASCII-Daten erforderlich. Wenn sie nicht installiert ist, wird im Standardverhalten die Bytereihenfolge-Markierung (Byte Order Mark, BOM) ausgelassen. Ist sie dagegen installiert, setzen Sie sie auf "1" oder "Yes".

-f *formatstring*

Extrahiert bestimmte Datensätze und Felder gemäß *formatstring*, was eine Anweisung der SQL-Untermenge ist.

Verwenden Sie für ein Datum nach einem Zeitraum die folgende Syntax:

```
pdm_extract -v -f "select id, ref_num from Call_Req where open_date >= DATE '2005-02-24'" > daterange1.txt
```

Für einen Datumsbereich verwenden Sie folgende die Syntax:

```
pdm_extract -v -f "select id, ref_num from Call_Req where open_date >= DATE '2004-01-20' and open_date < DATE '2004-02-25'" > daterange2.txt
```

Hinweis: Setzen Sie Datumsangaben des Formats JJJJ-MM-TT in einfache Anführungszeichen.

Die Syntax für "DATE" lautet wie folgt:

DATE 'yyyy-mm-dd'

yyyy = Ganzzahl, die für ein Jahr steht (zwischen 1970 und 2038)

mm = Ganzzahl, die für einen Monat steht

dd = Ganzzahl, die für einen Tag steht

Beispiele:

DATE '2005-01-18'

DATE '1999-12-25'

Die Syntax für TIMESTAMP lautet:

TIMESTAMP 'yyyy-mm-dd hh.mm.ss[.nnnnn][[+|-][hh.mm]]

yyyy = Ganzzahl, die für ein Jahr steht (zwischen 1970 und 2038)

mm = Ganzzahl, die für einen Monat steht

dd = Ganzzahl, die für einen Tag steht

hh = Ganzzahl, die für die Stunde steht

mm = Ganzzahl, die für Minuten steht

ss = Ganzzahl, die für Sekunden steht

nnnn = optionale Ganzzahl, die für Bruchteile von Sekunden steht

[+|-][hh.mm] = optionaler Zeitonenabstand

Beispiele:

TIMESTAMP '1998-04-28 12:00:00,000000'

TIMESTAMP '2004-10-17 18:30:45'

TIMESTAMP '2005-03-21 12:00:12+08:00'

TIMESTAMP '1999-05-10 09:12:23,005-03:30'

Hinweis: Die Option "-d" ist nicht notwendig. Sie beeinflusst lediglich das Format der Ausgabe.

Beispiel für die Verwendung eines Befehls:

```
pdm_extract -f "select * from Call_Req where open_date > TIMESTAMP '2004-01-12 12:00:00'"
```

In diesem Beispiel werden alle Spalten aus der Tabelle „Call_Req“ extrahiert, für die open_date nach Mitternacht 1/12/2004 ist.

ALLE

Extrahiert die Ausgabe aus allen Tabellen in der Datenbank.

tabelle1. . . tabelleN

Extrahiert die Ausgabe aus den angegebenen Tabellen. Die Tabellennamen müssen durch Leerzeichen getrennt werden.

Wenn kein Format angegeben wird, ist das Standardformat eine ASCII-Datei, die mit "pdm_userload</cs> kompatibel ist.

Weitere Informationen:

[pdm_deref – Dereferenzieren von ASCII-Daten](#) (siehe Seite 1159)

[pdm_replace – Ersetzen einer Datenbanktabelle](#) (siehe Seite 1186)

[pdm_userload – Hinzufügen, Aktualisieren und Löschen von Datenbank-Datensätzen](#) (siehe Seite 1199)

[rpt_srv – Generieren von Berichten](#) (siehe Seite 1206)

pdm_halt – Beenden von Daemons oder Anhalten von Diensten

pdm_halt beendet alle CA SDM-Daemons (UNIX) oder den Systemserverdienst (Windows) ordnungsgemäß auf dem System, auf dem pdm_halt ausgeführt wird. Das Dienstprogramm pdm_halt benötigt für seine Ausführung in der Regel ungefähr 30 Sekunden. Wenn es mehr als zwei Minuten lang hängt, drücken Sie STRG+C, um pdm_halt anzuhalten, und versuchen Sie es erneut.

Syntax

Dieser Befehl hat das folgende Format:

```
pdm_halt [-w] [-a] [time]
```

-w

Warten Sie, dass die Daemons angehalten werden.

-a

Hält alle Proctors an, die in der Datei pdm_startup-Datei definiert sind.

[time]

Gibt die Anzahl von Sekunden an, die gewartet werden soll, bis der Befehl ausgeführt wird.

Einschränkungen

pdm_halt kann auf einem CA SDM-Server (primärer oder sekundärer Server) oder auf einem CA SDM-UNIX-Client ausgeführt werden. Zur Ausführung von pdm_halt müssen Sie der privilegierte Anwender sein.

pdm_init – Starten von Daemons

Gilt nur für UNIX

pdm_init startet alle automatischen Prozesse von CA SDM auf dem System, auf dem pdm_init ausgeführt wird. Diese automatischen Prozesse werden als *Daemons* bezeichnet und laufen kontinuierlich im Hintergrund, während Sie arbeiten. Nicht alle Daemons werden gestartet; einige beziehen sich nur auf bestimmte Betriebssysteme. Weitere Informationen über eine Liste von Daemons, die man mit diesem Befehl ausführen kann finden Sie im Kapitel "Verwalten von Servern".

Hinweis: Mit dem Befehl "pdm_d_refresh" führen Sie Daemons aus, die nicht mehr ausgeführt werden können, nachdem die Daemons das Problem gelöst haben, dass ihren Start anfänglich hervorgerufen hat. In den meisten Fällen müssen Sie die laufenden Daemons nicht beenden, um diejenigen zu starten, die anfänglich nicht gestartet werden konnten.

Syntax

pdm_init

Einschränkungen

pdm_init kann auf einem CA SDM-Server (primärer oder sekundärer Server) oder auf einem CA SDM-UNIX-Client ausgeführt werden. Zur Ausführung von "pdm_init" müssen Sie der privilegierte Benutzer sein.

pdm_key_refresh – Aktualisieren von im Cache gespeicherten Schlüsselinformationen

Das Hilfsprogramm "pdm_key_refresh" aktualisiert zwischengespeicherte Schlüsselinformationen von der Tabelle "key control" in der Datenbank. Wenn Schlüsselsteuerinformationen aktualisiert werden, kann dieses Dienstprogramm ausgeführt werden, anstatt das System herunterzufahren und neu zu starten, um CA SDM zu zwingen, den neuen Basiswert für keyid zu verwenden.

Wichtig! Eine Änderung der Tabelle „key control“ kann eine Datenbeschädigung verursachen. Ändern Sie nicht die Schlüsselsteuerung ohne spezielle Anweisungen vom CA Technischen Support.

Syntax

Dieser Befehl hat das folgende Format:

pdm_key_refresh

Wichtig! Bei UNIX muss der LIBPATH vor der Ausführung mehrerer CA SDM-Dienstprogramme festgelegt werden. Verwenden Sie *pdm_task*, um den LIBPATH vor der Ausführung eines Dienstprogramms festzulegen. Geben Sie zum Beispiel "pdm_task pdm_clean_attachments ..." ein.

"pdm_lexutil" – CA SDM-Lexika ändern

Das Dienstprogramm "pdm_lexutil" erlaubt Ihnen, Service Desk-Lexika zu ändern, um dem Rechtschreibwörterbuch Wörter hinzuzufügen oder zu löschen.

Syntax

Dieser Befehl hat das folgende Format:

pdm_lexutil -a | -d [-f] [-l] wordlist

-a

Wörter hinzufügen

-d

Wörter löschen

-f

Datei oder Lexikon mit einer Liste von hinzuzufügenden oder zu löschenden Wörtern

-l

Lexikonname

Standard: userdict.tlx

Wortliste

Hinzuzufügende oder zu löschende Wörter

Wichtig! Bei UNIX muss der LIBPATH vor der Ausführung mehrerer CA SDM-Dienstprogramme festgelegt werden. Verwenden Sie *pdm_task*, um den LIBPATH vor der Ausführung eines Dienstprogramms festzulegen. Geben Sie zum Beispiel "pdm_task pdm_clean_attachments ..." ein.

"pdm_k_reindex" — Dienstprogramm zur Knowledge-Neuindizierung

Das Hilfsprogramm zur Neuindizierung von Knowledge, "pdm_k_reindex.exe", befindet sich im Installationsverzeichnis von Knowledge Management.

Hinweis: Die Neuindizierung der Dokumente in der Knowledge Base kann in Abhängigkeit von der Größe Ihrer Datenbank ein zeitaufwändiger Vorgang sein. Wir empfehlen, dass Sie das Programm zur Neuindizierung der Knowledge Base ausführen, nachdem alle Änderungen hinzugefügt worden sind. Für die Konfiguration für erweiterte Verfügbarkeit können Sie während des Failovers das Hilfsprogramm zur Neuindizierung der Knowledge nicht ausführen.

Wichtig! Unter UNIX muss "LIBPATH" festgelegt sein, bevor mehrere CA SDM-Hilfsprogramme ausgeführt werden. Verwenden Sie "pdm_task", um "LIBPATH" festzulegen, bevor Sie ein Hilfsprogramm ausführen. Geben Sie zum Beispiel "pdm_task pdm_clean_attachments ..." ein.

Gehen Sie wie folgt vor:

1. Öffnen Sie die Eingabeaufforderung.
2. Geben Sie folgenden Befehl in der Eingabeaufforderung ein, um die Neuindizierung der Knowledge auszuführen:

Beispiel:

```
pdm_k_reindex
```

Folgende Optionen sind mit diesem Befehl verfügbar.

-D

Definiert den Debug-Modus, zum Beispiel Drucken in das Befehlsfenster.

-v

Definiert den Modus "Verbose" (Ausführlich), zum Beispiel Drucken in die Datei "stdlog".

-i

Erstellt keine Tabellenindizes in der Neuindizierungstabelle, nachdem die Neuindizierung durchgeführt wurde.

Hinweis: Parameter mit einem Bindestrich als Präfix, z. B. "-D", müssen anderen Parametern, die dieses Präfix nicht haben, vorausgehen.

Die andere Option ist:

Datei:reindex.txt

Dokumente werden zur angegebenen Datei neu indiziert.

+i

Erstellt nur die Indizes der neu indizierten Tabelle (entspricht der Suchtabelle nach der Neuindizierung). Die alten Indizes werden vor der Neuindizierung entfernt.

+t

Tauscht nur die Namen der Tabellen "search" und "reindex" aus.

Hinweis: Das Präfix "+" kennzeichnet nur diesen Parameter.

sdtout

Definiert, wie häufig die Statistik im Befehlsfenster erscheint. Standardmäßig zeigt das Dienstprogramm zur Knowledge-Neuindizierung jeweils nach 1.000 verarbeiteten Dokumenten Statistiken im Befehlsfenster an. Es kann jedoch vorkommen, dass Statistiken häufiger erforderlich sind. Verwenden Sie den folgenden Parameter:

```
pdm_k_reindex -i sdtout:10
```

In diesem Fall wird im Befehlsfenster die Statistik für alle 10 Dokumente angezeigt.

Die Dokumente werden in der Knowledge Base neu indiziert.

Verwenden von pdm_k_reindex

Führen Sie das Dienstprogramm 'pdm_k_reindex' aus, wenn eine oder mehrere der folgenden Sucheinstellungen geändert wurden:

- Füllwörter
- Synonyme
- Sonderbegriffe
- Sprache
- Ähnliche Wörter entfernen
- Füllwörter entfernen
- Gültiger Zeichenbereich
- Sonderbegriffe erkennen

Wenn eine Änderung stattfindet, wird eine entsprechende Meldung im Knowledge-Knoten der Registerkarte „Administration“ angezeigt.

Verfolgen der Neuindizierung

Während der Neuindizierung können Sie den Status des Prozesses im Bereich zur Verfolgung der Neuindizierung in der unteren Hälfte der Seite beobachten. Es folgt eine Beschreibung dieser Felder:

Dokumentnr.

Dies ist die Anzahl der bereits verarbeiteten Dokumente.

Durchschnittliche Größe (Wörter)

Dies ist die Größe der aktuellen Dokumente, berechnet als Anzahl der Wörter minus der Anzahl der Füllwörter.

Geschwindigkeit (Dokumente/Sekunde)

Die Anzahl von Dokumenten, die pro Sekunde verarbeitet werden.

Zeit vom Start

Gibt die Dauer des Neuindizierungsvorgangs seit dem Start an.

Verbleibende Zeit

Dies ist die geschätzte restliche Zeit für den Prozess. Sie wird auf der Basis der aktuellen Geschwindigkeit und der verbleibenden Anzahl von Dokumenten ermittelt.

Anzahl Fehlschläge

Dies ist die Anzahl der Dokumente mit Fehlern (Höchstwert = 100). Wenn die maximale Anzahl von Fehlern erreicht ist, wird der Administrator aufgefordert, den Prozess fortzusetzen oder abubrechen.

Hinweis: Wenn Sie Änderungen an Füllwörtern, Sonderbegriffen, Synonymen oder Einstellungen durchgeführt haben, aber keine Neuindizierung durchgeführt haben, werden Sie das nächste Mal, wenn Sie auf den Knowledge-Knoten der Registerkarte "Administration" zugreifen, dazu aufgefordert. Änderungen treten erst in Kraft, wenn das Hilfsprogramm zur Neuindizierung von Knowledge ausgeführt wurde.

Importieren und Neuindizieren

Wenn "pdm_kit.exe" in der Befehlszeile aufgerufen wird, importiert das Dienstprogramm "pdm_kit" die Dokumente in die Datenbank. Nachdem die Ausführung von 'pdm_kit' abgeschlossen ist (vorausgesetzt, die Indizierung bzw. Neuindizierung der Dokumente wurde nicht über die Befehlszeilenoptionen deaktiviert), wird das Neuindizierungsdienstprogramm ('pdm_k_reindex.exe') automatisch aufgerufen. Der Status und die Ausgabe der Neuindizierungsoperation werden automatisch in EBR_REINDEX.LOG im Verzeichnis "\$NX_ROOT\log" aufgezeichnet.

Indizieren der Warteschlangeneinstellungen für Batch-Verarbeitung und sofortige Verarbeitung bzw. Entfernen der Indizierung

Das Indizieren und das Entfernen der Indizierung führt einen Batch-Vorgang aus, um eine vordefinierte Anzahl von Dokumenten auf einmal zu bearbeiten. Diese Batch-Vorgänge werden für die Leistungsoptimierung verwendet. Wenn mehr Dokumente im Batch enthalten sind, erhöht sich die Systemleistung.

Sie können nur eine begrenzte Anzahl von Dokumenten verarbeiten. Die Anzahl richtet sich nach der Größe der Dokumente und nach den mit ihnen verknüpften Anhängen. Die Dokumentgröße wird auf Grundlage des Texts (Nur-Text) und den Anhängen berechnet. Bild- und Formatierungselemente werden nicht berechnet.

Hinweis: Sie können die Größe der Anhänge beschränken, indem Sie auf der Registerkarte "Administration" zu "Anhangsbibliothek" > "Repositorys" navigieren und das Repository bearbeiten, um die "Dateigrößenbeschränkung" (KB) festzulegen.

Die empfohlene maximale Batch-Größe sollte zwischen 2-12 MB liegen (gemäß Parameter "EBR_MAX_INDEX_BATCH_SIZE" der Datei "NX.env" und durchschnittlicher Dokumentgröße).

- Wenn die durchschnittliche Größe Ihres Dokuments (einschließlich Anhänge) ca. 0,1 MB beträgt, behalten Sie die Standardeinstellung in der Datei "NX.env" bei:

```
@EBR_MAX_INDEX_BATCH_SIZE=128
@NX_EBR_INDEX_QUEUE_TIMEOUT=10
@NX_EBR_REINDEX_QUEUE_TIMEOUT=1
@NX_EBR_INDEX_QUEUE_ONLINE=Yes
@NX_EBR_NON_KD_INDEX_QUEUE_ONLINE=Yes
```

Diese Einstellung gibt an, dass in einem Batch 128 Dokumente verarbeitet werden, dass Batch-Ausführungen in Intervallen von zehn Sekunden stattfinden und dass während einer Neuindizierung das Intervall zwischen zwei Batches 1 Sekunde beträgt.

- Wenn die durchschnittliche Größe Ihres Dokuments (einschließlich Anhänge) ca. 0,5 MB beträgt, behalten Sie die Standardeinstellung in der Datei "NX.env" bei:

```
@EBR_MAX_INDEX_BATCH_SIZE=25
@NX_EBR_INDEX_QUEUE_TIMEOUT=10
@NX_EBR_REINDEX_QUEUE_TIMEOUT=10
@NX_EBR_INDEX_QUEUE_ONLINE=No
@NX_EBR_NON_KD_INDEX_QUEUE_ONLINE=No
```

Diese Einstellung gibt an, dass in einem Batch 25 Dokumente verarbeitet werden, dass Batch-Ausführungen in Intervallen von zehn Sekunden stattfinden und dass während einer Neuindizierung das Intervall zwischen zwei Batches 1 Sekunde beträgt.

pdm_listconn – Auflisten der aktiven Verbindungen

Mit dem Dienstprogramm "pdm_listconn" können Sie die aktiven Verbindungen sowohl für Clients als auch für Server auflisten.

Syntax

Dieser Befehl hat das folgende Format:

```
pdm_listconn [-c] [-s] [-s -c] [-t nn] [proc1 [proc2...]]
```

Wenn keine anderen Parameter angegeben sind, hat der Standardbefehl die folgende Syntax:

```
pdm_listconn -s -t 2
```

-c

Führt Verbindungen nach Client auf. Das Dienstprogramm zeigt zwei Zeilen für jeden Client an:

```
(n secs) client_type node|cproc
```

```
connected to alias (sproc) at time
```

n ist die Reaktionszeit des Client in Sekunden

client_type ist „vbop“, „Animator-Daemon“ oder „Web-Engine“

node ist die IP-Adresse des Client-Node

cpoc ist der Slump-Prozessname des Client

alias ist der Aliasname des Servers, mit dem der Client verbunden ist

sproc ist der Slump-Prozessname des Servers

time ist die Verbindungszeit

Beispiel:

```
(0 secs) vbop client 141.202.211.34|vbop-0x40120000:anthill:0
```

```
connected to CMD40120 on anthill (domsrvr) at 19.02.99 10:44:16
```

-s

Führt Verbindungen nach Server auf (Standardwert). Das Dienstprogramm zeigt zwei Zeilen für jeden Server an:

```
(n secs) server alias (node|sproc) willingness willingness
```

```
count connected clients (use pdm_listconn -c -s to list clients by server)
```

n ist die Reaktionszeit des Servers gemessen in Sekunden.

node ist die IP-Adresse des Server-Node

alias ist der Aliasname des Servers, mit dem der Client verbunden ist

sproc ist der Slump-Prozessname des Servers

willingness ist die Bereitswilligkeit des Servers, neue Clients (0 - 100) zu akzeptieren.

count ist die Anzahl der kontaktierten Clients.

Beispiel:

```
(0 secs) server CMD40120 on anthill (domsrvr) willingness 98
2 connected clients (use pdm_listconn -c -s to list clients by server)
  vbop client 141.202.211.34|vbop2 connected 02/19/1999 10:53:16
  vbop client 141.202.211.34|vbop-0x40120000:anthill:0 connected 02/19/1999
10:44:17
```

-s -c

Führt Verbindungen nach Server auf, einschließlich von Clientdetails für jeden Server. Das Dienstprogramm zeigt mehrere Zeilen für jeden Server an:

```
(n secs) server alias (node|sproc) willingness willingness
count connected clients:
client_type node|cproc connected time
```

wobei:

n ist die Reaktionszeit des Servers gemessen in Sekunden.

node ist die IP-Adresse des Server-Node

alias ist der Aliasname des Servers, mit dem der Client verbunden ist

sproc ist der Slump-Prozessname des Servers

willingness ist die Bereitswilligkeit des Servers, neue Clients (0 - 100) zu akzeptieren.

count ist die Anzahl der kontaktierten Clients.

client_type ist „vbop“, „Animator-Daemon“ oder „Web-Engine“

node ist die IP-Adresse des Client-Node

cproc ist der Slump-Prozessname des Client

time ist die Verbindungszeit

Beispiel:

```
(0 secs) server CMD40120 on anthill (domsrvr) willingness 98
2 connected clients:
  vbop client 141.202.211.34|vbop2 connected 02/19/1999 10:53:16
  vbop client 141.202.211.34|vbop-0x40120000:anthill:0 connected 02/19/1999
10:44:17
```

-t nn

Gibt ein Zeitüberschreitungsintervall in Sekunden an. Da mit "pdm_listconn" Informationen von einer unbekannten Anzahl von Clients und Servern angefragt werden, bricht der Prozess ab, wenn das eingestellte Zeitlimitintervall nach der letzten erhaltenen Meldung abläuft.

Standard: 2

proc1

Gibt einen oder mehrere durch Leerstellen getrennte Slump-Prozessnamen an. Das Dienstprogramm zeigt entsprechend Client- oder Serverinformationen von diesen an.

Wichtig! Bei UNIX muss der LIBPATH vor der Ausführung mehrerer CA SDM-Dienstprogramme festgelegt werden. Verwenden Sie *pdm_task*, um den LIBPATH vor der Ausführung eines Dienstprogramms festzulegen. Geben Sie zum Beispiel "pdm_task pdm_clean_attachments ..." ein.

pdm_load – Hinzufügen, Aktualisieren und Löschen von Datenbank-Datensätzen

Wichtig! Beim Ausführen von "pdm_load" kann es zu Datenverlust kommen. Erstellen Sie deshalb eine Sicherheitskopie Ihrer Datenbank bevor Sie "pdm_load" ausführen, und wenden Sie stets "pdm_userload" an, es sei denn Sie werden dazu aufgefordert, "pdm_load" auszuführen.

pdm_load aktualisiert eine CA SDM-Datenbank unter Verwendung einer von Ihnen angegebenen Eingabedatei mit maximal 112 Attributen.

Wenn Sie Tickets (wie zum Beispiel Anforderungen oder Problemanfragen) laden, sollte die Ticketnummer ein eindeutiges Präfix oder Suffix in der Zeichenfolge enthalten. CA SDM zeigt diese Zahl als Zeichenfolge und nicht als Sequenznummer an. Somit kann nicht garantiert werden, dass den hochgeladenen Tickets eine eindeutige Nummer zugewiesen wird. Solange Sie mit awk oder einem anderen Textverarbeitungsprogramm ein eindeutiges Präfix oder Suffix zuweisen, können Sie Tickets laden, ohne dass CA SDM zuvor zugewiesene Nummern überschreibt.

Syntax

Dieser Befehl hat das folgende Format:

```
pdm_load [-c] [-h] [-m] [-r] [-u] [-v] -f filename
```

Die Eingabedateieinträge befolgen dieses Format:

```
TABLE table_name
fieldname1 fieldname2 . . . fieldnameN
{ "value11", "value12", . . . "value1N" }
{ "value21", "value22", . . . "value2N" }
.
.
.
{ "valueN1", "valueN2", . . . "valueNN" }
```

"*table_name*" ist der Name der zu ladenden Tabelle, so wie in der CA SDM-Datenbankschema-Datei aufgelistet. Die Datei befindet sich in \$NX_ROOT/site/schema.sch (UNIX) oder in *installation-directory*\site\schema.sch (Windows). \$NX_ROOT bzw. *installation-directory* bezieht sich auf das Verzeichnis, in dem Sie CA SDM installiert haben.

-f *filename*

Gibt eine Eingabe-ASCII-Datei an.

-c

Überprüft die Eingabedatei gegen die Datenbank und die Berichte der durchzuführenden Aktualisierungen, führt jedoch keine Aktualisierungen durch.

-m

Gibt eine Massenaktualisierung an. Geben Sie diese Option an, wenn Sie mit "pdm_load</cs>" eine große Anzahl von Datensätzen hinzufügen oder löschen. Diese Option unterdrückt alle Clientbenachrichtigungen hinsichtlich Aktualisierungen und sendet eine Meldung zur Aktualisierung des Caches für eine Tabelle, wenn "pdm_load</cs>" die Verarbeitung der Tabelle abschließt.

-r

Entfernt Datenbank-Datensätze, die Eingabe-Datensätzen entsprechen.

Wichtig! Bevor Sie "pdm_load</cs>" mit dieser Option ausführen, erstellen Sie eine Sicherungskopie der Datenbank. Sobald alte Datenbankdatensätze entfernt worden sind, müssen Sie die CA SDM-Datenbank mit dieser Sicherungskopie wiederherstellen, wenn Sie gelöschte Datensätze wiederherstellen möchten.

-u

Aktualisiert vorhandene Datensätze, fügt jedoch keine neuen Datensätze in die Datenbank ein.

Weitere Informationen:

[pdm_replace – Ersetzen einer Datenbanktabelle](#) (siehe Seite 1186)

[pdm_userload – Hinzufügen, Aktualisieren und Löschen von Datenbank-Datensätzen](#)
(siehe Seite 1199)

[pdm_backup – Exportieren der Datenbank in eine ASCII-Datei](#) (siehe Seite 1155)

[pdm_restore – Wiederherstellen einer Datenbank](#) (siehe Seite 1189)

pdm_logfile – Ändern der Cutover-Größe von STDLog

Mit "pdm_logfile" können Sie die Cutover-Größe Ihrer Datei "STDLog.x" ändern. Der Cutover kann stattfinden, nachdem eine angegebene Anzahl von Byte geschrieben wurde. Bei UNIX wird dieser Wert bei jedem "pdm_init</cs>" zurückgesetzt. Bei Windows werden die Einstellungen bei jedem "pdm_halt</cs>" und "pdm_init</cs>" beibehalten.

Syntax

Dieser Befehl hat das folgende Format:

```
pdm_logfile [-L|-h]
```

oder

```
pdm_logfile [-g -h] [-b bytes]
```

Beispiel

Um die Cutover-Größe zu ändern und einen Cutover Ihrer Datei "STDLog.x</cs>" bei 500.000 Byte festzulegen, setzen Sie den folgenden Befehl ab:

```
pdm_logfile -f STD -b 500000
```

-L

Erstellt eine Liste der aktuellen Cutovers.

-q

Führt pdm_logfile im Ruhemodus aus.

-b bytes

Gibt die Anzahl der geschriebenen Byte an, bevor ein Cutover stattfindet.

Einschränkungen

Sie können `pdm_load` ausführen, während CA SDM aktiv ist; die Leistung kann jedoch sehr beeinträchtigt werden. Führen Sie `pdm_load` am besten aus, wenn kein Benutzer CA SDM verwendet.

Wichtig! Bei UNIX muss der `LIBPATH` vor der Ausführung mehrerer CA SDM-Dienstprogramme festgelegt werden. Verwenden Sie `pdm_task`, um den `LIBPATH` vor der Ausführung eines Dienstprogramms festzulegen. Geben Sie zum Beispiel "`pdm_task pdm_clean_attachments ...`" ein.

pdm_log4j_config-Hilfsprogramm: Ändern der log4j-Eigenschaftsdatei

Mit dem Hilfsprogramm `pdm_log4j_config.p` können Sie die log4j-Eigenschaftsdatei von CA SDM, Webkomponenten, PDM_RPC, Support-Automatisierung, REST und CMDb Visualizer konfigurieren. Führen Sie das Batch-Skript des Hilfsprogramms aus, das auf Ihrer Umgebung basiert. Führen Sie für Windows in der Befehlszeile `pdm_log4j_config` aus. Führen Sie für UNIX die Datei `pdm_log4j_config.sh` aus.

Dieser Befehl hat das folgende Format:

```
pdm_log4j_config -f <Komponente> -d
pdm_log4j_config -h
pdm_log4j_config -f <Komponente> [-a | -n <Name>] [-l <Protokollebene>] [I
<Max.Anzahl von Protokolldateien>] [-s <Max. Größe von Protokolldateien>] [-t
<Protokollebenengrenzwert>]
```

-f

Gibt die log4j-Konfiguration von CA SDM oder der CA SDM-Komponente an, die Sie ändern möchten. Geben Sie einen der folgenden Werte ein:

SDM_WEB, SDM_RPC, REST, SA oder Viz.

Hinweis: Verwenden Sie die obligatorische Option zusammen mit den anderen Optionen.

-d

Zeigt die aktuelle log4j.properties-Konfiguration an.

-h

Zeigt Hilfe zum Dienstprogramm an.

-a

Führt alle Änderungen an log4j.properties global durch.

-n

Gibt an, dass Sie nur Klassen oder Pakete mit einem spezifischen Namen ändern wollen.

Geben Sie einen Namen einer spezifischen Klassen, z. B. bop_logging, oder eines vollständigen Pakets, z. B. com.ca.ServicePlu, an

-l

Gibt die Protokollebene an, die Sie festlegen wollen.

Hinweis: Legen Sie die Option -a- oder -n-Option fest.

-i

Gibt die Obergrenze für die Anzahl von Dateien an, die Sie festlegen wollen.

Hinweis: Legen Sie die Option -a- oder -n-Option fest.

-s

Gibt die Obergrenze für die Dateigröße an, die Sie festlegen wollen.

Hinweis: Legen Sie die Option -a- oder -n-Option fest.

Wichtig! Ändern Sie den Appender in der log4j.properties-Datei von Visualizer in "Rolling File Appender" um, bevor Sie den Befehl mit diesem Parameter ausführen. Wenn Sie den Appender nicht ändern, generiert MaxFileSize Protokolle in derselben Datei.

-t

Gibt den Grenzwert für die Protokollebene an.

Hinweis: Legen Sie die Option -a- oder -n-Option fest.

Beispiele für die Verwendung des Hilfsprogramms

Die folgende Liste zeigt Beispiele für die Verwendung des Hilfsprogramms `pdm_log4j_config` an:

- Ändern Sie den in der Eigenschaftsdatei konfigurierten Ausführlichkeitsgrad des Protokolls für alle Logger mithilfe der Variablen `-l` und `-a`.

Legen Sie zum Beispiel für alle in Support-Automatisierung konfigurierten Logger auf eine DEBUG-Ebene fest:

```
pdm_log4j_config -f SA -a -l DEBUG
```

- Ändern Sie den Ausführlichkeitsgrad des Protokolls für eine spezifische Logger-Klasse oder einen spezifischen Paketnamen in der CA SDM-log4j-Eigenschaftsdatei mithilfe der Variablen `-l` und `-a`.

Legen Sie zum Beispiel den Logger für das `pdm_rpc`-Paket mithilfe eines der folgenden Codebeispiele auf DEBUG fest:

```
pdm_log4j_config -f SDM_RPC -n pdm_rpc -l DEBUG
```

```
pdm_log4j_config -f SDM_RPC -n com.ca.ServicePlus.pdm_rpc -l DEBUG
```

- Ändern Sie die Höchstanzahl von Protokolldateien, die für alle Appender erstellt werden sollen (Eigenschaft "MaxBackupIndex"), mithilfe der Variablen `-i` und `-a` in der log4j-Eigenschaftsdatei von REST.

Legen Sie zum Beispiel die Höchstanzahl von Dateien für alle Appender auf 9 fest.

```
pdm_log4j_config -f REST -a -i 9
```

- Ändern Sie die in der CA SDM-log4j-Eigenschaftsdatei konfigurierte Höchstanzahl von Protokolldateien für einen Appender für eine bestimmte Klasse oder Gruppe von Klassen (Eigenschaft "MaxBackupIndex") mithilfe der Variablen `-i` und `-n`.

Legen Sie zum Beispiel die Höchstanzahl von Dateien für alle Dateien für `bop_logging` auf 7 fest.

```
pdm_log4j_config -f SDM_WEB -n bop_logging -i 7
```

- Ändern Sie die in der REST-log4j-Eigenschaftsdatei konfigurierte maximale Größe aller Protokolldateien, die für sämtliche Appender erstellt werden (Eigenschaft "MaxFileSize") mithilfe der Variablen `-s` und `-a`.

Legen Sie zum Beispiel die maximale Größe für Dateien für alle Appender auf 9 MB fest.

```
pdm_log4j_config -f REST -a -s 9MB
```

- Ändern Sie die in der CA SDM-log4j-Eigenschaftsdatei konfigurierte maximale Größe von Protokolldateien für einen Appender für eine bestimmte Klasse oder Gruppe von Klassen (Eigenschaft "MaxFileSize") mithilfe der Variablen `-s` und `-n`.

Legen Sie zum Beispiel die maximale Größe für Dateien für `bop_logging` auf 7 MB fest.

```
pdm_log4j_config -f SDM_WEB -n bop_logging -s 7MB
```

- Ändern Sie den in der log4j-Eigenschaftsdatei für Support-Automatisierung konfigurierten Grenzwert der Protokollebene für alle Appender (Eigenschaft "Threshold") mithilfe der Variablen -t und -a.

Legen Sie zum Beispiel den Protokollebenengrenzwert auf DEBUG fest.

```
pdm_log4j_config -f SA -a -t DEBUG
```

Hinweis: Der Parameter-Protokollebenengrenzwert -t überschreibt die Parameterprotokollebene -l. Wenn Sie die Protokollebene und den Grenzwert ändern, werden die Debug-Protokolle vom Servlet nicht in der Datei angezeigt.

- Ändern Sie den in der in der CA SDM-log4j-Eigenschaftsdatei konfigurierten Protokollebenengrenzwert für einen Appender für eine bestimmte Klasse oder Gruppe von Klassen (Eigenschaft "Threshold") mithilfe der Variablen -t- und -n.

Legen Sie zum Beispiel den Protokollebenengrenzwert auf WARN fest.

```
pdm_log4j_config -f SDM_WEB -n bop_logging -t WARN
```

- Führen Sie den folgenden Befehl aus, um die aktuelle Logger- und Appender-Konfiguration der REST-log4j-Eigenschaftsdatei anzuzeigen:

```
pdm_log4j_config -f REST -d
```

Wichtig! Verwenden Sie die Variablen -l, -i, -s und -t-Variablen zusammen mit der Option -a- oder -n. Verwenden Sie nicht beide Optionen gleichzeitig. Die Option -f ist obligatorisch. Die Optionen -h- und -d sind für alle anderen Optionen gegenseitig exklusiv.

Manuelles Ändern Sie des Aktualisierungsintervalls der Protokolldatei

Administratoren können ändern, wie oft CA SDM die log4j.properties-Datei nach Änderungen durchsucht. Standardmäßig beträgt das Aktualisierungsintervall 60 Sekunden. CA SDM-Komponenten einschließlich SDM-Servlets, PDM_RPC, Support-Automatisierung, CMDDB Visualizer und REST verwenden für die Protokollierung log4j.

Gehen Sie wie folgt vor:

1. Öffnen Sie das folgende Verzeichnis auf dem CA SDM-Server:

```
NX_ROOT
```

2. Öffnen Sie die Datei "NX.env" zum Bearbeiten.
3. Ändern Sie die Variable NX_LOG4J_REFRESH_INTERVAL mit einem Wert in Millisekunden.

Hinweis: Wenn Sie einen negativen oder nicht numerischen Wert eingeben, wird der Standardwert von 60 Sekunden verwendet.

4. Speichern Sie die Datei "NX.env".

Ändern des Appenders jsrvr.log

Standardmäßig wird in Protokollen von Servlets wie PDMContextListener, pdmweb, UploadServlet und pdm_report in der Datei jsrvr.log die Protokollebene INFO verwendet. Sie können die Grenzwertebene des jsrvr.log-Appenders, so ändern, dass für alle Meldungen auf INFO-Ebene Protokolleinträge erstellt werden.

Gehen Sie wie folgt vor:

1. Ändern Sie die Ebene in der log4j.properties-Datei auf folgenden Grenzwert:
`log4j.appender.jsrvrlog.Threshold=debug`
2. Ändern Sie die Protokollebene von UploadServlet:
`log4j.logger.com.ca.ServicePlus.uploadservlet=debug, jsrvrlog`
3. Öffnen Sie die Datei jsrvr.log.
4. Stellen Sie sicher, dass die Debug-Protokollmeldungen von UploadServlet angezeigt werden.

Hinweis: Wenn Sie die Protokollebene ändern, ohne den Grenzwert zu ändern, werden die DEBUG-Protokolle vom Servlet nicht in der Datei angezeigt. Es sind nicht an alle Servlets explizite Logger angehängt. Zum Beispiel enthält die Datei log4j.properties nicht pdmweb, BOServlet, pdm_export, pdm_report und pdm_cache, die zum pdmweb-Servlets gehören. Um DEBUG-Protokolle von diesen Servlets zu sehen, ändern Sie die Protokollebene für pdmweb.

Ändern des Appenders jstd.log

Sämtliche Protokolle von Anwendungen, bei denen es sich nicht um Web-Anwendungen handelt, werden separat in der Datei jstd.log-Datei abgelegt. Sie können Protokolle für alle Anwendungen dieser Art, wie z. B. pdm_rpc, anzeigen, indem Sie die Protokollebene der spezifischen Anwendung ändern.

Gehen Sie wie folgt vor:

1. Ändern Sie die folgende Protokollebene:
`log4j.logger.com.ca.ServicePlus.pdm_rpc=debug`
2. Öffnen Sie log4j.properties und überprüfen Sie, ob die Protokolleinträge angezeigt werden.

pdm_proctor_init – Starten von Proctor auf sekundären Servern

Gilt nur für UNIX

Mit "pdm_proctor_init" starten Sie den Proctor auf sekundären Servern. Alle sekundären Server sollten vor Starten der Daemons des primären Servers gestartet werden. Nachdem alle Daemons des primären Servers angehalten wurden, verwenden Sie "pdm_halt" auf dem sekundären Server, um diesen Proctor anzuhalten.

Hinweis: Verwenden Sie "pdm_proctor_init" nicht auf dem Primärserver.

Syntax

Dieser Befehl hat das folgende Format:

```
pdm_proctor_init
```

pdm_replace – Ersetzen einer Datenbanktabelle

"pdm_replace" löscht eine Tabelle in einer CA SDM-Datenbank und ersetzt sie durch eine Tabelle aus einer temporären Datei, die Sie über die Option "-f" angeben. Die Daten aus der Eingabedatei sind die einzigen Daten, die nach Ausführen von "pdm_replace" in dieser Tabelle enthalten sind. Erstellen Sie eine Sicherungskopie Ihrer Tabelle, bevor Sie "pdm_replace" ausführen.

Hinweis: Als Teil der Verarbeitung schließt "pdm_replace" zunächst die Daemons (UNIX) oder Dienste (Windows).

"pdm_replace" akzeptiert eine Textdatei als Eingabe, die das gleiche Dateiformat hat, das von "pdm_userload" verwendet wird. Sie können mithilfe von pdm_extract eine Eingabedatei für pdm_replace erstellen, jedoch nicht die Ausgabe von pdm_backup als Eingabe für pdm_replace verwenden.

Wichtig! Geben Sie Ihrer Eingabedatei unbedingt einen anderen Namen als den Namen der Tabelle, die Sie ersetzen möchten. Ersetzen Sie beispielsweise eine Tabelle namens "ca_contacts" und nennen die Eingabedatei "ca_contacts.dat", wird die Datei nach Ausführung des Befehls "pdm_replace", der auf die Eingabedatei ("ca_contacts.dat") verweist, gelöscht, da sie den gleichen Namen wie die Tabelle hat.

Einschränkungen

- "pdm_replace" kann abhängig von Ihrer CA SDM-Konfiguration nur auf folgenden Servern ausgeführt werden:

- Konventionell: Primärserver
- Erweiterte Verfügbarkeit: Hintergrundserver

Wichtig! Stellen Sie sicher, dass Sie alle Anwendungsserver und Standby-Server angehalten haben, bevor Sie diesen Befehl auf dem Hintergrundserver ausführen.

- Nur der berechtigte Anwender oder Root können "pdm_replace" ausführen.
- Führen Sie pdm_replace nicht aus, wenn Anwender in CA SDM angemeldet sind.

Syntax

Dieser Befehl hat das folgende Format:

```
pdm_replace [-v] -f filename
```

-v

Gibt den Verbose-Modus an.

-f *filename*

Gibt eine ASCII-Datei mit dem folgenden Format an:

```
TABLE table_name
fieldname1 fieldname2 . . . fieldnameN
{ "value11", "value12", . . . "value1N" }
{ "value21", "value22", . . . "value2N" }
.
.
.
{ "valueN1", "valueN2", . . . "valueNN" }
```

Dies ist das gleiche Dateiformat, das von "pdm_userload" verwendet wird. Sie können mithilfe von pdm_extract eine Eingabedatei für pdm_replace erstellen, jedoch nicht die Ausgabe von pdm_backup als Eingabe für pdm_replace verwenden.

Weitere Informationen:

[pdm_extract – Extrahieren von Daten aus der Datenbank](#) (siehe Seite 1165)

[pdm_userload – Hinzufügen, Aktualisieren und Löschen von Datenbank-Datensätzen](#)
(siehe Seite 1199)

pdm_rest_util: Verwalten der CA SDM-Webservices-Anwendung RESTful

CA SDM verwendet dieses Hilfsprogramm automatisch. Sie können es im Bedarfsfall manuell ausführen, beispielsweise nachdem ein unerwarteter Fehler aufgetreten ist. Dieses REST-Webservices-Hilfsprogramm stellt die Webanwendung des REST-Dienstes bereit. Dieses Hilfsprogramm stellt die REST-Anwendung für die dedizierte REST-Tomcat-Instanz bereit. Die können das Hilfsprogramm mit einer Batch-Datei im Verzeichnis NX_ROOT\bin (pdm_rest_util.bat für Windows oder ./pdm_rest_util.sh für UNIX) aufrufen.

Dieser Befehl hat die folgenden Formate Optionen:

```
pdm_rest_util -h | [-deploy] | [-undeploy]
```

-h

Gibt die Befehlszeilenhilfe aus.

-deploy

Generiert und kompiliert alle Majic-Factorys und stellt sie bereit.

-undeploy

Hebt die Bereitstellung von REST-Webservices auf dem lokalen Server auf.

Aufheben der Bereitstellung der REST-Webservices-Anwendung

Sie können die Bereitstellung der REST-Webservices-Anwendung mit dem Hilfsprogramm `pdm_rest_util`-Utility aufheben. Zum Beispiel möchten Sie Wartungsaufgaben für CA SDM durchführen und die Bereitstellung von REST währenddessen aufheben.

Gehen Sie wie folgt vor:

1. Öffnen Sie eine Eingabeaufforderung.
2. Führen Sie folgenden Befehl aus:

```
pdm_rest_util -undeploy
```

Die Bereitstellung der REST-Webservices-Anwendung wird aufgehoben.

Wichtig! Wenn Sie die Bereitstellung der REST-Webservices-Anwendung mit diesem Hilfsprogramm aufheben, kann REST automatisch erneut bereitgestellt werden, wenn CA SDM neu startet. Wir empfehlen, dass Sie die CA SDM-Konfiguration verwenden, um REST unbeschränkt zu deaktivieren.

pdm_restore – Wiederherstellen einer Datenbank

`pdm_restore` hält CA SDM an, löscht alle Datensätze aus einer CA SDM-Datenbank und ersetzt sie dann durch Datensätze aus einer Datei, die Sie über die Option "-f" angeben. Die Daten aus der Eingabedatei sind die einzigen Daten, die nach Ausführung von `pdm_restore` in der CA SDM-Datenbank enthalten sind.

Die Eingabedatei muss mit "`pdm_extract`" oder "`pdm_backup`" erstellt worden oder andernfalls speziell für "`pdm_restore`" formatiert sein. "`pdm_backup`" kann eine Sicherungskopie von Nichtdatenbankdaten erstellen, und "`pdm_restore`" kann diese Daten auch wiederherstellen. "`pdm_backup`" und "`pdm_restore`" werden nicht empfohlen, wenn andere Werkzeuge zur Sicherung und Wiederherstellung zur Verfügung stehen.

Hinweis: Als Teil der Verarbeitung schließt "`pdm_restore`" zunächst die Daemons (UNIX) oder Dienste (Windows).

Syntax

Dieser Befehl hat das folgende Format:

```
pdm_restore [-d] [-g] [-n] [-w] [-v] -f filename
```

Einschränkungen

pdm_restore kann nur auf einem CA SDM-Server ausgeführt werden. Nur der berechtigte Anwender oder Root können "pdm_restore" ausführen. Folgende Einschränkungen sind anwendbar, wenn Sie die Konfiguration für erweiterte Verfügbarkeit verwenden:

- Wenn Sie die Datenbank wiederherstellen, führen Sie den Befehl "pdm_restore" nur auf dem Hintergrundserver aus.
- Stellen Sie sicher, dass Sie alle Server (Anwendungsserver, Hintergrundserver und Standby-Server) angehalten haben, bevor Sie den Befehl "pdm_restore" ausführen.

Wichtig! Verwenden Sie "pdm_restore" nur in Verbindung mit einer vollständigen Datenbanksicherung, die von "pdm_backup" erstellt wurde, da Ihre aktuelle Datenbank gelöscht und durch den Inhalt der Sicherungsdatei ersetzt wird. Führen Sie pdm_restore nicht aus, wenn Anwender in CA SDM angemeldet sind.

-d

Gibt an, dass nur Datenbankdaten wiederhergestellt werden.

-g

Gibt an, dass nur Nicht-Datenbankdaten wiederhergestellt werden. Nur Windows-(Formulare) und andere Nichtdatenbankdaten werden wiederhergestellt.

-n

Gibt an, dass "NX.env" ebenfalls wiederhergestellt werden soll, wenn Nicht-Datenbankdaten wiederhergestellt werden. Standardmäßig wird "NX.env" nicht wiederhergestellt. Es wird empfohlen, die Datei "NX.env" nicht wiederherzustellen, es sei denn, die Wiederherstellung erfolgt auf dem gleichen Server, von dem die Sicherung stammt. Die Wiederherstellung einer falschen "NX.env" kann unbeabsichtigte Auswirkungen auf die Datenbanken haben.

-w

Gibt an, dass "web.cfg" ebenfalls wiederhergestellt werden soll, wenn Nicht-Datenbankdaten wiederhergestellt werden. Standardmäßig wird "web.cfg" nicht wiederhergestellt.

-v

Gibt den Verbose-Modus an.

-f filename

Gibt eine Eingabedatei an, die eine vollständige Sicherung enthält, die von "pdm_backup</cs> erstellt wurde.

Wichtig! Bei UNIX muss der LIBPATH vor der Ausführung mehrerer CA SDM-Dienstprogramme festgelegt werden. Verwenden Sie *pdm_task*, um den LIBPATH vor der Ausführung eines Dienstprogramms festzulegen. Geben Sie zum Beispiel "pdm_task pdm_clean_attachments ..." ein.

Weitere Informationen:

[pdm_userload – Hinzufügen, Aktualisieren und Löschen von Datenbank-Datensätzen](#)

(siehe Seite 1199)

[pdm_backup – Exportieren der Datenbank in eine ASCII-Datei](#) (siehe Seite 1155)

[Datenbankwiederherstellung](#) (siehe Seite 543)

pdm_status – Anzeigen des Status von Daemons oder Prozessen

pdm_status zeigt den Status aller Daemons (UNIX) oder Prozesse (Windows) von CA SDM auf dem System an, auf dem der Befehl ausgeführt wird.

Die Ausgabe wird in folgendem Format angezeigt:

DAEMON		STATUS	HOST	PID	SLUMP	CONNECT	TIME
Agent anthill		Running	anthill	455	Tue Feb 17	17:55:12	
Ddict_rd	(ddictrd)	Completed	anthill				
Data Dictionary	(ddictbuild)	Completed	anthill				
...							
User Validation	(boplgln)	Running	anthill	456	Tue Feb 17	17:55:21	

Syntax

Dieser Befehl hat das folgende Format:

pdm_status

pdm_task – Einstellen der Umgebungsvariablen

Gilt nur für UNIX

Das Dienstprogramm "pdm_task" legt Umgebungsvariablen für Befehle fest, die über keinen Wrapper verfügen. Zum Beispiel muss der Befehl „pdm_task“ dem Berichtsbefehl auf der gleichen Befehlszeile **nur** dann vorausgehen, wenn der Befehl durch ein Skript oder die Befehlszeile aufgerufen wird. Wenn Sie den Berichtsbefehl von einem Menü aus ausgeben, brauchen Sie pdm_task nicht mit einschließen, weil alle Umgebungsvariablen von der Anwendung festgelegt werden.

Hinweis: Berichte können nicht von der Befehlszeile auf einem Client erstellt werden.

Syntax

Dieser Befehl hat das folgende Format:

```
pdm_task command
```

Befehl

Gibt einen Befehl an, der über keinen Wrapper verfügt und somit Umgebungsvariablen nicht automatisch festlegt. Weitere Informationen über das Ausführen von "pdm_task" in Zusammenhang mit einem Befehl finden Sie in [report: Erstellen von Berichten](#) (siehe Seite 1205).

pdm_text_cmd – Befehlszeilenschnittstelle für Text-API

pdm_text_cmd ist der Befehl für die Text-API, mit der Sie verschiedene Objekte wie zum Beispiel Requests, Changes, Issues, Assets und Kontakte erstellen und aktualisieren können.

Wichtig! Sie können kein einzelnes oder doppeltes Anführungszeichen als Parameter der Befehle pdm_text_nxd oder bop_cmd verwenden.

Syntax

Dieser Befehl hat das folgende Format:

```
pdm_text_cmd -t table {-u from_userid -p from_persid} [-o operation] [-f input file]
[-T timeout] [-h]
```

-t table

(Erforderlich) Gibt die zu verarbeitende Tabelle an. Der *Tabellenname* kann einer der folgenden Werte sein (keine Unterscheidung zwischen Groß- und Kleinschreibung):

- Asset
- Kontakt
- Ändern
- Issue
- Request

Hinweis: Eine vollständige Liste der gültigen Tabellennamen finden Sie im Abschnitt [OPTIONS] der Datei "text_api.cfg".

-u from_userid | -p from_persid

(Eine Option erforderlich) Bestimmt den Kontakt für diese Operation:

-u from_userid

Bestimmt den Kontakt über die Anwenderkennung.

-p from_persid

Bestimmt den Kontakt über die eindeutige Objektkennung für den Kontaktdatensatz. "*from_persid*" muss folgendes Format haben: **cnt:xxxx. xxxx** ist die permanente ID des Objekts.

Hinweis: Der Wert, den Sie mit dieser Option angeben, wird am Ende der Eingabe für den Befehl "pdm_text_cmd" angehängt, wobei das entsprechende Schlüsselwort, %FROM_USERID oder %FROM_PERSID, verwendet wird.

-o operation

Gibt die durchzuführende Operation an. Die *Operation* muss einer der folgenden Werte sein (keine Unterscheidung zwischen Groß- und Kleinschreibung):

- NEU – Erstellt ein Objekt. Dies ist der Standardwert, wenn keine Operation angegeben wird.
- UPDATE | UPD – Erstellt ein Objekt wenn kein Objekt gefunden wurde oder aktualisiert ein bestehendes Objekt, wenn ein Objekt gefunden wurde.

- UPDATE_ONLY | UPDO – Aktualisierung erfolgt, wenn ein Objekt gefunden wurden, andernfalls erfolgt keine Aktion.

Sowohl für UPDATE als auch für UPDATE_ONLY ist das %SEARCH-Schlüsselwort bei der Eingabe des Befehls erforderlich. Bei jedem Aufruf von "pdm_text_cmd " können Sie nur eine Operation ausführen.

-f *input_file*

Gibt den vollständigen Pfad der zu verarbeitenden Datei an. Dies ist eine Textdatei, die gültige Text-API-Befehle enthält. Wenn Sie diesen Parameter weglassen, werden Befehle aus STDIN benutzt. Die Text-API verwendet das folgende grundlegende Eingabeformat:

%keyword=value

Sie können mehrere Befehle eingeben, indem Sie die Befehlsanfrage durch mindestens fünf Prozentzeichen trennen (%%%%%).

Hinweis: Weitere Informationen über gültige Schlüsselwörter und über das Formatieren einer Eingabe zur Text-API finden Sie in der Datei "text_api.cfg".

-T *timeout*

Gibt die Anzahl der Sekunden an, die auf eine Antwort vom Server gewartet wird, bevor eine Zeitüberschreitung eintritt. Der Standardwert ist 30 Sekunden.

Hinweis: "pdm_text_cmd" zeigt die textbasierten Antworten von Text-API an: Erfolgs- oder Fehlermeldungen sowie den ursprünglichen gesendeten und über die API verarbeiteten Text. "pdm_text_cmd" gibt "0" zurück, wenn der Befehl erfolgreich ohne Warnungen oder Fehler ausgeführt wurde oder "1", wenn der Befehl zwar erfolgreich abschließt, jedoch Warnungen aufweist. Jeder andere Rückgabewert zeigt an, dass ein Fehler aufgetreten ist.

Wichtig! Bei UNIX muss der LIBPATH vor der Ausführung mehrerer CA SDM-Dienstprogramme festgelegt werden. Verwenden Sie *pdm_task*, um den LIBPATH vor der Ausführung eines Dienstprogramms festzulegen. Geben Sie zum Beispiel "pdm_task pdm_clean_attachments ..." ein.

Hinweis: Wenn Sie Parameter über die Eingabeaufforderung weitergeben, verwenden Sie STRG+Z in Windows und STRG+D in POSIX.

Weitere Informationen:

[Verwenden der Text-API](#) (siehe Seite 579)

Beispiele für Eingaben

"pdm_text_cmd" ist die Befehlszeilenschnittstelle für die Text-API, mit der Sie verschiedene Objekte, wie zum Beispiel Anfragen, Changes, Issues, Assets und Kontakte erstellen und aktualisieren können.

Beispiel: Verwenden einer Eingabedatei zum Erstellen eines Issue

Das folgende Beispiel zeigt, wie eine pdm_text_cmd-Eingabedatei zum Erstellen eines Issue verwendet wird:

```
%DESCRIPTION=Dies ist mein Test.  
%PRIORITY=3
```

Angenommen, der vollständige Pfad dieser Datei ist "c:\update.txt". Dann geben Sie den folgenden Befehl ein, um diese Datei zu verarbeiten:

```
pdm_text_cmd -t Issue -u user01 -f c:\input.txt
```

Beispiel: Verwenden einer Eingabedatei zum Aktualisieren eines Issue

Das folgende Beispiel zeigt eine Eingabedatei, um die Priorität der Problemanfrage 123 in 2 zu aktualisieren:

```
%SEARCH=ISSUE_ID  
%ISSUE_ID=123  
%PRIORITY=2
```

Angenommen, der vollständige Pfad dieser Datei ist "c:\update.txt". Dann geben Sie den folgenden Befehl ein, um diese Datei zu verarbeiten:

```
pdm_text_cmd -t Issue -o UPDATE_ONLY -u user01 -f c:\update.txt
```

Beispiel: Verwenden einer Eingabedatei, um mehrere Anfragen zu erstellen

Das folgende Beispiel zeigt, wie Sie mehrere Anfragen mit einer einzelnen Eingabedatei erstellen. Dieser Befehl ist nützlich, wenn Sie Testdaten auf einem Testsystem erstellen möchten.

```
%DESCRIPTION=Dies ist Test 1.  
%PRIORITY=3  
%  
%DESCRIPTION=Dies ist Test 2.  
%PRIORITY=2  
%  
%DESCRIPTION=Dies ist Test 3.  
%PRIORITY=None
```

Angenommen, der vollständige Pfad dieser Datei ist "c:\testdata.txt". Dann geben Sie den folgenden Befehl ein, um diese Datei zu verarbeiten:

```
pdm_text_cmd -t Request -u user01 -f c:\testdata.txt
```

pdm_uconv – Konvertiert den lokalen Zeichensatz in UTF-8

Das Hilfsprogramm "pdm_uconv" unterstützt Sie bei der Konvertierung von Daten von früheren Releases von CA SDM oder von Daten aus Integrationen mit anderen CA Technologies-Produkten. Dieses Hilfsprogramm wird normalerweise dazu verwendet, lokale Zeichensätze in UTF-8, und umgekehrt, zu konvertieren.

Syntax

Dieser Befehl hat das folgende Format:

```
pdm_uconv -h [-V] [-s] [-v] [-l | --list-code  
| --default-code | -L] [--cannon] [-x] [--to-callback | -c] [--from-callback | -i]  
[--fallback | --no-fallback] [-b] [-f] [--t] [--add-signature] [--remove-signature]  
[-o] [file ...]
```

-h

Öffnet das Hilifemenü.

-V

Druckt die Programmversion.

-s

Verwendet den automatischen Betrieb und unterdrückt Meldungen.

-v

Zeigt Informationen zum Bearbeitungsstatus des Hilfsprogramms an.

-l

Listet alle für die Transliteration verfügbaren Codierungen auf. Die folgenden sind zulässig:

--list-code

Listet nur die bestehende Codierung auf.

--default-code

Listet nur die bestehende Codierung auf.

-L

Listet alle verfügbaren Codierungen auf.

--cannon

Druckt die Liste im Format cnvtrts.txt(5).

-x

Anwendung von Transliteration auf bereits bearbeitete Elemente.

--to-callback *Rückruf*

Rückruf für die Codierung von Zielelementen.

-c

Schließt ungültige Zeichen von der Ausgabe aus.

--from-callback *Rückruf*

Rückruf für kodierte Ursprungselemente.

-i

Ignoriert ungültige Sequenzen in der Eingabe.

-- callback *Rückruf*

Rückruf für beide Codierungen.

-b

Legt die Blockgröße fest.

Standard: 4096

--fallback

Verwendet Fallback-Zuordnung.

--no-fallback

Verwendet keine Fallback-Zuordnung.

-f

Legt die ursprüngliche Codierung fest.

-t

Legt die Zielcodierung fest.

--add-signature

Fügt das Unicode-Signaturzeichen U+FEFF hinzu (BOM).

--remove-signature

Entfernt das Unicode-Signaturzeichen U+FEFF (BOM).

-o

Schreibt Ausgabe in Datei.

Beispiele:

Von einem lokalem Zeichensatz zu UTF-8

```
pdm_uconv -t UTF-8 inputfile.txt > outputfile.txt
```

Von einem bestimmten Zeichensatz (iso-2022-jp) zu UTF-8

```
pdm_uconv -f iso-2022-jp -t UTF-8 inputfile.txt > outputfile.txt
```

Von UTF-8 zu einem lokalen Zeichensatz

```
pdm_uconv -t utf-8 inputfile.txt > outputfile.txt
```

Von UTF-8 zu einem lokalen Zeichensatz

```
pdm_uconv -f UTF-8 -t iso-2022-jp inputfile.txt > outputfile.txt
```

Das Dienstprogramm "pdm_uconv" besitzt die folgenden gültigen Rückrufe:

- substitute
- skip
- stop
- Interpretation verzögern
- escape-icu
- escape-java
- escape-c
- escape-xml
- escape-xml-hex
- escape-xml-dec
- escape-unicode

pdm_userload – Hinzufügen, Aktualisieren und Löschen von Datenbank-Datensätzen

Das Hilfsprogramm "pdm_userload" aktualisiert eine CA SDM-Datenbank und verwendet dazu eine Eingabedatei, die Sie festgelegt haben.

Wichtig! Vor der Ausführung von "pdm_userload" sollten Sie Ihre Datenbank immer sichern.

Wenn Sie Tickets (wie zum Beispiel Problemanfragen oder Anforderungen) laden, sollte die Ticketnummer ein eindeutiges Präfix oder Suffix in der Zeichenfolge enthalten. CA SDM zeigt diese Zahl als Zeichenfolge und nicht als Sequenznummer an. Somit kann nicht garantiert werden, dass den hochgeladenen Tickets eine eindeutige Nummer zugewiesen wird. Solange Sie mit awk oder einem anderen Textverarbeitungsprogramm ein eindeutiges Präfix oder Suffix zuweisen, können Sie Tickets laden, ohne dass CA SDM zuvor zugewiesene Nummern überschreibt.

Syntax

Dieser Befehl hat das folgende Format:

```
pdm_userload [-a] [-c] [-h] [-r] [-v] [-u] [-m] -f filename
```

Eingabedateiformat

Die Eingabedateieinträge befolgen dieses Format:

```
TABLE table_name
fieldname1 fieldname2 . . . fieldnameN
{ "value11", "value12", . . . "value1N" }
{ "value21", "value22", . . . "value2N" }
.
.
.
{ "valueN1", "valueN2", . . . "valueNN" }
```

"table_name" ist der Name der hochzuladenden Tabelle, die in der Schema-Datei der CA SDM-Datenbank aufgeführt wird. Diese Datei befindet sich unter \$NX_ROOT/site/schema.sch (UNIX) oder unter installation-directory\site\schema.sch (Windows), wobei \$NX_ROOT oder installation-directory das Verzeichnis ist, in dem Sie CA SDM installiert haben.

-f filename

Gibt eine Eingabe-ASCII-Datei an.

-a

Aktualisiert alle vorhandenen Datensätze, unabhängig davon, ob mehr als ein vorhandener Datensatz einem einzelnen Eingabedatensatz entspricht. Ohne diese Option werden Datensätze, die mehr als einem vorhandenen Datensatz entsprechen, zurückgewiesen.

Wichtig! Verwenden Sie diese Option mit Vorsicht.

-c

Überprüft die Eingabedatei gegen die Datenbank und die Berichte der durchzuführenden Aktualisierungen, führt jedoch keine Aktualisierungen durch.

-r

Entfernt Datenbank-Datensätze, die Eingabe-Datensätzen entsprechen. Die Option „-a“ kann zusammen mit der Option „-r“ verwendet werden.

Hinweis: Es empfiehlt sich, eine Sicherungskopie der Datenbank anzufertigen, bevor Sie "pdm_userload" mit dieser Option ausführen. Sobald alte Datenbank-Datensätze entfernt worden sind, müssen Sie die CA SDM-Datenbank mit dieser Sicherungskopie wiederherstellen, wenn Sie gelöschte Datensätze wiederherstellen möchten.

-v

Gibt den Verbose-Modus an.

-u

Aktualisiert vorhandene Datensätze, fügt jedoch keine neuen Datensätze in die Datenbank ein.

-m

Bedeutet Massenaktualisierung. Geben Sie diese Option an, wenn Sie mit "pdm_userload" eine große Anzahl von Datensätzen hinzufügen oder löschen. Diese Option unterdrückt alle Clientbenachrichtigungen hinsichtlich Aktualisierungen und sendet eine Meldung zur Aktualisierung des Caches für eine Tabelle, wenn "pdm_userload" die Verarbeitung der Tabelle abschließt.

-x

Verwendet Lokale-spezifische numerische Eingabeformate.

-t

Gibt den Namen oder die UUID von Mandanten an, um alle geladenen Daten mit dem angegebenen Mandanten zu verknüpfen. Dieses Argument ist nur gültig, wenn Mandantenfähigkeit installiert ist.

"Pdm_userload" unterstützt neue Argumente ("Kürzen" und "NoNewID") auf der Anweisung TABLE. Diese Argumente sind in einer optionalen eingeklammerten Option nach dem Tabellennamen angegeben. Beispiel:

```
TABLE Call_Req (TRUNCATE, NONEWID)
```

Kürzen

Veranlasst "pdm_userload" dazu, einen datenbankspezifischen TRUNCATE-Befehl für die Tabelle auszugeben, bevor Daten geladen werden. Da es sich ausschließlich um neue Datensätze handelt, bewirkt das Argument auch, dass "pdm_userload" die Datensätze lediglich einfügt – ohne die in der Befehlszeile angegebenen Argumenten zu berücksichtigen.

NoNewID

Bewirkt, dass "pdm_userload" für neue Zeilen in der Tabelle den ID-Wert der Eingabekontrolldatei verwendet. Es wird keine neue ID für eingefügte Daten erzeugt (Standardlogik der Option "pdm_userload -i").

Einschränkungen

Sie können pdm_userload ausführen, während CA SDM aktiv ist; die Leistung kann jedoch sehr beeinträchtigt werden. Führen Sie pdm_userload am besten aus, wenn kein Anwender CA SDM verwendet.

Weitere Informationen:

[pdm_replace – Ersetzen einer Datenbanktabelle](#) (siehe Seite 1186)

[pdm_backup – Exportieren der Datenbank in eine ASCII-Datei](#) (siehe Seite 1155)

[pdm_restore – Wiederherstellen einer Datenbank](#) (siehe Seite 1189)

pdm_webstat – Zurückgeben von Webnutzungsstatistiken

Verwenden Sie pdm_webstat, um Statistiken für CA SDM-Sitzungen und Benutzerstatistiken für einen oder mehrere Web-Engine-Prozesse zurückzugeben. Der Befehl "pdm_webstat" zeigt die Gesamtzahl der Sitzungen an, die maximalen gleichzeitig vorhandenen Sitzungen und die aktuell aktiven Sitzungen. Außerdem können Informationen über die einzelnen Benutzer geliefert werden.

Syntax

Dieser Befehl hat das folgende Format:

```
pdm_webstat [-r] [-d | -D] [-i] [-t timeout] [-p webengine process] [-n] [-h]
```

-r

Geben Sie diese Option für reinen Text an, ohne Titel und andere Formatierungen. Innerhalb der Ausgabe für einen einzelnen Web-Engine-Prozess gibt es keine Zeilenumbrüche. Die Ausgabe beginnt aber für jeden Web-Engine-Prozess immer in einer neuen Zeile.

Im reinen Textmodus werden Daten in genau der gleichen Reihenfolge angezeigt wie bei Verwendung von "pdm_webstat" ohne Option „-r“. Wählen Sie den reinen Textmodus, wenn Sie die ausgegebenen Daten in einer Tabellenkalkulation oder in einer anderen Art von Bericht verwenden möchten. Die folgende Syntax:

```
pdm_webstat -r
```

zeigt beispielsweise folgende Ausgabe an:

```
11.10.05 10:31:49 web:local:0 12 4 2
11.10.05 10:31:49 web:local:1 9 2 2
```

-d

Geben Sie diese Option für eine ausführliche Ausgabe an, die Benutzersitzungen anzeigt. Die Option „-d“ führt alle aktuellen Sitzungen im Format *userid@IPaddress* auf. Wenn eine Sitzung ohne Benutzer-ID angezeigt wird, bedeutet dies gewöhnlich, dass die Sitzung noch nicht angemeldet ist. Die folgende Syntax:

```
pdm_webstat -d
```

zeigt beispielsweise folgende Ausgabe an:

```
PDM_Webstat: Aufgerufen am 11.10.2005 10:27:31
```

```
=====
Bericht der Web-Engine: web:local:0
```

```
=====
Cumulative sessions so far = 12
Most sessions at a time    = 4
Currently active sessions  = 2
    @192.168.1.16
    usery@192.168.1.20
```

```
=====
Bericht der Web-Engine: web:local:1
```

```
=====
Cumulative sessions so far = 7
Most sessions at a time    = 2
Currently active sessions  = 2
    SrvcPlus@192.168.1.14
    userx@192.168.1.8
```

-D

Liefert eine detaillierte Ausgabe für Debugging-Zwecke. Diese Option sollte nur angegeben werden, wenn Sie dazu vom Computer Associates Support ausdrücklich aufgefordert werden. Sie fügt interne Informationen über jede Sitzung zur normalen Detailausgabe hinzu. Die folgende Syntax:

```
pdm_webstat -D
```

zeigt beispielsweise folgende Ausgabe an:

```
PDM_Webstat: Aufgerufen am 11.10.2007 10:28:10
```

```
=====
Bericht der Web-Engine: web:local:0
=====
```

```
Cumulative sessions so far = 12
Most sessions at a time    = 4
Currently active sessions  = 2
  @192.168.1.16           SessionStat  1
  userx@192.168.1.20      SessionStat  5
=====
```

```
Bericht der Web-Engine: web:local:1
=====
```

```
Cumulative sessions so far = 7
Most sessions at a time    = 2
Currently active sessions  = 2
  SrvcPlus@192.168.1.14   SessionStat  7
  userx@192.168.1.8       SessionStat 13
=====
```

-i

Gibt ein Intervall in Sekunden zwischen aufeinander folgenden Berichten an. Wenn das Argument `-i` angegeben ist, wird "pdm_webstat" kontinuierlich ausgeführt. Der Befehl "pdm_webstat" erzeugt einen Bericht in dem von anderen Argumenten verlangten Format, wartet auf das angegebene Intervall und erzeugt den Bericht erneut. Bei Angabe von `-i` wird "pdm_webstat" nur beendet, wenn es explizit abgebrochen wird, normalerweise mit STRG+C. Die folgende Syntax:

```
pdm_webstat -i 5 -p web:local -r
```

zeigt beispielsweise folgende Ausgabe an:

```
21.09.05 16:27:25 web:local 14 10 6
21.09.05 16:27:30 web:local 17 10 9
21.09.05 16:27:35 web:local 18 10 10
21.09.05 16:27:41 web:local 21 13 13
```

-t timeout

Gibt einen Zeitlimitwert in Sekunden an. Dieser Parameter bewirkt, dass "pdm_webstat" vor seiner Beendigung eine bestimmte Anzahl von Sekunden auf eine Antwort wartet. Der Standardwert ist 30 Sekunden.

-p webengine_process

Geben Sie den Prozessnamen der Web-Engine an, für die Sie Berichte erstellen möchten. Standardmäßig werden Berichte für alle Web-Engine-Prozesse erstellt. Der Prozessname (auch als Slump-Name bezeichnet) ist der gleiche Name, der auch in einer slstat-Ausgabe angezeigt wird; er beginnt immer mit „web:“.

-n

Diese Option unterdrückt den normalen Protokolleintrag für jede Web-Engine, über die berichtet wird. Standardmäßig wird ein Protokolleintrag erstellt, der eine Zusammenfassung zu jeder Web-Engine enthält.

Hinweis: Wenn Sie keine Parameter angeben, zeigt "pdm_webstat" standardmäßig Zusammenfassungsdaten für alle aktiven Prozesse an.

"pdm_webstat" gibt null zurück, wenn der Befehl erfolgreich ausgeführt wurde. Ein Wert ungleich null weist auf einen Fehler hin (zum Beispiel eine Zeitüberschreitung oder keine aktiven Web-Engine-Prozesse).

Beispiel: Ausgabe von "pdm_webstat", wenn keine Parameter angegeben werden

Das folgende Beispiel zeigt die Ausgabe von "pdm_webstat", wenn dieser Befehl ohne Parameter ausgeführt wird:

PDM_Webstat: Aufgerufen am 11.10.2007 10:26:42

=====

Bericht der Web-Engine: web:local:0

=====

Cumulative sessions so far = 12
Most sessions at a time = 4
Currently active sessions = 2

=====

Bericht der Web-Engine: web:local:1

=====

Cumulative sessions so far = 7
Most sessions at a time = 2
Currently active sessions = 2

Wichtig! Bei UNIX muss der LIBPATH vor der Ausführung mehrerer CA SDM-Dienstprogramme festgelegt werden. Verwenden Sie *pdm_task*, um den LIBPATH vor der Ausführung eines Dienstprogramms festzulegen. Geben Sie zum Beispiel "pdm_task pdm_clean_attachments ..." ein.

report – Generieren von Berichten

Gilt nur für UNIX

Mit dem Berichtsprogramm können Sie einen Bericht von der Befehlszeile auf dem Server erstellen. Um den Berichtsbefehl an der Befehlszeile oder in einem Skript auszugeben, müssen Sie `pdm_task` mit einschließen. Der Befehl „`pdm_task`“ legt Umgebungsvariablen für Befehle fest, die über keinen Wrapper verfügen. Geben Sie "`pdm_task`" mit dem Berichtsbefehl auf der gleichen Befehlszeile *nur* dann ein, wenn der Bericht durch ein Skript oder die Befehlszeile aufgerufen wurde. Wenn Sie den Berichtsbefehl von einem Menü aus ausgeben, brauchen Sie `pdm_task` nicht mit einschließen, weil alle Umgebungsvariablen von der Anwendung festgelegt werden.

Syntax

Dieser Befehl hat das folgende Format:

```
pdm_task report [-h] [-e] [-f] [-F ffstring] [-p pagelength] filename [ command line arguments]
```

-e

Wiederholt ein kompiliertes Skript (für Debugzwecke).

-f

Verwendet einen Seitenvorschub zwischen Seiten.

-F ffstring

Legt die optionale Seitenvorschubzeichenfolge fest.

-p pagelength

Legt die Seitenlänge fest. Die Länge der Standardseite ist 66.

filename (Dateiname)

Die Berichtsvorlage. Wenn Sie den Berichtsbefehl nicht von dem Verzeichnis aus ausführen, in dem sich die Vorlagendatei befindet, schließen Sie den vollständigen Dateipfadnamen mit ein. Der Befehl sendet die Ausgabe als Standardausgabe (stdout).

Befehlszeilenargumente

Gibt von der Berichtsvorlage empfangende Parameter an. Wenn der Bericht so ausgerichtet ist, dass er Befehlszeilenargumente akzeptiert, müssen Sie ein Befehlszeilenargument für jeden Parameter in der Berichtsvorlage eingeben. Wenn das Argument leer ist, geben Sie die Zeichenfolge Null ein.

Der folgende Befehl stellt beispielsweise die Befehlszeilenargumente "Smith", "Jane" und "L" bereit. Die Berichtsvorlage benötigt diese drei Parameter, um den Bericht für die betroffenen Kontakte zu erstellen.

Geben Sie z. B. ein:

```
pdm_task report /opt/CAisd/samples/sdk/reports/affected.rpt
```

Im nächsten Beispiel hat Jane Smith keinen zweiten Vornamen:

```
pdm_task report /opt/CAisd/samples/sdk/reports/affected.rpt Smith Jane "
```

rpt_srv – Generieren von Berichten

Gilt nur für Windows.

Mit dem Berichtsprogramm können Sie einen Bericht von der Befehlszeile auf dem Server erstellen. Um den Berichtsbefehl an der Befehlszeile oder in einem Skript auszugeben, müssen Sie `pdm_task` mit einschließen. Der Befehl „`pdm_task`“ legt Umgebungsvariablen für Befehle fest, die über keinen Wrapper verfügen. Geben Sie "pdm_task" mit dem Berichtsbefehl auf der gleichen Befehlszeile nur ein, wenn der Bericht durch ein Skript oder die Befehlszeile aufgerufen wurde. Wenn Sie den Berichtsbefehl von einem Menü aus ausgeben, brauchen Sie `pdm_task` nicht mit einschließen, weil alle Umgebungsvariablen von der Anwendung festgelegt werden.

Syntax

Dieser Befehl hat das folgende Format:

```
rpt_srv -m [-h] [-e] [-f] [-F ffstring] [-p pagelength] filename [ command line arguments]
```

-m

Gibt an, dass der Bericht manuell von der Befehlszeile ausgeführt wird.

-e

Wiederholt ein kompiliertes Skript (für Debugzwecke).

-f

Verwendet einen Seitenvorschub zwischen Seiten.

-F ffstring

Legt die optionale Seitenvorschubzeichenfolge fest.

-p pagelength

Legt die Seitenlänge fest. Die Länge der Standardseite ist 66.

-C

Ändert die Codierung von UTF-8 in einen anderen Zeichensatz. Die Standardausgabe ist UTF-8.

Beispiel: Um die Ausgabe nach JIS zu konvertieren, würden Sie den Befehl "-C iso-2022-jp" ausführen.

Beispiel: Um den systemeigenen Zeichensatz zu kodieren, verwenden Sie "DEFAULT" oder "NATIVE".

-B

Unterdrückt die Bytereihenfolge-Markierung, wenn die Variable NX_ADD_UTF8_BYTE_ORDER_MARK gesetzt ist.

Die Option NX_ADD_UTF8_BYTE_ORDER_MARK ist eine Signatur für eine Datei. Sie ermöglicht Editoren, die UTF-8 unterstützen, die UTF-8-Integrität der Datei zu bewahren.

Hinweis: Die Option ist nur für Nicht-ASCII-Daten erforderlich. Wenn sie nicht installiert ist, wird im Standardverhalten die Bytereihenfolge-Markierung (Byte Order Mark, BOM) ausgelassen. Ist sie dagegen installiert, setzen Sie sie auf "1" oder "Yes".

filename (Dateiname)

Gibt die Berichtsvorlage an. Wenn Sie den Berichtsbefehl nicht von dem Verzeichnis aus ausführen, in dem sich die Vorlagendatei befindet, schließen Sie den vollständigen Dateipfadnamen mit ein. Der Befehl sendet die Ausgabe als Standardausgabe (stdout).

Befehlszeilenargumente

Gibt von der Berichtsvorlage empfangende Parameter an. Wenn der Bericht so ausgerichtet ist, dass er Befehlszeilenargumente akzeptiert, müssen Sie ein Befehlszeilenargument für jeden Parameter in der Berichtsvorlage eingeben. Wenn das Argument leer ist, geben Sie die Zeichenfolge Null ein.

Der folgende Befehl stellt beispielsweise die Befehlszeilenargumente "Smith", "Jane" und "L" bereit. Die Berichtsvorlage benötigt diese drei Parameter, um den Bericht für die betroffenen Kontakte zu erstellen.

Geben Sie beispielsweise folgenden Befehl ein:

```
rpt_srv -m c:\reports\affected.rpt Smith Jane L
```

Im nächsten Beispiel hat Jane Smith keinen zweiten Vornamen:

```
rpt_srv -m c:\reports\affected.rpt Smith Jane "
```

uniconv – Starten des UNIX CA NSM-Event Converter-Daemons

Gilt nur für UNIX

Wenn CA SDM mit CA NSM integriert wird, können Sie uniconv verwenden, um generische Ereignisdaten an Filter-Daemons in <USDK zu schicken. "uniconv" wird in einer Meldungsaktion in CA NSM-Event Management verwendet.

Syntax

Dieser Befehl hat das folgende Format:

```
uniconv -h &opnode -e &'text' [-n &
nodeid] [-u &userid] [-d &datem] [-t &
time']
```

Einschränkungen

"uniconv</cs> muss in "\$NX_ROOT/bin</cs> unter UNIX ausgeführt werden. Zur Verwendung dieses Hilfsprogramms muss Ihr Standort mit CA NSM integriert sein.

-h &opnode

Gibt den Knotennamen des Computers an, auf dem Sie "uniconv</cs> ausführen (erforderlich).

-e &'text'

Gibt den vollständigen Text der Meldung an (erforderlich).

-n &nodeid

Gibt den Knotennamen an, von dem die Meldung stammt (erforderlich).

-u &userid

Gibt die Anmelde-ID der Person an, von der die Meldung stammt.

-d &datem

Gibt das Systemdatum im Format *mm/dd/yy* an.

-t &'time'

Gibt die Systemzeit an.

Dienstprogramm "pdm_mail" - Senden von E-Mail-Informationen

Das Dienstprogramm "pdm_mail" wird in Benachrichtigungen verwendet, um E-Mails durch Senden von E-Mail-Informationen an den Prozess "pdm_mail_nxd" zu senden. Das Dienstprogramm "pdm_mail" kann auch für Befehle, nicht aber für beide Vorgänge gleichzeitig verwendet werden. Wenn keine Parameter verwendet werden, gilt das Standardverhalten, nach dem die Variable "NX_NTF_xxxx" zum Übergeben von Parametern verwendet wird.

Für E-Mail wird das Dienstprogramm folgendermaßen aufgerufen:

```
pdm_mail [-i [-s subject] [-e email_address] [-q]] [-p] [-M] [-F] [-T] [-B] [-H] [-N] [-R] [-h]
```

-i

Verwendet STDIN an Stelle von NTF-Variablen. Die folgenden Parameter werden nur für STDIN-E-Mail-Verhalten benutzt:

-e

Gibt die E-Mail-Adresse (des Empfängers) an.

-s

Gibt den Betreff der E-Mail an.

-q

Deaktiviert die Anzeigaufforderung für STDIN.

-p

Verwendet Pagerlogik. Diese Option schließt die Verwendung der Pager-E-Mail-Adresse an Stelle der regulären E-Mail-Adresse ein. Nur die Klartextversion der Benachrichtigung wird benutzt (kein HTML).

-M

Verwendet im Nachrichtentext lediglich Nur-Text-Format (nicht aber MIME).

-F

Gibt die Absenderadresse der E-Mail an.

-T

Gibt die Antwortadresse der E-Mail an.

-B

Gibt den Zeichensatz des Texts an. Dies ist für Pager nützlich, die UTF-8- nicht unterstützen.

-H

Gibt den Zeichensatz für Kopfzeilen an. Dies ist für Pager nützlich, die UTF-8- nicht unterstützen.

-N

Gibt die Option "Benachrichtigen" von DSN (Delivery Status Notification) an.

-R

Gibt die Option "Return" von DSN (Delivery Status Notification) an.

-h

(Optional) Zeigt Hilfe zum Dienstprogramm an.

Für Befehle wird das Dienstprogramm folgendermaßen aufgerufen:

Befehl an Mailserver

Option "pdm_mail -c" [Parameter]

Befehl an Mail Eater

Option "pdm_mail -x" [Parameter]

check_interval

(nur -x) Ändert das Mail-Überprüfungsintervall in einen angegebenen Wert (in Sekunden).

report_interval

Ändert das Berichtsintervall in einen angegebenen Wert (in Sekunden).

report_now

Erzwingt einen Bericht über die Protokolle. Der Zähler wird nicht zurückgesetzt.

send_q

(nur -c) Sendet die lokale E-Mail-Server-Warteschlange an den Remote-E-Mail-Server.

Trace

Aktiviert bzw. deaktiviert Tracing.

Wichtig! Bei UNIX muss der LIBPATH vor der Ausführung mehrerer CA SDM-Dienstprogramme festgelegt werden. Verwenden Sie *pdm_task*, um den LIBPATH vor der Ausführung eines Dienstprogramms festzulegen. Geben Sie zum Beispiel "pdm_task pdm_clean_attachments ..." ein.

pdm_server_control Utility--Identify Servers

Die pdm_server_utility-Befehle identifizieren den Server als Hintergrund- oder Standby-Server in einer Konfiguration mit erweiterter Verfügbarkeit.

Führen Sie den folgenden Befehl an der Eingabeaufforderung aus:

```
pdm_server_control -h | -b | -q interval [-s Servername] | -t | -c [-Servername]
```

-h

Zeigt die Hilfeseite an.

-b

Benachrichtigt einen lokalen Standby-Server, der in den Hintergrundserver gewechselt wird. Der Standby-Server muss bereits ausgeführt werden. Wenn der Server nicht ausgeführt wird, wird er gestartet, aber es wird kein Failover ausgeführt. Um ein Failover zu starten, führen Sie den Befehl erneut aus.

-q interval [-s Servername]

Benachrichtigt einen lokalen Anwendungsserver oder einen Remote-Anwendungsserver, eine Stilllegung in einem angegebenen Zeitintervall durchzuführen. Dieses Intervall ist die Anzahl von Sekunden, bevor der Server offline geschaltet wird. Wenn Sie diese Option ohne "Servername" verwendet, dann wird der lokale Server zur Stilllegung benachrichtigt. Diese Option kann für einen Hintergrundserver oder einen Standby-Server nicht verwendet werden.

-t

Zeigt den Typ dieses CA SDM-Servers für die erweiterte Verfügbarkeit an.

-c [-s Servername]

Benachrichtigt einen lokalen oder Remote-Anwendungsserver, um die frühere Anforderung zum Stilllegen abzuberechnen.

Anhang B: Beschreibungen der Felder in Ansichten

Dieses Kapitel enthält folgende Themen:

[Beschreibungen der Felder in Ansichten](#) (siehe Seite 1214)

[View Act Log](#) (siehe Seite 1214)

[View Audit Assignee](#) (siehe Seite 1216)

[View Audit Group](#) (siehe Seite 1216)

[View Audit Priority](#) (siehe Seite 1217)

[View Audit Status](#) (siehe Seite 1218)

[View Change Act Log](#) (siehe Seite 1218)

[View Change](#) (siehe Seite 1220)

[View Change to Assets](#) (siehe Seite 1225)

[View Change to Change Act Log](#) (siehe Seite 1225)

[View Change to Change WF](#) (siehe Seite 1227)

[View Change to Properties](#) (siehe Seite 1229)

[View Contact Full](#) (siehe Seite 1230)

[View Contact to Environment](#) (siehe Seite 1233)

[View Group](#) (siehe Seite 1234)

[View Group to Contact](#) (siehe Seite 1235)

[View Issue](#) (siehe Seite 1235)

[View Issue Act Log](#) (siehe Seite 1240)

[View Issue to Assets](#) (siehe Seite 1241)

[View Issue to Issue Act Log](#) (siehe Seite 1242)

[View Change to Request](#) (siehe Seite 1243)

[View Issue to Issue WF](#) (siehe Seite 1247)

[View Issue to Properties](#) (siehe Seite 1249)

[View Request](#) (siehe Seite 1250)

[View Request to Act Log](#) (siehe Seite 1255)

[View Request to Properties](#) (siehe Seite 1255)

Beschreibungen der Felder in Ansichten

Sie können die Feldbeschreibungsinformationen in den grundlegenden und erweiterten Ansichten von CA SDM verwenden.

Die folgenden Punkte gelten für die meisten der Tabellen:

- Um Daten in den erweiterten Ansichten anzuzeigen, müssen Sie die Audit-Protokollfunktion unter 'Administration', 'Optionsmanager', 'Audit-Protokoll' aktivieren.

Hinweis: Weitere Informationen zur Audit-Protokollierung finden Sie in der *Online-Hilfe*.

- „pdmtime“ bezieht sich auf Datums- und Zeitfelder im GMT-Format (die Anzahl der verstrichenen Sekunden seit 1/1/1970).
- Die Begriffe Änderungsanforderung und Änderungsauftrag sind austauschbar.

Weitere Informationen:

[Generieren von Berichten in USDK](#) (siehe Seite 941)

View_Act_Log

Dies ist eine grundlegende Ansicht der Tabelle „request activity log“. Der Aktivitätstyp und der vollständige Name des Analysten werden ebenfalls in der Ansicht aufgeführt. Die Tabelle „activity log“ (act_log) wurde mit den Tabellen „activity type“ (act_type) und „contact“ (ca_contact) verknüpft, um den tatsächlichen Aktivitätstyp eines jeden Aktivitätsprotokolleintrags sowie den Analytiker zu liefern, der die Aktivität durchgeführt hat. Extrahierte Felder aus den Verbindungen, die nützlich sein können, befinden sich am Ende dieser Liste.

Feld	Anmerkungen
ID	act_log.id: Die eindeutige ID für diesen Datensatz in der Tabelle "act_log".
persid	act_log.persid: Die eindeutige ID für diesen Datensatz in der Tabelle "act_log", der die Objektkennung ("alg" für "act_log") und ein Doppelpunkt vorangehen.
call_req_id	act_log.call_req_id: Zeiger für das Aufrufen der Anfrage-persid, zu der diese Aktivität gehört. act_log.call_req_id = call_req.persid.
last_mod_dt	issalg.last_mod_dt: Letztes Änderungsdatum/Änderungszeit (pdmtime).
time_spent	issalg.time_spent: Dauer dieser Aktivität, als Gesamtzahl von Sekunden gespeichert. Zum Beispiel 80 = 1 Minute, 20 Sekunden.

Feld	Anmerkungen
time_stamp	act_log.time_stamp: Benutzerdefinierbares Datum/Zeit einer Aktivität (pdmtime).
system_time	issalg.system_time: Datum/Zeit der Datensatzerstellung (pdmtime).
analyst	issalg.analyst: UUID-Zeiger zur Kontakt-UUID, um den Analysten zu finden, der die Aktivität durchgeführt hat. issalg.analyst = ca_contact.contact_uuid
description	issalg.description: Textbeschreibung dieser Aktivität, die vom Anwender geändert werden kann.
action_desc	act_log.action_desc: Textbeschreibung einer automatisierten Aktion, die vom Anwender nicht geändert werden kann.
type	issalg.type: Textzeiger zu einem Datensatz in der Aktivitätstyp-Tabelle. Zum Beispiel act_log.type = act_type.code.
knowledge_session	act_log.knowledge_session: Eine ID für eine bestimmte Sitzung eines bestimmten Anwenders.
knowledge_tool	act_log.knowledge_tool: Ein Indikator des Knowledge Tools, das für die Suche verwendet wird, z. B. NLS_FAQ oder EXPERT usw.
internal	act_log.internal: Ganzzahl-Flag (1 oder 0), das angibt, ob dieser Protokolleintrag von allen Anwendern angezeigt werden kann oder nur für die interne Verwendung bestimmt ist.
activity_type	act_type.symActivity: Abgeleitet von act_log.type = act_type.code.
analyst_lastname	View_Contact_Full.last_name: Der Nachname des Analysten, abgeleitet von "act_log.analyst = ca_contact.contact_uuid".
analyst_firstname	View_Contact_Full.first_name: Vorname des Analysten.
analyst_middlename	View_Contact_Full.middle_name: Der zweite Vorname des Analysten.

View_Audit_Assignee

Dies ist eine erweiterte Ansicht des Audit-Protokolls, in der der Zuständige verfolgt wird. Diese Ansicht zeigt die Zeitdauer zwischen einer Änderung des Zuständigen für jede Anfrage und jeden Change. Für Anfragen oder Changes, die von einem bestimmten Zuständigen in einen NULL-Zuständigen geändert und anschließend von einem NULL-Zuständigen zurück in einen bestimmten Zuständigen geändert werden, wird die Zeitdauer des NULL-Zuständigen nicht in dieser Ansicht aufgeführt. In dieser Liste werden die folgenden Felder für sowohl Anfragen als auch Changes aufgeführt. Es kann mehr als einen Eintrag pro "audoobj_uniqueid" (Anfrage oder Change) geben.

Feld	Anmerkungen
audoobj_uniqueid	audit_log.audoobj_uniqueid – Die eindeutige ID des Audit-Protokollobjekts, die die "chg.id" oder die "call_req.id" darstellt.
from_val	audit_log.attr_after_val: Der Wert "Geändert von" des Zuständigen.
to_val	audit_log.attr_after_val: Der Wert "Geändert in" des Zuständigen.
from_time	audit_log.attr_from_time: Zeit des Beginns der Zuweisung eines Zuständigen (pdmtime).
to_time	audit_log.attr_from_time: Zeit des Endes der Zuweisung desselben Zuständigen (pdmtime).

View_Audit_Group

Dies ist eine erweiterte Ansicht des Audit-Protokolls, in der die Gruppe verfolgt wird. Diese Ansicht zeigt die Zeitdauer zwischen einer Änderung der Gruppe für jede Anfrage und jeden Change. Für Anfragen oder Changes, die von einer bestimmten Gruppe in eine NULL-Gruppe geändert und anschließend von einer NULL-Gruppe zurück in eine bestimmte Gruppe geändert werden, wird die Zeitdauer der NULL-Gruppe nicht in dieser Ansicht aufgeführt. In dieser Liste werden die folgenden Felder für sowohl Anfragen als auch Changes aufgeführt. Es kann mehr als einen Eintrag pro "audoobj_uniqueid" (Anfrage oder Change) geben.

Feld	Anmerkungen
audoobj_uniqueid	audit_log.audoobj_uniqueid: Die eindeutige ID des Audit-Protokollobjekts, die die "chg.id" oder die "call_req.id" darstellt.
from_val	audit_log.attr_after_val: Der Wert "Geändert von" des Zuständigen.

Feld	Anmerkungen
to_val	audit_log.attr_after_val: Der Wert "Geändert in" des Zuständigen.
from_time	audit_log.attr_from_time: Zeit des Beginns der Zuweisung der Gruppe (pdmtime).
to_time	audit_log.attr_from_time: Zeit des Endes der Zuweisung derselben Gruppe (pdmtime).

View_Audit_Priority

Dies ist eine erweiterte Ansicht des Audit-Protokolls, in der die Priorität verfolgt wird. Diese Ansicht zeigt die Zeitdauer zwischen einer Änderung der Priorität für jede Anfrage und jeden Change. In dieser Liste werden die folgenden Felder für sowohl Anfragen als auch Changes aufgeführt. Es kann mehr als einen Eintrag pro "audobj_uniqueid" (Anfrage oder Change) geben.

Feld	Anmerkungen
audobj_uniqueid	audit_log.audobj_uniqueid: Die eindeutige ID des Audit-Protokollobjekts, die die "call_req.id" einer Anfrage oder die "chg.id" eines Change darstellt.
from_val	audit_log.attr_after_val: Der Prioritätswert "Geändert von".
to_val	audit_log.attr_after_val: Der Prioritätswert "Geändert in"
from_time	audit_log.attr_from_time: Zeitpunkt, ab dem die Priorität einen bestimmten Zustand hatte (pdmtime).
to_time	audit_log.attr_from_time: Zeitpunkt, bis zu dem die Priorität denselben Zustand hatte (pdmtime).

View_Audit_Status

Dies ist eine erweiterte Ansicht des Audit-Protokolls, in der der Status verfolgt wird. Diese Ansicht zeigt die Zeitdauer zwischen einer Änderung des Status für jede Anfrage und jeden Change. In dieser Liste werden die folgenden Felder für sowohl Anfragen als auch Changes aufgeführt. Es kann mehr als einen Eintrag pro "audobj_uniqueid" (Anfrage oder Change) geben.

Feld	Anmerkungen
audobj_uniqueid	Eindeutige ID des Audit-Protokollobjekts, die die "call_req.id" einer Anfrage oder die "chg.id" eines Change darstellt.
from_val	audit_log.attr_after_val: Der Prioritätswert "Geändert von".
to_val	audit_log.attr_after_val: Der Prioritätswert "Geändert in".
from_time	audit_log.attr_from_time: Zeitpunkt, ab dem der Status einen bestimmten Zustand hatte (pdmtime).
to_time	audit_log.attr_from_time: Zeitpunkt, bis zu dem der Status einen bestimmten Zustand hatte (pdmtime).

View_Change_Act_Log

Dies ist eine grundlegende Ansicht aller Aktivitätsprotokolle für Changes. Es handelt sich um eine Ansicht der Tabelle „change request activity log“ (chgalg), verknüpft mit der Tabelle „activity type“ (act_type) und der Tabelle „contact“ (ca_contact), um aussagefähigere Daten zu liefern, wie zum Beispiel die Beschreibung des tatsächlichen Aktivitätstyps und den vollständigen Namen des Analytikers, der die Aktivität durchgeführt hat.

Feld	Anmerkungen
ID	chgalg.id: Die eindeutige Kennung für diesen Datensatz in der Tabelle "chgalg".
persid	chgalg.persid: Die eindeutige ID für diesen Datensatz in der Tabelle "chgalg", der die Objektkennung ("chgalg" für "chgalg") und ein Doppelpunkt vorangehen.
change_id	chgalg.change_id: Der Zeiger auf die Change-ID, zu der diese Aktivität gehört. chgalg.change_id = chgalg.id
last_mod_dt	chgalg.last_mod_dt: Letztes Änderungsdatum/Änderungszeit (pdmtime)
time_spent	chgalg.time_spent: Für diese Aktivität benötigte Dauer, als Gesamtzahl von Sekunden gespeichert. Zum Beispiel 80 = 1 Minute, 20 Sekunden.

Feld	Anmerkungen
time_stamp	chgalg.time_stamp: Datum/Zeit einer Aktivität (pdmtime), die der Anwender ändern kann.
system_time	chgalg.system_time: Datum/Zeit der Datensatzerstellung (pdmtime).
analyst	issalg.analyst: Ein UUID-Zeiger zur Kontakt-UUID, um den Analysten zu finden, der die Aktivität durchgeführt hat. chgalg.analyst = ca_contact.contact_uuid
description	chgalg.description: Textbeschreibung dieser Aktivität, die vom Anwender geändert werden kann.
action_desc	issalg.action_desc: Textbeschreibung einer automatisierten Aktion, die vom Anwender nicht geändert werden kann.
type	chgalg.type: Textzeiger zu einem Datensatz in der Aktivitätstyp-Tabelle. chgalg.type = act_type.code
internal	chgalg.internal: Ganzzahl-Flag (1 oder 0), das angibt, ob dieser Protokolleintrag von allen Anwendern angezeigt werden kann oder nur für die interne Verwendung bestimmt ist.
knowledge_session	chgalg.knowledge_session: Eine ID für eine bestimmte Sitzung eines bestimmten Anwenders.
knowledge_tool	chgalg.knowledge_tool: Ein Indikator des Knowledge Tools, das für die Suche verwendet wird, z. B. NLS_FAQ oder EXPERT usw.
analyst_lastname	View_Contact_Full.last_name: Der Nachname des Analysten, abgeleitet von "chgalg.analyst = ca_contact.contact_uuid".
analyst_firstname	View_Contact_Full.first_name: Der erste Vorname des Analysten.
analyst_middlename	View_Contact_Full.middle_name: Zweiter Vorname des Analysten.
activity_type	act_type.sym: Aktivitätstyp, referenziert durch chgalg.type = act_type.code

View_Change

Dies ist eine grundlegende Ansicht aller Changes, die folgende Informationen enthält: Status, Priorität, Kategorie, Organisationen, vollständiger Name des betroffenen Endanwenders, vollständiger Name des Anforderers, vollständiger Name des Zuständigen, Gruppenname und ID usw. Hier wurde die Tabelle "change request" (chg) mit vielen anderen Tabellen verknüpft, um einige aussagefähigere Daten zum Change zu liefern.

Feld	Anmerkungen
ID	chg.id: Die eindeutige ID für diesen Datensatz in der Tabelle "chg"
persid	chg.persid: Die eindeutige ID für diesen Datensatz in der Tabelle "chg", der die Objektkennung ("chg" für die Tabelle "chg") und ein Doppelpunkt vorangehen.
chg_ref_num	chg.chg_ref_num: Change-Referenznummer, die von Analysten und Kunden verwendet wird, um auf einen bestimmten Change zu verweisen.
description	chg.description: Langversion einer Beschreibung eines Changes, die von einem Analysten oder Kunden angegeben wurde.
status	chg.status: Eindeutige ID eines Change-Status, der ein Zeiger auf die Tabelle "chgstat" ist: chg.status = chgstat.code
active_flag	chg.active_flag: Ganzzahl-Flag, um zu bestimmen, ob dieser Change-Datensatz aktiv ist oder nicht (1 oder 0).
start_date	chg.start_date: Das Datum, an dem die erste Aufgabe in den Status "Ausstehend" wechselt.
open_date	chg.open_date: Erstellungsdatum des Changes (pdmtime)
last_mod_dt	chg.last_mod_dt: Datum der letzten Änderung (pdmtime)
last_mod_by	chg.last_mod_by: Zeiger auf die Kontakt-UUID, die den Kontakt angibt, der diesen Change zuletzt geändert hat. chg.last_mod_by = ca_contact.contact_uuid.
close_date	chg.close_date: Datum, an dem der Change auf inaktiv gestellt wurde (pdmtime).
resolve_date	chg.resolve_date: Datum, an dem der Change auf einen Status eingestellt wurde, der konfiguriert wurde, um die Lösung der Änderung anzugeben (pdmtime).
rootcause	chg.rootcause: Ein Zeiger auf einen Datensatz in der Tabelle "rootcause", der die ursprüngliche Situation angibt, die die Durchführung dieses Changes veranlasste. call_req.rootcause = rootcause.id

Feld	Anmerkungen
est_total_time	chg.est_total_time: Geschätzte Gesamtzeit (pdmtime) für die Durchführung diese Changes.
actual_total_time	chg.actual_total_time: Tatsächliche Gesamtzeit (pdmtime) für die Durchführung dieses Changes.
log_agent	chg.log_agent: Eine binäre, eindeutige ID, die auf die Tabelle "ca_contact" verweist, die auf die Person verweist, von der der Change ursprünglich erstellt wurde. chg.log_agent = ca_contact.contact_uuid.
Verantwortlicher	chg.assignee: Der Zeiger auf die Kontakt-UUID, die aktuell dem Change zugewiesen ist. chg.assignee = ca_contact.contact_uuid
organization	chg.organization: Zeiger auf die UUID der internen Organisation, die die Organisation darstellt, der dieser Change angehört. issue.organization = ca_organization.organization_uuid
group_id	chg.group_id: Zeiger auf die Kontakt-UUID, die die Gruppe darstellt, die aktuell dem Change zugewiesen ist. chg.group_id = ca_contact.contact_uuid
affected_contact	chg.affected_contact: Zeiger auf die Kontakt-UUID, die den Kontakt repräsentiert, der von diesem Change betroffen ist. chg.affected_contact = ca_contact.contact_uuid
requestor	chg.requestor: Zeiger auf die Kontakt-UUID, die die Person darstellt, von der die Änderung angefordert wurde. chg.requestor = ca_contact.contact_uuid
category	chg.category: Zeiger auf den Change-Kategoriecode, um die Kategorie abzurufen, in die diese Änderung fällt. chg.category = chgcat.code
priority	chg.priority: Zeiger auf die Prioritätsaufzählung, wo die Priorität dieses Changes repräsentiert ist. chg.priority = pri.enum
need_by	chg.need_by: Datum, das angibt, bis wann der jeweilige Endanwender (affected_end_user) die Änderung benötigt (pdmtime).
est_comp_date	chg.est_comp_date: Geschätztes Beendigungsdatum (pdmtime) für diesen Change.
actual_comp_date	chg.actual_comp_date: Tatsächliches Abschlussdatum (pdmtime) für diesen Change.
est_cost	chg.est_cost: Geschätzte Kosten für diesen Change.
actual_cost	chg.actual_cost: Tatsächliche Kosten für die Implementierung dieses Changes.

Feld	Anmerkungen
justification	chg.justification: Ein Textfeld, in dem der Requestor die Gründe für diesen Change angeben kann.
backout_plan	chg.backout_plan: Ein Textfeld, in dem ein Analyst einen Backout-Plan für diesen Change angeben kann.
impact	chg.impact: Ein Zeiger auf einen Tabellendatensatz, der angibt, welche Ressourcen von diesem Change betroffen sind. chg.impact = impact.enum
parent	chg.parent: Zeiger auf eine andere Change-ID, die die Erstellung einer Hierarchie von Changes erlaubt. chg.parent = chg.id
effort	chg.effort: Ein Textfeld, in dem der Plan für die Implementierung dieses Changes erläutert wird.
support_lev	chg.support_lev: Zeiger auf einen Service Desk-Datensatz, der einige Bedingungen automatisiert, unter denen dieser Change durchgeführt werden muss. chg.support_lev = srv_desc.code
template_name	chg.template_name: Der Name einer Change-Vorlage und deren Zeiger chg.template_name = chg_template.template_name
sla_violation	chg.sla_violation: Ganzzahl zur Angabe der Häufigkeit, in der mit dieser Änderung verbundene SLAs verletzt wurden.
predicted_sla_viol	chg.predicted_sla_viol: (r5.5) Auf Neugent-Technologie bezogenes Feld
macro_predict_viol	chg.macro_predict_viol: (r5.5) Auf Neugent-Technologie bezogenes Feld
created_via	chg.created_via: Ein Zeiger auf einen Datensatz in der Tabelle "interface", der angibt, von welcher Schnittstelle der Change stammt. call_req.created_via = interface.id
call_back_date	chg.call_back_date: Ein Datums-/Zeitfeld (pdmtime), das ein zukünftiges Datum/eine zukünftige Zeit angibt, zu dem/der der Requestor kontaktiert werden soll.
call_back_flag	chg.call_back_flag: Ein Boolescher Indikator, der dem Anwender als Kontrollkästchen angezeigt wird und der angibt, ob der Analyst zum Datum "chg.call_back_date" benachrichtigt werden soll oder nicht.
string1	Dieses Textfeld ist anwenderdefinierbar.
string2	Dieses Textfeld ist anwenderdefinierbar.
string3	Dieses Textfeld ist anwenderdefinierbar.
string4	Dieses Textfeld ist anwenderdefinierbar.
string5	Dieses Textfeld ist anwenderdefinierbar.

Feld	Anmerkungen
string6	Dieses Textfeld ist anwenderdefinierbar.
service_date	chg.service_date: Das Datum/Zeit (pdmtime), die ein externer Lieferant auf diesen Change verwenden darf.
service_num	chg.service_num: Textfeld zur Angabe der Service- oder Bestellnummer eines externen Lieferanten.
Produkt	chg.product: Ein Zeiger auf einen Datensatz in der Produkttabelle, der das Produkt angibt, das von dieser Änderung betroffen ist. chg.product = product.id
Aktionen	chg.actions: Großes Textfeld zur Angabe von Aktionen
type_of_contact	chg.type_of_contact: Zeiger auf einen Datensatz in der Tabelle "toc", der die allgemeine Kategorie des betroffenen Endanwenders (affected_end_user) für den Change angibt. chg.type_of_contact = toc.id
reporting_method	chg.reporting_method: Zeiger auf einen Datensatz in der Tabelle "repmeth", der die Herkunft des Changes klassifiziert und der von der Person ausgewählt wird, die den Change erstellt. chg.reporting_method = repmeth.id
person_contacting	chg.person_contacting: Zeiger auf einen Datensatz in der Tabelle "perscon", der die Rolle des betroffenen Endanwenders (affected_end_user) oder die Rolle des Requestors angibt. chg.person_contacting = perscon.id
status_name	chgstat.sym: Beschreibung des Status aus Anwendersicht. chg.status = chgstat.code
priority_num	pri.sym: Beschreibung der Priorität aus Anwendersicht. chg.priority = pri.enum
category_name	chgcat.sym: Name der Change-Kategorie, der einem Anwender angezeigt wird. chg.category = chgcat.code
organization_name	ca_organization.org_name: Name der Organisation, der Anwendern angezeigt wird. issue.organization = ca_organization.organization_uid
affected_end_user_lastname	ca_contact.last_name: Der Nachname des betroffenen Endanwenders. chg.affected_end_user = ca_contact.contact_uid
affected_end_user_firstname	ca_contact.first_name: Der Vorname des betroffenen Endanwenders. chg.affected_end_user = ca_contact.contact_uid
affected_end_user_middlename	ca_contact.middle_name: Der zweite Vorname des betroffenen Endanwenders. chg.affected_end_user = ca_contact.contact_uid

Feld	Anmerkungen
requester_lastname	ca_contact.last_name: Nachname des Requestors chg.requestor = ca_contact.contact_uuid
requester_firstname	ca_contact.first_name: Vorname des Requestors chg.requestor = ca_contact.contact_uuid
requester_middlename	ca_contact.middle_name: Der zweite Vorname des Requestors. chg.requestor = ca_contact.contact_uuid
Geschäft	ca_organization.org_name: Der Name der Organisation des Requestors aus Anwendersicht chg.requestor = ca_organization.organization_uuid
assignee_lastname	ca_contact.last_name: Nachname des Zuständigen. chg.assignee = ca_contact.contact_uuid
assignee_firstname	ca_contact.first_name: Vorname des Zuständigen. chg.assignee = ca_contact.contact_uuid
assignee_middlename	ca_contact.middle_name: Zweiter Vorname des Zuständigen. chg.assignee = ca_contact.contact_uuid
groupid	ca_contact.contact_uuid: Eine binäre Darstellung der internen ID, die für die Gruppe verwendet wird, der dieser Change zugewiesen ist. chg.group_id = ca_contact.contact_uuid
group_name	ca_contact.last_name: Der Name der Gruppe, die diesem Change zugewiesen ist. chg.group = ca_contact.contact_uuid
service_type	srv_desc.sym: Der Name des Servicetyps, der für diesen Change gilt. chg.support_lev = srv_desc.code
impact_num	impact.sym: Beschreibung der Auswirkung, die Anwendern angezeigt wird. chg.impact = impact.enum
product_sym	product.sym: Produktbeschreibung, die Anwendern angezeigt wird. chg.product = product.id
type_of_contact_sym	toc.sym: Beschreibung des Kontakttyps, die Anwendern angezeigt wird. chg.type_of_contact = toc.id
rpting_method_sym	repmeth.sym: Beschreibung der Berichtsmethode, die Anwendern angezeigt wird. chg.reporting_method = repmeth.id
person_contacting_sym	perscon.sym: Beschreibung der Kontakt aufnehmenden Person, die Anwendern angezeigt wird. chg.person_contacting = perscon.id

View_Change_to_Assets

Dies ist eine grundlegende Ansicht von Changes und ihren Assets. Die Tabelle "change request" (chg) wird indirekt mit der Tabelle "network resource" (ca_owned_resource) verknüpft, um eine Liste der Anlagen für jeden Change zu erhalten. Es werden nicht alle Changes aufgeführt, insbesondere diejenigen nicht, die keine Assets besitzen.

Feld	Anmerkungen
View_Change.*	Alle Felder, die in der Ansicht „View_Change“ aufgeführt werden, und bereits in diesem Dokument definiert wurden.
assetID	ca_owned_resource.own_resource_uuid: Binäres Feld, das als interne, unveränderliche und eindeutige Kennung eines Anlagendatensatzes dient.
asset_serial_num	ca_owned_resource.serial_number: Seriennummer eines Anlagendatensatzes.
asset_class	ca_resource_class.name: Kurze Beschreibung der Klasse, zu der eine Anlage gehört. ca_owned_resource.resource_class = ca_resource_class.id
asset_family	ca_resource_family.name: Anlagenfamilie, zu der die Anlage gehört. ca_owned_resource.resource_class = ca_resource_class.id AND ca_resource_class.family_id = ca_resource_family.id
asset_name	ca_owned_resource.resource_name: Netzwerkname, unter dem die Anlage läuft.

View_Change_to_Change_Act_Log

Dies ist eine grundlegende Ansicht aller Changes und der zugehörigen Aktivitätsprotokolle. Diese Ansicht verknüpft die Ansicht "View_Change" mit dem Aktivitätsprotokoll für Changes (chgalg), um ausführliche Informationen über Changes und ihre Aktivitätsprotokolle zu liefern.

Feld	Anmerkungen
View_Change.*	Es werden alle Felder aufgeführt, die in der Ansicht „View_Change“ zuvor in diesem Dokument definiert wurden.
chgalg_id	chgalg.id: Die eindeutige Kennung für diesen Datensatz in der Tabelle "chgalg".
chgalg_persid	chgalg.persid: Die eindeutige ID für diesen Datensatz in der Tabelle "chgalg", der die Objektkennung ("chgalg" für "chgalg") und ein Doppelpunkt vorangehen.

Feld	Anmerkungen
change_id	chgalg.change_id: Mit diesem Zeiger kann die Reihenfolgen-ID geändert werden, zu der diese Aktivität gehört. chgalg.change_id = chgalg.id
chgalg_last_mod_dt	chgalg.last_mod_dt: Letztes Änderungsdatum/Änderungszeit (pdmtime)
time_spent	chgalg.time_spent: Für diese Aktivität benötigte Dauer, als Gesamtzahl von Sekunden gespeichert. Zum Beispiel 80 = 1 Minute, 20 Sekunden.
time_stamp	chgalg.time_stamp: Datum/Zeit einer Aktivität (pdmtime), die der Anwender ändern kann.
system_time	chgalg.system_time: Datum/Zeit der Datensatzerstellung (pdmtime).
analyst	chgalg.analyst: Ein UUID-Zeiger zur Kontakt-UUID, um den Analysten zu finden, der die Aktivität durchgeführt hat. chgalg.analyst = ca_contact.contact_uuid
chgalg_description	chgalg.description: Textbeschreibung dieser Aktivität, die vom Anwender geändert werden kann.
action_desc	act_log.action_desc: Textbeschreibung einer automatisierten Aktion, die vom Anwender nicht geändert werden kann.
type	chgalg.type: Textzeiger zu einem Datensatz in der Aktivitätstyp-Tabelle. chgalg.type = act_type.code
internal	chgalg.internal: Ganzzahl-Flag (1 oder 0), das angibt, ob dieser Protokolleintrag von allen Anwendern angezeigt werden kann oder nur für die interne Verwendung bestimmt ist.
knowledge_session	chgalg.knowledge_session: Eine ID für eine bestimmte Sitzung eines bestimmten Anwenders.
knowledge_tool	chgalg.knowledge_tool: Ein Indikator des Knowledge Tools, das für die Suche verwendet wird, z. B. NLS_FAQ oder EXPERT usw.
chgalg_analyst_id	chgalg.analyst: Ein UUID-Zeiger zur Kontakt-UUID, um den Analysten zu finden, der die Aktivität durchgeführt hat. chgalg.analyst = ca_contact.contact_uuid

View_Change_to_Change_WF

Diese Ansicht ist das Ergebnis der Verknüpfung der Ansicht „View_Change“ mit der Tabelle „Workflow task“ (wf), um eine grundlegende Ansicht von Änderungsaufträgen und ihren Workflow-Aufgaben zu liefern. Es werden nicht alle Änderungsaufträge aufgeführt, insbesondere diejenigen nicht, denen keine Workflow-Aufgaben zugewiesen sind.

Feld	Anmerkungen
View_Change.*	Es werden alle Felder aufgeführt, die in der Ansicht „View_Change“ zuvor in diesem Dokument definiert wurden.
wf_id	wf.id: Eindeutige ID für einen Datensatz in der Tabelle "wf".
wf_persid	wf.persid: Eindeutige ID für diesen Datensatz in der Tabelle "wf", der die Objektkennung ("wf" für "wf") und ein Doppelpunkt vorangehen.
del	wf.del: Dies ist ein Boolescher Indikator. Gibt an, ob dieser Datensatz dem Anwender angezeigt werden soll.
object_type	wf.object_type: Factory-Name zur Angabe des Datensatztyps (z. B. "chg"), dem diese Workflow-Aufgabe zugewiesen ist.
object_id	wf.object_id: Eindeutige ID zur Angabe des Datensatzes, dem diese Workflow-Aufgabe zugewiesen ist. wf.object_id = chg.id
task	wf.task: ID zur Angabe des Aufgabentyps, den dieser Datensatz darstellt. wf.task = tsqty.code
wf_template	wf.wf_template: ID, die angibt, von welcher Vorlage dieser Workflow-Aufgaben-Datensatz erstellt wurde. wf.wf_template = wftpl.id
sequence	wf.sequence: Dies ist eine Ganzzahl, die die Reihenfolge angibt, in der dieser Workflow-Aufgaben-Datensatz von CA SDM angezeigt und ausgeführt werden soll (z. B. aufsteigend).
wf_status	wf.status: ID, die auf einen tsqty-Datensatz verweist, der den aktuellen Status dieser Workflow-Aufgabe angibt. wf.status = tsqty.code
group_task	wf.group_task: Boolescher Indikator, der angibt, ob diese Aufgabe zu einer Gruppe gehört.
asset	wf.asset: Binäre UUID, die auf einen Datensatz in der Tabelle "ca_owned_resource" verweist. wf.asset = ca_owned_resource.own_resource_uuid

Feld	Anmerkungen
creator	wf.creator: Binäre UUID, die auf einen Datensatz in der Tabelle "ca_contact" verweist. Gibt die Person an, die diese Workflow-Aufgabe erstellt hat. wf.creator = ca_contact.contact_uuid
date_created	wf.date_created: Zeitstempel (Datum/Uhrzeit), zu dem die Workflow-Aufgabe erstellt wurde (pdmtime).
wf_assignee	wf.assignee: Binäre UUID, die auf einen Datensatz in der Tabelle "ca_contact" verweist. Gibt die Person an, die dieser Workflow-Aufgabe derzeit zugewiesen ist. wf.assignee = ca_contact.contact_uuid
done_by	wf.done_by: Binäre UUID, die auf einen Datensatz in der Tabelle "ca_contact" verweist. Gibt die Person an, die diese Workflow-Aufgabe abgeschlossen oder genehmigt hat. wf.done_by = ca_contact.contact_uuid
wf_start_date	wf.start_date: Zeitstempel, zu dem die Workflow-Aufgabe in einen aktiven Status versetzt wurde (pdmtime).
wf_est_comp_date	wf.est_comp_date: Zeitstempel (pdmtime), zu dem die Aufgabe voraussichtlich abgeschlossen sein wird.
est_duration	wf.est_duration: Geschätzte Zeitdauer für diese Workflow-Aufgabe.
completion_date	wf.completion_dat: Zeitstempel (pdmtime), zu dem die Workflow-Aufgabe abgeschlossen wurde.
actual_duration	wf.actual_duration: Tatsächliche Zeitdauer, die der Abschluss dieser Workflow-Aufgabe in Anspruch genommen hat.
wf_est_cost	wf.est_cost: Dies sind die geschätzten Kosten für diese Workflow-Aufgabe.
cost	wf.cost: Dies sind die tatsächlichen Kosten, die der Abschluss dieser Workflow-Aufgabe in Anspruch genommen hat.
wf_description	wf.description: Beschreibung der Workflow-Aufgabe.
wf_last_mod_dt	wf.last_mod_dt: Zeitstempel (pdmtime), zu dem die Workflow-Aufgabe abgeschlossen wurde.
wf_last_mod_by	wf.last_mod_by: Eindeutige binäre UUID, die auf einen Datensatz in der Kontakttabelle verweist, der die Person angibt, die diese Workflow-Aufgabe zuletzt geändert hat. wf.last_mod_by = ca_contact.contact_uuid

View_Change_to_Properties

Diese Ansicht ist das Ergebnis der Verknüpfung der Ansicht „View_Change“ mit der Tabelle „Properties“ (prp), um eine grundlegende Ansicht von Änderungsaufträgen und ihren zugehörigen Eigenschaften zu liefern. Es werden nicht alle Änderungsaufträge aufgeführt, insbesondere diejenigen nicht, denen keine Eigenschaften zugewiesen sind.

Feld	Anmerkungen
View_Change.*	Es werden alle Felder aufgeführt, die in der Ansicht „View_Change“ zuvor in diesem Dokument definiert wurden.
prp_id	prp.id: Eindeutige ID in Form einer Ganzzahl für den Eigenschaftendatensatz.
prp_persid	prp.persid: Eindeutige ID für diesen Datensatz in der Tabelle "wf", der die Objektkennung ("prp" für "prp") und ein Doppelpunkt vorangehen.
object_type	prp.object_type: Factory-Name zur Angabe des Datensatztyps (z. B. chg), dem dieser Eigenschaftendatensatz zugewiesen ist.
object_id	prp.object_id: Eindeutige ID zur Angabe des Datensatzes, dem diese Eigenschaft zugewiesen ist. prp.object_id = chg.id
sequence	prp.sequence: Dies ist eine Ganzzahl, die die Reihenfolge angibt, in der dieser Eigenschaftendatensatz von CA SDM angezeigt werden soll (z. B. aufsteigend).
Eigenschaft	prp.property: ID, die auf einen Datensatz in der Tabelle "prptpl" verweist. Stellt die Vorlage dar, mit der diese Eigenschaft erstellt wurde. prp.property=prptpl.code
value	prp.value: Wert, der vom Anwender als Antwort auf die Felder "prp_description" und "prp.label" eingegeben wurde.
prp_last_mod_dt	prp.last_mod_dt: Zeitstempel (pdmtime), zu dem diese Eigenschaft zuletzt geändert wurde.
prp_last_mod_by	prp.last_mod_by: Binäre ID, die auf einen Datensatz in der Tabelle "ca_contact" verweist. Stellt die Person dar, die diesen Datensatz zuletzt geändert hat. prp.last_mod_by = ca_contact.contact_uuid
required	prp.required: Boolescher Indikator, der angibt, ob für diese Eigenschaft ein prp.value vorhanden sein muss, bevor der Datensatz gespeichert wird.
sample	prp.sample: Textfeld, das Beispielwerte anzeigt, um den Anwender bei der Eingabe eines sinnvollen Wertes in "prp.value" zu unterstützen.
prp_description	prp.description: Textfeld, das erklärt, welche Art von Wert in "prp.value" eingegeben werden sollte.

Feld	Anmerkungen
label	prp.label: Kurze Beschreibung zu dem Wert, der in das Feld "prp.value" einzugeben ist.

View_Contact_Full

Die folgenden Felder bilden eine grundlegende Ansicht aller Kontakte. Diese Ansicht führt alle Felder in der Tabelle „ca_contact“ auf, sowie referenzierte Felder wie zum Beispiel kurze Beschreibungen für Kontakttyp, Positionsname, Organisationsnamen und Diensttyp für jeden Kontakt. Sie wurde bereits mit den Tabellen „ca_location“, „ca_organization“, „srv_desc“ und „ca_contact_type“ verknüpft, um die tatsächlichen Namen und Symbole für einige der Felder in der Tabelle „ca_contact“ zu erhalten. Die tatsächlichen Namen und Symbole befinden sich am Ende der folgenden Liste der Felder in dieser Ansicht.

Feld	Anmerkung
contact_uuid	ca_contact.contact_uuid: Eindeutige binäre ID für jeden "ca_contact"-Datensatz
middle_name	ca_contact.middle_name: Zweiter Vorname für diesen Kontakt.
alias	ca_contact.alias: Alternativer, oft informeller Name für diesen Kontakt.
last_name	ca_contact.last_name: Der Nachname dieses Kontakts.
first_name	ca_contact.first_name: Der offizielle Vorname dieses Kontakts.
pri_phone_number	ca_contact.pri_phone_number: Die primäre Telefonnummer dieses Kontakts.
alt_phone_number	ca_contact.alt_phone_number: Die alternative Telefonnummer dieses Kontakts.
fax_number	ca_contact.fax_number: Die Faxnummer dieses Kontakts.
mobile_phone	ca_contact.mobile_phone: Die Mobiltelefonnummer dieses Kontakts.
pager_number	ca_contact.pager_number: Nummer zur Ausgabe einer Pager-Nachricht an den Kontakt.
email_address	ca_contact.email_address: Die E-Mail-Adresse des Kontakts.
location_uuid	ca_contact.location_uuid: Eindeutige binäre ID, die auf einen Datensatz in der Tabelle "ca_location" verweist, der die permanente Lokation des Kontakts angibt. ca_contact.location_uuid = ca_location.location_uuid
floor_location	ca_contact.floor_location: Die Nummer der Etage des Kontakts

Feld	Anmerkung
pager_email_address	ca_contact.pager_email_address: Die E-Mail-Adresse für den Pager eines Kontakts
room_location	ca_contact.room_location: Der Raum des Kontakts auf der Etage an der permanenten Lokation.
contact_type	ca_contact.contact_type: Eindeutige ID in Form einer Ganzzahl, die auf eine Zeile in der Tabelle "ca_contact_type" verweist, die die allgemeine Funktion dieses Kontakts innerhalb der Service Desk-Anwendung angibt. ca_contact.contact_type = ca_contact_type.id
inactive	ca_contact.inactive: Ein Boolescher Indikator für den Status dieses Datensatzes, der bestimmt, ob der Datensatz in Standardsuchen innerhalb von Service Desk einbezogen oder ausgeschlossen wird.
creation_user	ca_contact.creation_user: Anwender-ID des Kontakts, der diesen Datensatz erstellt hat. ca_contact.creation_user = ca_contact.userid
creation_date	ca_contact.creation_date: Zeitstempel (pdmtime), der das Datum und die Uhrzeit angibt, zu denen dieser Kontakt erstellt wurde.
last_update_user	ca_contact.last_update_user: Anwender-ID des Kontakts, der diesen Kontaktdatensatz zuletzt aktualisiert hat. ca_contact.last_update_user = ca_contact.userid
last_update_date	ca_contact.last_update_date: Zeitstempel (pdmtime), der das Datum und die Uhrzeit angibt, zu denen dieser Datensatz zuletzt geändert wurde.
version_number	ca_contact.version number: Die interne Versionsanzeige
Abteilung	ca_contact.department: Eindeutige ID in Form einer Ganzzahl, die auf eine Zeile in der Tabelle "ca_resource_department" verweist, die die Abteilung des Kontakts angibt. ca_contact.department = ca_resource_department.id
comment	ca_contact.comment: Formatfreies Textfeld für Kommentare, in dem Analysten wichtige Fakten dokumentieren können, die die Handhabung des betroffenen Kontakts beeinflussen.
company_uuid	ca_contact.company_uuid: Eindeutige binäre ID, die auf eine Zeile in der Tabelle "ca_company" verweist. Gibt die Zugehörigkeit dieses Kontakts zu einer Firma an. ca_contact.company_uuid = ca_company.company_uuid
organization_uuid	ca_contact.organization_uuid: Eindeutige binäre ID, die auf eine Zeile in der Tabelle "ca_organization" verweist. Gibt die Arbeitsorganisation dieses Kontakts an. ca_contact.organizaiton_uuid = ca_organization.organization_uuid

Feld	Anmerkung
admin_organization_uuid	ca_contact.admin_organization_uuid: Eindeutige binäre ID, die auf eine Zeile in der Tabelle "ca_organization" verweist. Gibt die administrative Organisation dieses Kontakts an. ca_contact.admin_organization_uuid = ca_organization.organization_uuid
alternate_identifizier	ca_contact.alternate_identifizier: Eine benutzerdefinierte ID, für gewöhnlich eine von der Personalabteilung verwendete Entität zur eindeutigen Bestimmung dieses Kontakts.
job_title	ca_contact.job_title: Eindeutige ID in Form einer Ganzzahl, die auf die Tabelle "ca_job_title" verweist. Gibt die standardisierte Position für diesen Kontakt an. ca_contact.job_title = ca_job_title.id
job_function	ca_contact.job_function: Eindeutige ID in Form einer Ganzzahl, die auf die Tabelle "ca_job_function" verweist. Gibt eine standardisierte allgemeine Beschreibung der Aufgabenfunktion des Kontakts an. ca_contact.job_function = ca_job_function.id
mail_stop	ca_contact.mail_stop: Mail Stop
cost_center	ca_contact.cost_center: Eindeutige ID in Form einer Ganzzahl, die auf die Tabelle "ca_resource_cost_center" verweist. Gibt die primäre Kostenstelle dieses Kontakts an. ca_contact.cost_center = ca_cost_center.id
userid	ca_contact.userid: Die Anwender-ID, mit der sich dieser Kontakt bei Service Desk anmeldet.
supervisor_contact_uuid	ca_contact.supervisor_contact_uuid: Eindeutige binäre ID, die auf eine Zeile in der Tabelle "ca_contact" verweist, die eine Hierarchie der Kontakte erstellt, um die Berichterstellungsstruktur für jeden Kontakt anzugeben. ca_contact.supervisor_contact_uuid = ca_contact.contact_uuid
exclude_registration	ca_contact.exclude_registration: Internes Flag für die Registrierung.
delete_time	ca_contact.delete_time: Zeitstempel, der angibt, wann das inaktive Flag auf 1 gesetzt wurde.
contact_type_name	ca_contact_type.name: Eine kurze Beschreibung von "ca_contact.contact_type" dieses Kontakts.
location_name	ca_location.name: Eine kurze Beschreibung der permanenten Lokation dieses Kontakts.
organization	ca_organization.org_name: Eine kurze Beschreibung von "ca_contact.organization_uuid" dieses Kontakts.

Feld	Anmerkung
admin_organization	ca_organization.org_name: Eine kurze Beschreibung von "ca_contact.organization_uuid" dieses Kontakts. ca_contact.admin_organization_uuid
service_type	srv_desc.sym: Eine kurze Beschreibung von "usp_contact.c_service_type" dieses Kontakts. ca_contact.contact_uuid = usp_contact.contact_uuid AND usp_contact.c_service_type = srv_desc.code
state_sym	ca_location.state: Eindeutige ID in Form einer Ganzzahl, die auf eine Zeile in der Tabelle "ca_state_province" verweist, die den Bundesstaat, die Provinz oder ein anderes frei definiertes geografisches Gebiet angibt. ca_contact.location_uuid = ca_location.location_uuid AND ca_location.state = ca_state_province.id

View_Contact_to_Environment

Die folgende Liste ist eine grundlegende Ansicht von Kontakten und deren Umgebung (Assets). Diese Ansicht ist eine Ansicht der Tabelle „contact“ (ca_contact); sie ist aber auch mit der Tabelle „owned resource“ (ca_owned_resource) verknüpft, um eine Liste aller mit einem Kontakt verbundenen Anlagen zu erhalten. Diese Ansicht kann mit der Ansicht „View_Contact_Full“ verknüpft werden, um den Kontakttyp, den Dienstyp, die Organisationen und die Position für jeden Kontakt zu erhalten. Alternativ kann diese Ansicht auch mit den einzelnen Tabellen verknüpft werden, um diese Informationen zu erhalten.

Feld	Anmerkungen
ca_contact.*	Die Felder "ca_contact", die in der Ansichtsdefinition "View_Contact_Full" festgelegt sind.
asset_uuid	ca_owned_resource.own_resource_uuid: Eine eindeutige binäre ID für ein Asset in der Tabelle "ca_owned_resource".
asset_name	ca_owned_resource.resource_name: Der festgelegte Netzwerkname dieses Assets.

View_Group

Die folgende Liste ist eine grundlegende Ansicht der Kontaktstabelle, die jedoch nur Gruppenkontakte aufführt. Die Kontakttyp-ID = 2308, die der Kontakttyp für Gruppen ist. Sie können diese Ansicht mit anderen CA SDM-Tabellen verknüpfen, um aussagefähigere Daten für die Berichterstellung zu erhalten. Zum Beispiel können Sie die Ansicht mit der Tabelle "Lokation" (ca_location) verknüpfen, um den tatsächlichen Namen und die Adresse für die Lokation der Gruppe zu finden. Außerdem können Sie diese Ansicht mit der Tabelle "Organisation" (ca_organization) verknüpfen, um die Namen der tatsächlichen funktionalen und administrativen Organisationen für die Gruppe zu erhalten.

Feld	Anmerkungen
ca_contact.*	Die Felder "ca_contact", die in der Ansichtsdefinition "View_Contact_Full" festgelegt sind.

Es folgt ein Beispiel für die Verknüpfung von Tabellen und für die Extraktion von Feldern für die Berichterstellung. Das Feld aus einer Tabelle (auf der rechten Seite) wird mit einem Feld aus einer anderen Tabelle (auf der linken Seite) verknüpft (->). Um korrekte Verbindungen zwischen Tabellen und Ansichten zu erstellen, müssen Sie die Unterschiede in den Verknüpfungen für die Datenbank verstehen. Das in Klammern angegebene Feld (siehe unten) können Sie, falls gewünscht, in Ihren Berichten verwenden, wenn die zuvor genannten Tabellen mit der Ansicht „View_Group“ verknüpft sind:

- View_Group.contact_type -> ca_contact_type.id (ca_contact_type.sym)
- View_Group.location_uuid -> ca_location.location_uuid
(ca_location.location_name)
- View_Group.organization_uuid -> ca_organization.organization_uuid
(ca_organization.org_name)
- View_Group.admin_organization_uuid -> ca_organization(2).organization_uuid
(ca_organization(2).org_name)

View_Group_to_Contact

Die folgende Liste ist eine grundlegende Ansicht aller Gruppenkontakte (Mitglieder). Sie schließt auch Manager mit ein. Hier ist „View_Group“ mit der Tabelle „Group_Member“ und dann mit der Tabelle „ca_contact“ verknüpft. Alle Felder in „View_Group“ werden aufgeführt sowie der Vorname, der zweite Vorname und der Nachname aus der Tabelle „ca_contact“. Das Manager-Kennzeichen von Group_Member wird ebenfalls aufgeführt. Das Manager-Kennzeichen des Gruppenmitglieds ist 1 oder 0; dies gibt an, dass das Mitglied entweder ein Manager (ja – 1) oder kein Manager (nein – 0) ist. Die meisten Informationen in dieser Ansicht beziehen sich auf die Gruppe und nicht auf die eigentlichen Mitglieder. Diese Ansicht wird verwendet, um Informationen über eine bestimmte Gruppe zu finden, einschließlich der Namen ihrer Mitglieder.

Feld	Anmerkungen
View_Group.*	Die Felder "View_Group", die in der Ansichtsdefinition "View_Group" festgelegt sind.
member_lastname	ca_contact.last_name: Der Nachname des Gruppenmitglieds
member_firstname	ca_contact.first_name: Der offizielle Vorname des Gruppenmitglieds
member_middlename	ca_contact.middle_name: Der zweite Vorname des Gruppenmitglieds
grpmem_manager_flag	ca_contact.manager_flag: Das Manager-Kennzeichen des Gruppenmitglieds (1 oder 0)

View_Issue

Dies ist eine grundlegende Ansicht aller Issues, die folgende Informationen enthält: Status, Priorität, Kategorie, Organisationen, vollständiger Name des Anforderers, vollständiger Name des Zuständigen, Gruppenname und ID usw. Hier ist die Tabelle "issue" mit vielen anderen Tabellen verknüpft, um einige aussagefähigere Daten zum Issue zu liefern.

Feld	Anmerkungen
ID	issue.id: Die eindeutige ID für diesen Datensatz in der Tabelle "issue".
persid	issue.persid: Die eindeutige ID für diesen Datensatz in der Tabelle "issue", der die Objekt-ID (iss für die Problemanfragentabelle) und ein Doppelpunkt vorangeht.
issue_ref_num	issue.iss_ref_num: Problemanfrage-Referenznummer, die von Analytikern und Kunden verwendet wird, um sich auf eine bestimmte Problemanfrage zu beziehen.

Feld	Anmerkungen
description	issue.description: Eine lange Beschreibung einer Problemanfrage, die von einem Analytiker oder Kunden angegeben wurde.
status	issue.status: Eindeutige ID eines Problemanfragestatus, die auf die Tabelle "issstat" verweist. issue.status = issstat.code
active_flag	issue.active_flag: Ganzzahl-Markierung, um zu bestimmen, ob diese Problemanfrage aktiv ist oder nicht (1 oder 0).
start_date	issue.start_date: Das Datum, das die erste Aufgabe zu einem unentschiedenen <A[Status Lage Stand]> geht (pdmtime).
open_date	issue.open_date: Erstellungsdatum der Problemanfrage (pdmtime).
last_mod_dt	issue.last_mod_dt: Datum der letzten Änderung (pdmtime).
last_mod_by	issue.last_mod_by: Der Zeiger auf das Kontakt-UUID, das den letzten Kontakt anzeigt, um diesen Issue zu ändern. issue.last_mod_by = ca_contact.contact_uuid
close_date	issue.close_date: Datum, an dem die Problemanfrage auf inaktiv eingestellt wurde (pdmtime).
resolve_date	issue.resolve_date: Datum, an dem die Problemanfrage auf einen Status eingestellt wurde, der konfiguriert wurde, um die Lösung der Problemanfrage anzugeben (pdmtime).
rootcause	issue.rootcause: Ein Zeiger auf einen Datensatz in der Tabelle "rootcause", der die ursprüngliche Situation angibt, die die Protokollierung dieser Problemanfrage veranlasste. issue.rootcause = rootcause.id
est_total_time	issue.est_total_time: Geschätzte Gesamtzeit (pdmtime) für die Durchführung dieser Problemanfrage.
actual_total_time	issue.actual_total_time: Tatsächliche Gesamtzeit (pdmtime) für die Durchführung dieser Problemanfrage.
log_agent	issue.log_agent: Ein binärwertiges eindeutiges Kennzeichen; referiert die Tabelle "ca_contact", die wiederum auf die Person verweist, die der ursprüngliche Ersteller des Issues war. issue.log_agent = ca_contact.contact_uuid
Verantwortlicher	issue.assignee: Ein Zeiger auf das Kontakt-UUID, die gegenwärtig dem Änderungsauftrag zugewiesen wird. issue.assignee = ca_contact.contact_uuid
organization	issue.organization: Ein Zeiger auf die interne Organisations-UUID, die die Organisation repräsentiert, der dieser Issue gehört. issue.organization = ca_organization.organization_uuid

Feld	Anmerkungen
group_id	issue.group_id: Ein Zeiger auf die Kontakt-UUID, die die Gruppe repräsentiert, die dem Issue aktuell zugewiesen ist. issue.group_id = ca_contact.contact_uuid
affected_contact	issue.affected_contact: Ein Zeiger auf die Kontakt-UUID, die den Kontakt repräsentiert, der von dem Issue betroffen ist. issue.affected_contact = ca_contact.contact_uuid
requestor	issue.requestor: Zeiger auf die Kontakt-UUID, die die Person darstellt, die die Protokollierung dieser Problemanfrage angefordert hat. issue.requestor = ca_contact.contact_uuid
category	issue.category: Zeiger auf den Problemanfragen-Kategoriecode; verweist auf die Kategorie, in die diese Problemanfrage fällt. issue.category = isscat.code
priority	issue.priority: Zeiger auf die Aufzählung "priority", die die Priorität darstellt, in die diese Problemanfrage fällt. issue.priority = pri.enum
need_by	issue.need_by: Datum, das angibt, wann der betroffene Endanwender (affected_end_user) die Problemanfrage abgeschlossen haben muss (pdmtime).
est_comp_date	issue.est_comp_date: Geschätztes Abschlussdatum (pdmtime) für diese Problemanfrage.
actual_comp_date	issue.actual_comp_date: Tatsächliches Abschlussdatum (pdmtime) dieser Problemanfrage.
est_cost	issue.est_cost: Geschätzte Kosten dieser Problemanfrage.
actual_cost	issue.actual_cost: Tatsächliche Kosten für die Implementierung dieser Problemanfrage.
justification	issue.justification: Ein Textfeld, in dem der Anforderer die Gründe angeben kann, aus denen diese Problemanfrage erforderlich wurde.
backout_plan	issue.backout_plan - Ein Textfeld, in dem ein Analyst einen Alternativplan für diesen Issue angeben kann.
impact	issue.impact - Ein Zeiger auf einen Datensatz in der Tabelle 'impact', der den Umfang der Ressourcen angibt, die von diesem Issue betroffen sind. issue.impact = impact.enum
parent	issue.parent - Ein Zeiger auf eine andere Issue-ID, die die Erstellung einer Hierarchie von Issues ermöglicht. issue.parent = issue.id
effort	issue.effort - Ein Textfeld, in dem der Plan für die Implementierung dieses Issues erläutert wird.

Feld	Anmerkungen
support_lev	issue.support_lev - Zeiger auf einen Service-Beschreibungsdatensatz, der einige Bedingungen automatisiert, unter denen dieser Issue abgeschlossen werden muss. issue.support_lev = srv_desc.code
template_name	issue.template_name: Der Name des Issues und Zeiger auf eine Issue-Vorlage. issue.template_name = iss_template.template_name
sla_violation	issue.sla_violation - Ganzzahl zur Angabe der Häufigkeit, in der mit diesem Issue verbundene SLAs verletzt wurden.
predicted_sla_viol	issue.predicted_sla_viol - (r5.5) Auf Neugent-Technologie bezogenes Feld.
macro_predict_viol	issue.macro_predict_viol - (r5.5) Auf Neugent-Technologie bezogenes Feld.
created_via	issue.created_via: Ein Zeiger auf einen Datensatz in der Schnittstellentabelle. Gibt an, von welcher Schnittstelle der Issue stammt. call_req.created_via = interface.id
call_back_date	issue.call_back_date - Ein Datums-/Zeitfeld (pdmtime), das ein zukünftiges Datum/eine zukünftige Zeit angibt, zu dem/der der Anforderer kontaktiert werden soll.
call_back_flag	issue.call_back_flag - Ein boolescher Indikator, der dem Anwender als Kontrollkästchen angezeigt wird und der angibt, ob der Analyst am issue.call_back_date benachrichtigt werden soll.
string1	Dieses Textfeld ist anwenderdefinierbar.
string2	Dieses Textfeld ist anwenderdefinierbar.
string3	Dieses Textfeld ist anwenderdefinierbar.
string4	Dieses Textfeld ist anwenderdefinierbar.
string5	Dieses Textfeld ist anwenderdefinierbar.
string6	Dieses Textfeld ist anwenderdefinierbar.
service_date	issue.service_date - Datum/Uhrzeit (pdmtime), zu dem/der vom externen Anbieter die Bearbeitung dieser Issue erwartet wird.
service_num	issue.service_num - Textfeld zur Angabe der Service- oder Bestellnummer eines externen Anbieters.
Produkt	issue.product - Zeiger auf einen Datensatz in der Produkttabelle, der das von diesem Issue betroffene Produkt angibt. issue.product = product.id
Aktionen	issue.actions - Großes Textfeld zur Angabe von Aktionen.

Feld	Anmerkungen
type_of_contact	issue.type_of_contact - Zeiger auf einen Datensatz in der Inhaltsverzeichnisstabelle 'toc', der die allgemeine Kategorie des betroffenen Endanwenders (affected_end_user) für den Issue angibt. issue.type_of_contact = toc.id
reporting_method	issue.reporting_method - Zeiger auf einen Datensatz in der Tabelle 'repmeth', der die Herkunft des Issues angibt und von der Person ausgewählt wird, die den Issue erstellt. issue.reporting_method = repmeth.id
person_contacting	issue.person_contacting - Zeiger auf einen Datensatz in der Tabelle 'perscon', der die Rolle des affected_end_user oder des Anforderers angibt. issue.person_contacting = perscon.id
status_name	issstat.sym: Beschreibung des Status aus Anwendersicht. issue.status = issstat.code
priority_num	pri.sym: Beschreibung der Priorität aus Anwendersicht. issue.priority = pri.enum
category_name	isscat.sym: Der Name der Issue-Kategorie, der einem Anwender angezeigt wird. issue.category = isscat.code
organization_name	ca_organization.org_name: Name der Organisation, der Anwendern angezeigt wird. issue.organization = ca_organization.organization_uuid
affected_end_user_lastname	ca_contact.last_name: Der Nachname des betroffenen Endanwenders. issue.affected_end_user = ca_contact.contact_uuid
affected_end_user_firstname	ca_contact.first_name: Der Vorname des betroffenen Endanwenders. issue.affected_end_user = ca_contact.contact_uuid
affected_end_user_middlename	ca_contact.middle_name: Der zweite Vorname des betroffenen Endanwenders. issue.affected_end_user = ca_contact.contact_uuid
assignee_lastname	ca_contact.last_name: Nachname des Zuständigen. issue.assignee = ca_contact.contact_uuid
assignee_firstname	ca_contact.first_name: Vorname des Zuständigen. issue.assignee = ca_contact.contact_uuid
assignee_middlename	ca_contact.middle_name: Zweiter Vorname des Zuständigen. issue.assignee = ca_contact.contact_uuid
groupid	View_Group.contact_uuid: Eine binäre Darstellung der internen ID, die für die diesem Issue zugewiesene Gruppe verwendet wird. issue.group_id = ca_contact.contact_uuid
group_name	View_Group.last_name: Der Name der diesem Issue zugewiesenen Gruppe. issue.group = ca_contact.contact_uuid

Feld	Anmerkungen
service_type	srv_desc.sym: Der Name des Servicetyps, der auf diesen Issue angewendet wird. issue.support_lev = srv_desc.code
impact_num	impact.sym: Beschreibung der Auswirkung, die Anwendern angezeigt wird. issue.impact = impact.enum
product_sym	product.sym: Produktbeschreibung, die Anwendern angezeigt wird. issue.product = product.id
type_of_contact_sym	toc.sym: Beschreibung des Kontakttyps, die Anwendern angezeigt wird. issue.type_of_contact = toc.id
rpting_method_sym	repmeth.sym: Beschreibung der Berichtsmethode, die Anwendern angezeigt wird. issue.reporting_method = repmeth.id
person_contacting_sym	perscon.sym: Beschreibung der Kontakt aufnehmenden Person, die Anwendern angezeigt wird. issue.person_contacting = perscon.id
created_via_sym	interface.sym: issue.created_via = interface.id.
rootcause_sym	rootcause.sym: issue.rootcause = rootcause.id.

View_Issue_Act_Log

Dies ist eine Standardansicht aller Aktivitätsprotokolle für Issues. Es handelt sich um eine Ansicht der Tabelle „issue activity log“ (issalg), verknüpft mit der Tabelle „activity type“ (act_type) und der Tabelle „contact“ (ca_contact), um aussagefähigere Daten zu liefern, wie zum Beispiel den tatsächlichen Aktivitätstyp und den vollständigen Namen des Analytikers, der die Aktivität durchgeführt hat.

Feld	Anmerkungen
ID	issalg.id: Die eindeutige Kennung für diesen Datensatz in der Tabelle "issalg".
persid	issalg.persid: Die eindeutige Kennung für diesen Datensatz in der Tabelle "issalg", der die Objektkennung ("issalg" für "issalg") und ein Doppelpunkt vorangehen.
issue_id	issalg.issue_id: Zeiger zur Issue-Kennung, zu der diese Aktivität gehört. issalg.issue_id = issalg.id
last_mod_dt	issalg.last_mod_dt: Letztes Änderungsdatum/Änderungszeit (pdmtime).
time_spent	issalg.time_spent: Für diese Aktivität benötigte Dauer, als Gesamtzahl von Sekunden gespeichert. Zum Beispiel 80 = 1 Minute, 20 Sekunden.

Feld	Anmerkungen
time_stamp	issalg.time_stamp: Benutzerdefinierbare Datum-/Zeitangaben einer Aktivität (pdmtime).
system_time	issalg.system_time: Datum/Zeit der Datensatzerstellung (pdmtime).
analyst	issalg.analyst: Eine eindeutige binäre ID, die auf die Kontakt-UUID verweist, um den Analysten zu finden, der die Aktivität durchgeführt hat. issalg.analyst = ca_contact.contact_uuid
description	issalg.description: Textbeschreibung dieser Aktivität, die vom Anwender geändert werden kann.
action_desc	issalg.action_desc: Textbeschreibung einer automatisierten Aktion, die vom Anwender nicht geändert werden kann.
type	issalg.type: Textzeiger zu einem Datensatz in der Aktivitätstyp-Tabelle. issalg.type = act_type.code
internal	issalg.internal: Ganzzahl-Flag (1 oder 0), das angibt, ob dieser Protokolleintrag von allen Anwendern angezeigt werden kann oder nur für die interne Verwendung bestimmt ist.
knowledge_session	issalg.knowledge_session: Kennung für eine bestimmte Sitzung eines bestimmten Anwenders.
knowledge_tool	issalg.knowledge_tool: Ein Indikator des Knowledge Tools, der für die Suche verwendet wird, z. B. NLS_FAQ oder EXPERT usw.
analyst_lastname	View_Contact_Full.last_name: Der Nachname des Analysten, abgeleitet von "issalg.analyst = ca_contact.contact_uuid".
analyst_firstname	View_Contact_Full.first_name: Vorname des Analysten.
analyst_middlename	View_Contact_Full.middle_name: Zweiter Vorname des Analysten.
activity_type	act_type.sym: Aktivitätstyp, referenziert durch issalg.type = act_type.code.

View_Issue_to_Assets

Die folgende Liste ist eine grundlegende Ansicht von Issues und ihren Assets. Die Tabelle "issue" (issue) wird indirekt mit der Tabelle "owned resource" (ca_owned_resource) und anderen anlagenspezifischen Tabellen verknüpft, um eine Liste der Anlagen für jedes Issue zu erhalten. Es werden nicht alle Issues aufgeführt, insbesondere diejenigen nicht, die keine Anlagen besitzen.

Feld	Anmerkungen
View_Issue.*	Die Ansicht "View_Issue", die alle Felder definiert, die in der Ansicht "View_Issue" erscheinen.

Feld	Anmerkungen
assetID	ca_owned_resource.own_resource_uuid: Binäres Feld, das als interne, unveränderliche und eindeutige Kennung eines Anlagendatensatzes dient.
asset_serial_num	ca_owned_resource.serial_number: Seriennummer eines Anlagendatensatzes.
asset_class	ca_resource_class.name: Kurze Beschreibung der Klasse, zu der eine Anlage gehört. ca_owned_resource.resource_class = ca_resource_class.id
asset_family	ca_resource_family.name: Anlagenfamilie, zu der die Anlage gehört. ca_owned_resource.resource_class = ca_resource_class.id AND ca_resource_class.family_id = ca_resource_family.id
asset_name	ca_owned_resource.resource_name: Netzwerkname, unter dem die Anlage läuft.

View_Issue_to_Issue_Act_Log

Dies ist eine grundlegende Ansicht aller Issues und der zugehörigen Aktivitätsprotokolle. Diese Ansicht verknüpft die Ansicht "View_Issue" mit der Ansicht "View_Issue_Act_Log", um ausführliche Informationen über Issues und ihre Aktivitätsprotokolle zu liefern. Die tatsächlichen Daten befinden sich am Ende der Liste der Felder.

Feld	Anmerkungen
View_Issue.*	Siehe Ansicht „View_Issue“, die weiter oben in diesem Dokument beschrieben wurde
issalg_id	issalg.id: Die eindeutige Kennung für diesen Datensatz in der Tabelle "issalg".
issalg_persid	issalg.persid: Die eindeutige Kennung für diesen Datensatz in der Tabelle "issalg", der die Objektkennung ("issalg" für "issalg") und ein Doppelpunkt vorangehen.
issue_id	issalg.issue_id: Zeiger zur Issue-Kennung, zu der diese Aktivität gehört. issalg.issue_id = issalg.id
issalg_last_mod_dt	issalg.last_mod_dt: Letztes Änderungsdatum/Änderungszeit (pdmtime).
time_spent	issalg.time_spent: Für diese Aktivität benötigte Dauer, als Gesamtzahl von Sekunden gespeichert. Zum Beispiel 80 = 1 Minute, 20 Sekunden.

Feld	Anmerkungen
time_stamp	issalg.time_stamp: Benutzerdefinierbare Datum-/Zeitangaben einer Aktivität (pdmtime).
system_time	issalg.system_time: Datum/Zeit der Datensatzerstellung (pdmtime).
analyst	issalg.analyst: Eindeutiger binärer Zeiger zur Kontakt-UUID, um den Analysten zu finden, der die Aktivität durchgeführt hat. issalg.analyst = ca_contact.contact_uuid
issalg_description	issalg.description: Textbeschreibung dieser Aktivität, die vom Anwender geändert werden kann.
action_desc	issalg.action_desc: Textbeschreibung einer automatisierten Aktion, die vom Anwender nicht geändert werden kann.
type	issalg.type: Textzeiger zu einem Datensatz in der Aktivitätstyp-Tabelle. issalg.type = act_type.code
internal	issalg.internal: Ganzzahl-Flag (1 oder 0), das angibt, ob dieser Protokolleintrag von allen Anwendern angezeigt werden kann oder nur für die interne Verwendung bestimmt ist.
knowledge_session	issalg.knowledge_session: Kennung für eine bestimmte Sitzung eines bestimmten Anwenders.
knowledge_tool	issalg.knowledge_tool: Ein Indikator des Knowledge Tools, der für die Suche verwendet wird, z. B. NLS_FAQ oder EXPERT usw.
issalg_analyst_id	issalg.analyst: Eindeutiger binärer Zeiger zur Kontakt-UUID, um den Analysten zu finden, der die Aktivität durchgeführt hat. issalg.analyst = ca_contact.contact_uuid

View_Change_to_Request

Dies ist eine grundlegende Ansicht von Changes, denen nur Anfragen zugewiesen sind. Diese Ansicht ist das Ergebnis der Verknüpfung der Ansicht "View_Change" mit der Tabelle "request" (call_req), um Einzelheiten zum Change und der ihm zugewiesenen Anfrage zu liefern.

Feld	Anmerkungen
View_Change.*	Es werden alle Felder aufgeführt, die in der Ansicht „View_Change“ zuvor in diesem Dokument definiert wurden.
cr_id	call_req.id: Eindeutige Kennung für diesen Datensatz in der Tabelle "call_req".
ref_num	call_req.ref_num: Anfragereferenznummer, die von Analysten und Kunden verwendet wird, um sich auf eine bestimmte Anfrage zu beziehen.
cr_summary	call_req.summary: Kurze Beschreibung der Anfrage als Ad-hoc-Referenz.
cr_persid	call_req.persid: Eindeutige Kennung für diesen Datensatz in der Tabelle "call_req", der die Objektkennung ("cr" für Tabelle "call_req") und ein Doppelpunkt vorangehen.
cr_description	call_req.description: Lange Beschreibung einer Anfrage, die von einem Analysten oder einem Kunden angegeben wurde.
cr_status	call_req.status: Eindeutige Kennung, die auf einen Datensatz in der Tabelle "cr_stat" verweist. Gibt den Status dieser Anfrage an: call_req.status = cr_stat.code
cr_active_flag	call_req.active_flag: Ganzzahl-Flag, um zu bestimmen, ob dieser Anforderungsdatensatz aktiv ist oder nicht (1 oder 0).
time_spent_sum	call_req.time_spent_sum: Die abgeleitete Summe der Felder "time_spent" aller act_log-Datensätze, gespeichert in Sekunden (d.h. 80 = 1 Minute 20 Sekunden).
cr_open_date	call_req.open_date: Zeitstempel, zu dem die Anfrage erstellt wurde (pdmtime).
cr_last_mod_dt	call_req.last_mod_dt: Zeitstempel, zu dem die letzte Änderung vorgenommen wurde (pdmtime).
cr_close_date	call_req.close_date: Zeitstempel, zu dem die Anfrage auf inaktiv gestellt wurde (pdmtime).
cr_log_agent	call_req.log_agent: Eindeutige binäre ID, die auf einen Datensatz in der Tabelle "ca_contact" verweist. Verweist auf die Person, die die Anfrage ursprünglich erstellt hat. call_req.log_agent = ca_contact.contact_uuid
cr_group_id	call_req.group_id: Eindeutige binäre ID, die auf einen Datensatz in der Tabelle "ca_contact" verweist. Stellt die Gruppe dar, die der Anfrage gegenwärtig zugewiesen ist. call_req.group_id = ca_contact.contact_uuid
cr_assignee	call_req.assignee: Eindeutige binäre ID, die auf einen Datensatz in der Tabelle "ca_contact" verweist. Stellt die Person dar, die der Anfrage gegenwärtig zugewiesen ist. call_req.assignee = ca_contact.contact_uuid

Feld	Anmerkungen
customer	call_req.customer: Eindeutige binäre ID, die auf einen Datensatz in der Tabelle "ca_contact" verweist. Stellt den betroffenen Endanwender für diese Anfrage dar. call_req.customer = ca_contact.contact_uuid
charge_back_id	charge_back_id: Textfeld, das als Buchhaltungsindikator verwendet wird, um die Kosten für diese Anfrage der entsprechenden Kostenstelle zuzuweisen.
affected_rc	call_req.affected_rc: Eindeutige binäre ID, die auf eine Zeile in der Tabelle "ca_owned_resource" verweist. Stellt das Asset dar, für das diese Anfrage gilt. call_req.affected_rc = ca_owned_resource.own_resource_uuid.
cr_support_lev	call_req.support_lev: Zeiger auf einen Service Desk-Datensatz, der einige Bedingungen automatisiert, unter denen diese Anfrage erledigt werden muss. call_req.support_lev = srv_desc.code
cr_category	call_req.category: Eindeutige Kennung, die auf einen Datensatz in der Tabelle "prob_ctg" verweist. Stellt die Kategorie dar, zu der diese Anfrage gehört. call_req.category = prob_ctg.persid
solution	call_req.solution: Zeiger zum Abrufen einer Lösung. call_req.solution = crsol.persid
cr_impact	call_req.impact: Eindeutige ID in Form einer Ganzzahl, die auf eine Zeile in der Tabelle "impact" verweist. Gibt den Umfang dieser Anfrage an. call_req.impact = impact.enum
cr_priority	call_req.priority: Eindeutige ID in Form einer Ganzzahl, die auf einen Datensatz in der Tabelle "pri" verweist. Gibt an, mit welcher Priorität die Analysten an dieser Anfrage arbeiten werden. call_req.priority = pri.enum
urgency	call_req.urgency: Eindeutige ID in Form einer Ganzzahl, die auf eine Zeile in der Tabelle "urgncy" verweist. Gibt die Lösungsdringlichkeit für diese Anfrage (nach Einschätzung des Anwenders) an. call_req.urgency = urgency.enum
severity	call_req.severity: Eindeutige ID in Form einer Ganzzahl, die auf eine Zeile in der Tabelle "severity" verweist. Gibt den Schweregrad der Konsequenzen für diese ungelöste Anfrage an. call_req.severity = severity.enum
extern_ref	Gibt ein zugeordnetes Ticket an.
last_act_id	ID der letzten Aktivität.
cr_ticket	Zeiger auf ein Trouble Ticket, um das zugeordnete Ticket zu ermitteln.
cr_parent	call_req.parent: PersID-Zeiger auf eine andere PersID einer Anfrage, was das Erstellen einer Change-Hierarchie erleichtert. call_req.parent = call_req.persid

Feld	Anmerkungen
cr_template_name	call_req.template_name: Textwert für den Verwendungszweck der Anfrage. Er kann aus einer Liste ausgewählt werden und dient als Vorlage für ähnliche Anfragen. cr_template.template = call_req.persid
cr_sla_violation	call_req.sla_violation: Eine Ganzzahl mit der ausgedrückt wird, wie oft mit dieser Anforderung verknüpfte SLAs verletzt wurden.
cr_predicted_sla_viol	call_req.predicted_sla_viol: (r5.5) Auf Neugent-Technologie bezogenes Feld
cr_created_via	call_req.created_via: Ein Ganzzahl-Zeiger auf einen Datensatz in der Tabelle "interface". Gibt an, von welcher Schnittstelle der Change stammt. call_req.created_via = interface.id
cr_call_back_date	call_req.call_back_date: Ein Zeitstempelfeld (pdmtime) das ein zukünftiges Datum/eine zukünftige Zeit anzeigt, in der der betroffene Endanwender (affected_end_user) kontaktiert werden soll.
cr_call_back_flag	call_req.call_back_flag: Boolescher Indikator, der dem Anwender als Kontrollkästchen angezeigt wird und der angibt, ob der Analyst zum Datum "call_req.call_back_date" benachrichtigt werden soll.
event_token	call_req.event_token: Wird von CA NSM für übereinstimmende Nachrichten verwendet.
type	call_req.type: Textfeld, das auf einen Datensatz in der Tabelle "crt" verweist. Gibt den ITIL-Typ dieser Anfrage an. call_req.type = crt.code
cr_string1	Benutzerdefinierbare Zeichenfolge.
cr_string2	Benutzerdefinierbare Zeichenfolge.
cr_string3	Benutzerdefinierbare Zeichenfolge.
cr_string4	Benutzerdefinierbare Zeichenfolge.
cr_string5	Benutzerdefinierbare Zeichenfolge.
cr_string6	Benutzerdefinierbare Zeichenfolge.
Änderung	call_req.change: Eindeutige ID in Form einer Ganzzahl, die auf eine Zeile in der Tabelle "chg" verweist. Gibt den Change an, der aufgrund dieser Anfrage erstellt wurde. call_req.change = chg.id.

View_Issue_to_Issue_WF

Diese Ansicht ist das Ergebnis der Verknüpfung der Ansicht „View_Issue“ mit der Tabelle „workflow task“ (isswf), um eine grundlegende Ansicht von Problemanfragen und ihren Workflow-Aufgaben zu liefern. Es werden nicht alle Problemanfragen aufgeführt, insbesondere, wenn ihnen keine Workflow-Aufgaben zugewiesen sind.

Feld	Anmerkungen
View_Issue.*	Eine Beschreibung zu jedem Feld finden Sie weiter oben in diesem Dokument in der Definition „View_Issue“.
wf_id	isswf.id: Eindeutige ID, die auf einen Datensatz in der Tabelle "isswf" verweist.
wf_persid	isswf.persid: Eindeutige ID für diesen Datensatz in der Tabelle "isswf", der die Objektkennung ("isswf") und ein Doppelpunkt vorangehen.
del	isswf.del: Boolescher Indikator, der angibt, ob dieser Datensatz dem Anwender angezeigt werden soll.
object_type	isswf.object_type: Factory-Name zur Angabe des Datensatztyps (z. B. iss), dem diese Workflow-Aufgabe zugewiesen ist.
object_id	isswf.object_id: Eindeutige ID zur Angabe des Datensatzes, dem diese Workflow-Aufgabe zugewiesen ist. isswf.object_id = issue.id
task	isswf.task: ID zur Angabe des Aufgabentyps, den dieser Datensatz darstellt. isswf.task = tsqty.code
wf_template	isswf.wf_template: ID, die angibt, von welcher Vorlage dieser Workflow-Aufgaben-Datensatz erstellt wurde. isswf.wf_template = wftpl.id
sequence	isswf.sequence: Die ist eine Ganzzahl, die die Reihenfolge angibt, in der dieser Workflow-Aufgaben-Datensatz von CA SDM angezeigt und ausgeführt werden soll (z. B. aufsteigend).
wf_status	isswf.status: ID, die auf den Datensatz "tskstat" verweist. Gibt den aktuellen Status dieser Workflow-Aufgabe an. isswf.status = tskstat.code
group_task	isswf.group_task: Boolescher Indikator, der angibt, ob diese Aufgabe zu einer Gruppe gehört.
asset	isswf.asset: Binäre UUID, die auf einen Datensatz in der Tabelle "ca_owned_resource" verweist. isswf.asset = ca_owned_resource.own_resource_uuid
creator	isswf.creator: Binäre UUID, die auf einen Datensatz in der Tabelle "ca_contact" verweist. Gibt die Person an, die diese Workflow-Aufgabe erstellt hat. isswf.creator = ca_contact.contact_uuid

Feld	Anmerkungen
date_created	isswf.date_created: Zeitstempel (Datum/Uhrzeit), zu dem die Workflow-Aufgabe erstellt wurde (pdmtime).
wf_assignee	isswf.assignee: Binäre UUID, die auf einen Datensatz in der Tabelle "ca_contact" verweist. Gibt die Person an, die dieser Workflow-Aufgabe derzeit zugewiesen ist. isswf.assignee = ca_contact.contact_uuid
done_by	isswf.done_by: Binäre UUID, die auf einen Datensatz in der Tabelle "ca_contact" verweist. Gibt die Person an, die diese Workflow-Aufgabe abgeschlossen oder genehmigt hat. isswf.done_by = ca_contact.contact_uuid
wf_start_date	wf_start_date: Zeitstempel, zu dem die Workflow-Aufgabe in einen aktiven Status versetzt wurde (pdmtime).
wf_est_comp_date	isswf.est_comp_date: Zeitstempel (pdmtime), zu dem die Aufgabe voraussichtlich abgeschlossen sein wird.
est_duration	isswf.est_duration: Geschätzte Zeitdauer für diese Workflow-Aufgabe.
completion_date	isswf.completion_date: Zeitstempel (pdmtime), zu dem die Workflow-Aufgabe abgeschlossen wurde.
actual_duration	isswf.actual_duration: Tatsächliche Zeitdauer, die der Abschluss dieser Workflow-Aufgabe in Anspruch genommen hat.
wf_est_cost	isswf.est_cost: Dies sind die geschätzten Kosten für diese Workflow-Aufgabe.
cost	isswf.cost: Dies sind die tatsächlichen Kosten, die der Abschluss dieser Workflow-Aufgabe in Anspruch genommen hat.
wf_description	isswf.description: Beschreibung der Workflow-Aufgabe.

Feld	Anmerkungen
wf_last_mod_dt	isswf.last_mod_dt: Zeitstempel (pdmtime), zu dem die Workflow-Aufgabe abgeschlossen wurde.
wf_last_mod_by	isswf.last_mod_by: Eindeutige binäre ID, die auf einen Datensatz in der Tabelle "contact" verweist. Gibt die Person an, die diese Workflow-Aufgabe zuletzt geändert hat. isswf.last_mod_by = ca_contact.contact_uuid

View_Issue_to_Properties

Diese Ansicht ist das Ergebnis der Verknüpfung der Ansicht „View_Issue“ mit der Tabelle „issue properties“ (issprp), um eine grundlegende Ansicht von Problemanfragen und ihren zugehörigen Eigenschaften zu liefern. Es werden nicht alle Problemanfragen aufgeführt, insbesondere, wenn ihnen keine Eigenschaften zugewiesen sind.

Feld	Anmerkungen
View_Issue.*	Eine Beschreibung zu jedem Feld finden Sie weiter oben in diesem Dokument in der View_Issue-Definition.
prp_id	issprp.id: Eindeutige ID in Form einer Ganzzahl für den Eigenschaftendatensatz.
prp_persid	issprp.persid: Eindeutige ID für diesen Datensatz in der Tabelle "prp", der die Objektkennung ("prp") und ein Doppelpunkt vorangehen.
sequence	issprp.sequence: Dies ist eine Ganzzahl, die die Reihenfolge angibt, in der dieser Eigenschaftendatensatz von CA SDM angezeigt werden soll (z. B. aufsteigend).
label	issprp.label: Kurze Beschreibung zu dem Wert, der in das Feld "issprp.value" einzugeben ist.
value	issprp.value: Wert, der vom Anwender als Antwort auf die Felder "prp_description" und "issprp.label" eingegeben wurde.
prp_last_mod_dt	issprp.last_mod_dt: Zeitstempel (pdmtime), zu dem diese Eigenschaft zuletzt geändert wurde.
prp_last_mod_by	issprp.last_mod_by: Binäre ID, die auf einen Datensatz in der Tabelle "ca_contact" verweist. Stellt die Person dar, die diesen Datensatz zuletzt geändert hat. issprp.last_mod_by = ca_contact.contact_uuid
required	issprp.required: Boolescher Indikator, der angibt, ob für diese Eigenschaft ein "prp.value" vorhanden sein muss, bevor der Datensatz gespeichert wird.
sample	issprp.sample: Textfeld, das Beispielwerte anzeigt, um den Anwender bei der Eingabe eines sinnvollen Wertes in "issprp.value" zu unterstützen.

Feld	Anmerkungen
owning_iss	issprp.owning_iss: Eindeutige ID zur Angabe des Datensatzes, dem diese Eigenschaft zugewiesen ist. issprp.object_id = issue.persid
prp_description	issprp.description: Textfeld, das erklärt, welche Art von Wert in issprp.value eingegeben werden sollte.

View_Request

Dies ist eine grundlegende Ansicht aller Anforderungen. Hier wurde die Tabelle "Request" mit anderen CA SDM-Tabellen verknüpft, um weitere spezielle Informationen zu liefern, wie zum Beispiel Anforderungsdiensttyp, Schweregrad, Dringlichkeit, Kategorie und Priorität. Außerdem werden einige weitere Informationen zur Anforderung aufgeführt. Alle Felder der Tabelle „Request“ (call_req) werden ausgewählt. Die extrahierten Felder, die das Ergebnis der verknüpften Tabellen sind, werden am Ende dieser Liste der Felder aufgeführt.

Feld	Anmerkungen
ID	call_req.id: Eindeutige Kennung für diesen Datensatz in der Tabelle "call_req".
persid	call_req.persid: Eindeutige Kennung für diesen Datensatz in der Tabelle "call_req", der die Objektkennung ("cr" für Tabelle "call_req") und ein Doppelpunkt vorangehen.
ref_num	call_req.ref_num: Anfragereferenznummer, die von Analysten und Kunden verwendet wird, um sich auf eine bestimmte Anfrage zu beziehen.
summary	call_req.summary: Kurze Beschreibung der Anfrage als Ad-hoc-Referenz.
description	call_req.description: Lange Beschreibung einer Anfrage, die von einem Analysten oder einem Kunden angegeben wurde.
status	call_req.status: Eindeutige Kennung, die auf einen Datensatz in der Tabelle "cr_stat" verweist. Gibt den Status dieser Anfrage an call_req.status = cr_stat.code
active_flag	call_req.active_flag: Ganzzahl-Flag, um zu bestimmen, ob dieser Anfragedatensatz aktiv ist oder nicht (1 oder 0).
open_date	call_req.open_date: Zeitstempel, zu dem die Anfrage erstellt wurde (pdmtime).

Feld	Anmerkungen
time_spent_sum	call_req.time_spent_sum: Die abgeleitete Summe der Felder "time_spent" aller act_log-Datensätze gespeichert in Sekunden (d.h. 80 = 1 Minute 20 Sekunden).
last_mod_dt	call_req.last_mod_dt: Zeitstempel, zu dem die letzte Änderung vorgenommen wurde (pdmtime).
close_date	call_req.close_date: Stempel für den Zeitpunkt, zu dem die Anfrage als inaktiv eingestellt wurde ("pdmtime").
resolve_date	Zeitpunkt (Datum), zu dem die Anforderung gelöst wurde (pdmtime).
rootcause	Zeiger auf rootcause.id.
log_agent	call_req.log_agent: Eindeutige binäre ID, die auf einen Datensatz in der Tabelle "ca_contact" verweist. Verweist auf die Person, die die Anfrage ursprünglich erstellt hat. call_req.log_agent = ca_contact.contact_uuid
Verantwortlicher	call_req.assignee: Eindeutige binäre ID, die auf einen Datensatz in der Tabelle "ca_contact" verweist. Stellt die Person dar, die der Anfrage gegenwärtig zugewiesen ist. call_req.assignee = ca_contact.contact_uuid
group_id	call_req.group_id: Eindeutige binäre ID, die auf einen Datensatz in der Tabelle "ca_contact" verweist. Stellt die Gruppe dar, die der Anfrage gegenwärtig zugewiesen ist. call_req.group_id = ca_contact.contact_uuid
customer	call_req.customer: Eindeutige binäre ID, die auf einen Datensatz in der Tabelle "ca_contact" verweist. Stellt den betroffenen Endanwender für diese Anfrage dar. call_req.customer = ca_contact.contact_uuid
charge_back_id	charge_back_id: Textfeld, das als Buchhaltungsindikator verwendet wird, um die Kosten für diese Anfrage der entsprechenden Kostenstelle zuzuweisen.
affected_rc	call_req.affected_rc: Eindeutige binäre ID, die auf eine Zeile in der Tabelle "ca_owned_resource" verweist. Stellt das Asset dar, für das diese Anfrage gilt. call_req.affected_rc = ca_owned_resource.own_resource_uuid.
support_lev	call_req.support_lev: Zeiger auf einen Service Desk-Datensatz, der einige Bedingungen automatisiert, unter denen diese Anfrage erledigt werden muss. call_req.support_lev = srv_desc.code.

Feld	Anmerkungen
category	call_req.category: Eindeutige Kennung, die auf einen Datensatz in der Tabelle "prob_ctg" verweist. Stellt die Kategorie dar, zu der diese Anfrage gehört. call_req.category = prob_ctg.persid
solution	call_req.solution: Zeiger zum Abrufen einer Lösung. call_req.solution = crsol.persid
impact	call_req.impact: Eindeutige ID in Form einer Ganzzahl, die auf eine Zeile in der Tabelle "impact" verweist. Gibt den Auswirkungsumfang dieser Anfrage an. call_req.impact = impact.enum
priority	call_req.priority: Eindeutige ID in Form einer Ganzzahl, die auf einen Datensatz in der Tabelle "pri" verweist. Gibt an, mit welcher Priorität die Analysten an dieser Anfrage arbeiten werden. call_req.priority = pri.enum
urgency	call_req.urgency: Eindeutige ID in Form einer Ganzzahl, die auf eine Zeile in der Tabelle "urgency" verweist. Gibt die Lösungsdringlichkeit für diese Anfrage (nach Einschätzung des Anwenders) an. call_req.urgency = urgency.enum
severity	call_req.severity: Eindeutige ID in Form einer Ganzzahl, die auf eine Zeile in der Tabelle "severity" verweist. Gibt den Schweregrad der Konsequenzen für diese ungelöste Anfrage an. call_req.severity = severity.enum
extern_ref	Externer Verweis auf ein verknüpftes Ticket.
last_act_id	ID der letzten Aktivität.
cr_ticket	Zeiger auf ein Problemticket, um das verknüpfte Ticket zu ermitteln.
parent	call_req.parent: PersID-Zeiger auf eine andere PersID einer Anfrage, der das Erstellen einer Hierarchie von Changes erleichtert. call_req.parent = call_req.persid
template_name	call_req.template_name: Textwert für den Verwendungszweck der Anfrage. Er kann aus einer Liste ausgewählt werden und dient als Vorlage für ähnliche Anfragen. cr_template.template = call_req.persid
sla_violation	call_req.sla_violation: Ganzzahl, mit der ausgedrückt wird, wie oft mit dieser Anforderung verknüpfte SLAs verletzt wurden.

Feld	Anmerkungen
predicted_sla_viol	Gibt an, dass laut Neugents eine Anforderung die SLA wahrscheinlich verletzen wird.
macro_predicted_violation	Gibt an, dass laut Neugents eine Anforderung die SLA wahrscheinlich verletzen wird.
created_via	call_req.created_via: Zeiger in Form einer Ganzzahl auf einen Datensatz in der Tabelle "interface", der angibt, von welcher Schnittstelle der Change stammt. call_req.created_via = interface.id
call_back_date	call_req.call_back_date: Ein Zeitstempelfeld (pdmtime) das ein zukünftiges Datum/eine zukünftige Zeit anzeigt, zu der der betroffene Endanwender (affected_end_user) kontaktiert werden soll.
call_back_flag	call_req.call_back_flag: Boolescher Indikator, der dem Anwender als Kontrollkästchen angezeigt wird und der angibt, ob der Analyst zum Datum "call_req.call_back_date" benachrichtigt werden soll.
event_token	call_req.event_token: Wird von CA NSM für übereinstimmende Nachrichten verwendet.
sched_token	call_req.sched_token: Wird von CA NSM für das Zuordnen von Meldungen verwendet.
type	call_req.type: Textfeld, das auf einen Datensatz in der Tabelle "crt" verweist. Gibt den ITIL-Typ für diese Anfrage an. call_req.type = crt.code
string1	Benutzerdefinierbare Zeichenfolge.
string2	Benutzerdefinierbare Zeichenfolge.
string3	Benutzerdefinierbare Zeichenfolge.
string4	Benutzerdefinierbare Zeichenfolge.
string5	Benutzerdefinierbare Zeichenfolge.
string6	Benutzerdefinierbare Zeichenfolge.

Feld	Anmerkungen
Problem	ITIL-Problem.
incident_priority	ITIL-Störungspriorität.
Änderung	call_req.change: Eindeutige ID in Form einer Ganzzahl, die auf eine Zeile in der Tabelle "chg" verweist. Gibt den Change an, der aufgrund dieser Anfrage erstellt wurde. call_req.change = chg.id.
service_type	srv_desc.sym: Gibt den tatsächlichen Servicetyp an. call_req.support_lev = srv_desc.code
severity_num	sevrty.sym: Gibt den tatsächlichen Schweregrad an. call_req.severity = severity.enum
urgency_num	urgncy.sym: Gibt die tatsächliche Dringlichkeit an. call_req.urgency = urgency.enum
category_name	prob_ctg.sym: Gibt den tatsächlichen Anfragebereich (Problemkategorie) an. call_req.category = prob_ctg.id
asset	ca_owned_resource.resource_name: Gibt den tatsächlichen Anlagenamen an. call_req.affected_rc = ca_owned_resource.own_resource_uuid
impact_num	impact.sym: Gibt den tatsächlichen Auswirkungscode an. call_req.impact = impact.enum
assignee_lastname	ca_contact.last_name: Gibt den tatsächlichen Nachnamen des Zuständigen an. call_req.assignee = ca_contact.contact_uuid
assignee_firstname	ca_contact.first_name: Gibt den tatsächlichen Vornamen des Zuständigen an. call_req.assignee = ca_contact.contact_uuid
assignee_middlename	ca_contact.middle_name: Gibt den tatsächlichen zweiten Vornamen des Zuständigen an. call_req.assignee = ca_contact.contact_uuid
customer_lastname	ca_contact.last_name: Gibt den tatsächlichen Nachnamen des betroffenen Endanwenders an. call_req.customer = ca_contact.contact_uuid

Feld	Anmerkungen
customer_firstname	ca_contact.first_name: Gibt den tatsächlichen Vornamen des betroffenen Endanwenders an. call_req.customer.ca_contact.contact_uuid
customer_middlename	ca_contact.middle_name: Gibt den tatsächlichen zweiten Vornamen des betroffenen Endanwenders an. call_req.customer = ca_contact.contact_uuid
group_name	View_Group.last_name: Gibt den tatsächlichen Gruppennamen an.
GroupID	View_Group.contact_uuid: Gibt die tatsächliche Gruppenschlüssel-ID an.
status_name	cr_stat.sym: Gibt den tatsächlichen Status an.
priority_num	pri.sym: Gibt die tatsächliche Priorität an.

View_Request_to_Act_Log

Dies ist eine Standardansicht aller Anfragen mit ihren zugehörigen Aktivitätsprotokollen. Die Ansicht "View_Request" ist mit der Ansicht "View_Act_Log" verknüpft, um ausführlichere Informationen zu jeder Aktivität nach Anfrage zu liefern.

Feld	Anmerkungen
View_Request.*	Weitere Informationen zu diesem Feld finden Sie weiter oben in diesem Dokument in der Definition der Ansicht „View_Request“.
View_Act_Log.*	Weitere Informationen zu diesen Feldern finden Sie weiter oben in diesem Dokument in der Definition der Ansicht „View_Act_Log“.

View_Request_to_Properties

Dies ist eine grundlegende Ansicht von Aufrufanforderungen und ihren Eigenschaften. Diese Ansicht enthält alle Informationen aus der Tabelle „call request“ (call_req) und der Tabelle „request property“ (cr_prp).

Feld	Anmerkungen
View_Request.*	Weitere Informationen zu diesen Feldern finden Sie weiter oben in diesem Dokument in der Definition der Ansicht „View_Request“.
crprp_id	cr_prp.id: Eindeutige ID in Form einer Ganzzahl für den Eigenschaftendatensatz.
crprp_persid	cr_prp.persid: Eindeutige ID für diesen Datensatz in der Tabelle "cr_prp", der die Objektkennung ("cr_prp") und ein Doppelpunkt vorangehen.
sequence	cr_prp.sequence: Dies ist eine Ganzzahl, die die Reihenfolge angibt, in der dieser Eigenschaftendatensatz von CA SDM angezeigt werden soll (z. B. aufsteigend).
label	cr_prp.label: Kurze Beschreibung zu dem Wert, der in das Feld "cr_prp.value" einzugeben ist.
value	cr_prp.value: Wert, der vom Benutzer als Antwort auf die Felder "prp_description" und "cr_prp.label" eingegeben wurde.
crprp_last_mod_dt	cr_prp.last_mod_dt: Zeitstempel (pdmtime), zu dem diese Eigenschaft zuletzt geändert wurde.
crprp_last_mod_by	cr_prp.last_mod_by: Binäre ID, die auf einen Datensatz in der Tabelle "ca_contact" verweist. Stellt die Person dar, die diesen Datensatz zuletzt geändert hat. cr_prp.last_mod_by = ca_contact.contact_uuid
required	cr_prp.required: Boolescher Indikator, der angibt, ob für diese Eigenschaft ein "cr_prp.value" vorhanden sein muss, bevor der Datensatz gespeichert wird.
sample	cr_prp.sample: Textfeld, das Beispielwerte anzeigt, um den Benutzer bei der Eingabe eines sinnvollen Wertes in "cr_prp.value" zu unterstützen.
owning_cr	cr_prp.owning_cr: Eindeutige ID zur Angabe des Datensatzes, dem diese Eigenschaft zugewiesen ist. cr_prp.object_id = call_req.persid
crprp_description	cr_prp.description: Textfeld, das erklärt, welche Art von Wert in "cr_prp.value" eingegeben werden sollte.

Anhang C: Formulargruppen

Dieses Kapitel enthält folgende Themen:

[Formulargruppe "Kunden"](#) (siehe Seite 1257)

[Formulargruppe "Mitarbeiter"](#) (siehe Seite 1258)

[Formulargruppe "Analysten"](#) (siehe Seite 1260)

Formulargruppe "Kunden"

Die folgenden Webformulare sind in den Formulargruppen "Kunden" enthalten:

- about.html
- bin_form_np.html
- chg_lr.html
- cr_lr.html
- detail_iss.html
- detail_issalg.html
- detail_KD.html
- generic.html
- home.html
- iss_lr.html
- issue_status_change.html
- list_iss.html
- list_isscat.html
- list_KD.html
- menu_frames.html
- std_body.html
- std_body_site.html
- std_footer.html
- std_footer_site.html
- std_head.html
- std_header.html
- std_head_site.html

Formulargruppe "Mitarbeiter"

Die folgenden Webformulare sind in den Formulargruppen "Mitarbeiter" enthalten:

- about.html
- bin_form_np.html
- buttons.html
- change_status_change.html
- chg_lr.html
- cr_lr.html
- detail_alg.html
- detail_chg.html
- detail_chgalg.html
- detail_cr.html
- detail_in.html
- detail_KD.html
- generic.html
- home.html
- iss_lr.html
- list_chg.html
- list_chgcat.html
- list_cr.html
- list_in.html
- list_KD.html
- list_pcat.html
- list_pcat_cr.html
- list_pcat_in.html
- menu_frames.html
- request_status_change.html
- show_error.html
- std_body.html
- std_body_site.html
- std_footer.html
- std_footer_site.html

- std_head.html
- std_header.html
- std_head_site.html

Formulargruppe "Analysten"

Die folgenden Webformulare sind in den Formulargruppen "Analysten" enthalten:

A

- about.html
- acctyp_role_tab.html
- acctyp_web_auth_tab.html
- acctyp_wsp_tab.html
- admin_empty.html
- admin_main_role.html
- admin_tab_dflt.html
- admin_tree.html
- attmnt_content_tab.html
- attmnt_fields.html
- attmnt_permissions_tab.html
- attmnt_upload_popup.html
- att_mgs_event.html
- att_stype_event.html
- aty_chg_ntfr_tab.html
- aty_chg_svy_tab.html
- aty_cr_ntfr_tab.html
- aty_cr_svy_tab.html
- aty_iss_ntfr_tab.html
- aty_iss_svy_tab.html
- aty_kdComment_ntfr_tab.html
- aty_kd_ntfr_tab.html
- aty_mgs_ntfr_tab.html

B

- bhvtpl_todo_tab.html
- bhvtpl_trans_info_tab.html
- bin_form_np.html

C

- cancel.html
- cancel_empty.html
- category_content_tab.html
- category_permissions_tab.html
- chgcat_auto_assignment_tab.html
- chgcat_prptpl_tab.html
- chgcat_wftpl_tab.html
- chg_accumulate.html
- chg_causedreq_tab.html
- chg_close_all_child.html
- chg_expedite.html
- chg_lr.html
- chg_relchg_tab.html
- chg_relreq_tab.html
- cia_bmhier_tab.html
- cia_export_bmhier.html
- cia_export_nr.html
- cia_nr_tab.html
- cia_pwd_tab.html
- cia_sync_stat.html
- cnote_tracker.html
- cnt_addr_tab.html
- cnt_auto_assignment_tab.html
- cnt_env_tab.html
- cnt_grp_tab.html
- cnt_mem_tab.html
- cnt_notif_tab.html
- cnt_org_tab.html
- cnt_rem_tab.html
- cnt_role_tab.html
- cr_attach_chg.html
- cr_close_all_child.html
- cr_detach_chg.html

- cr_lr.html
- cr_relreq_tab.html

D

- dcon_constraint_tab.html
- dcon_sql_tab.html
- detail.template
- detail_acctyp.html
- detail_act_type_assoc.html
- detail_ADMIN_TREE.html
- detail_alg.html
- detail_arcpur_rule.html
- detail_asset.html
- detail_atev.html
- detail_atomic_cond.html
- detail_atmnt_edit.html
- detail_atmnt_error.html
- detail_atmnt_folder.html
- detail_atmnt_ro.html
- detail_attr_alias.html
- detail_aty.html
- detail_audlog.html
- detail_bhvtpl.html
- detail_bmcls.html
- detail_bmhier.html
- detail_bmrep.html
- detail_BU_TRANS.html
- detail_ca_cmpny.html
- detail_chg.html
- detail_chgalg.html
- detail_chgcat.html
- detail_chgstat.html
- detail_chgtype.html

- detail_CI_ACTIONS.html
- detail_CI_ACTIONS_ALTERNATE.html
- detail_CI_DOC_TEMPLATES.html
- detail_CI_STATUSES.html
- detail_CI_WF_TEMPLATES.html
- detail_cmth.html
- detail_cnote.html
- detail_cnt.html
- detail_cost_cntr.html
- detail_country.html
- detail_cr.html
- detail_crs.html
- detail_crsq.html
- detail_cr_prptpl.html
- detail_ctab.html
- detail_ctimer.html
- detail_ctp.html
- detail_dcon.html
- detail_dept.html
- detail_dmn.html
- detail_doc_rep.html
- detail_DOC_VERSIONS.html
- detail_EBR_ACRONYMS.html
- detail_EBR_LOG.html
- detail_EBR_NOISE_WORDS.html
- detail_EBR_SYNONYMS_ADM.html
- detail_event_log.html
- detail_evt.html
- detail_fmgrp.html
- detail_grc.html
- detail_g_cnt.html
- detail_g_loc.html
- detail_g_org.html

- detail_g_prod.html
- detail_g_qname.html
- detail_g_srvrs.html
- detail_g_tblmap.html
- detail_g_tblrule.html
- detail_help_set.html
- detail_hier_edit.html
- detail_hier_ro.html
- detail_ical_event_template.html
- detail_imp.html
- detail_in.html
- detail_iss.html
- detail_issalg.html
- detail_isscat.html
- detail_issstat.html
- detail_iss_wf.html
- detail_kc.html
- detail_KCAT.html
- detail_KD.html
- detail_KD_FILE.html
- detail_KD_QA.html
- detail_KD_SAVE_AS.html
- detail_KD_TASK.html
- detail_KD_TASK_cancel_rework.html
- detail_KD_TASK_retire.html
- detail_KD_template.html
- detail_KEIT_TEMPLATES.html
- detail_KT_ACT_CONTENT.html
- detail_KT_BLC.html
- detail_KT_FILE_TYPE.html
- detail_KT_FLG_TYPE.html
- detail_ldap.html
- detail_ldap_group.html

- detail_loc.html
- detail_LONG_TEXTS.html
- detail_lr_ro.html
- detail_macro.html
- detail_macro_type.html
- detail_menu_bar.html
- detail_menu_tree_name.html
- detail_mfrmod.html
- detail_mgs.html
- detail_mgsalg.html
- detail_mgsstat.html
- detail_NOTIFICATION.html
- detail_no_contract_sdsc.html
- detail_nr.html
- detail_nrf.html
- detail_nr_com.html
- detail_ntfl.html
- detail_ntfm.html
- detail_ntfr.html
- detail_options.html
- detail_org.html
- detail_O_COMMENTS.html
- detail_O_EVENTS.html
- detail_pcat.html
- detail_perscnt.html
- detail_position.html
- detail_pr.html
- detail_prefs.html
- detail_pri.html
- detail_prod.html
- detail_projex.html
- detail_prptpl.html
- detail_prpval.html

- detail_prpval_rule.html
- detail_prp_edit.html
- detail_QUERY_POLICY.html
- detail_rc.html
- detail_response.html
- detail_role.html
- detail_role_go_form.html
- detail_rptmeth.html
- detail_rrf.html
- detail_rss.html
- detail_sapolicy.html
- detail_saprobtyp.html
- detail_sdsc.html
- detail_sdsc_map.html
- detail_seq.html
- detail_sev.html
- detail_site.html
- detail_slatpl.html
- detail_srvr_aliases.html
- detail_srvr_zones.html
- detail_state.html
- detail_svc_contract.html
- detail_svy_atpl.html
- detail_svy_qtpl.html
- detail_svy_tpl.html
- detail_tab.html
- detail_tenant.html
- detail_tenant_group.html
- detail_tskstat.html
- detail_tskty.html
- detail_tspan.html
- detail_typecnt.html
- detail_tz.html

- detail_urg.html
- detail_USP_PREFERENCES.html
- detail_usp_servers.html
- detail_vpt.html
- detail_web_form.html
- detail_wf.html
- detail_wftpl.html
- detail_wrkshft.html
- dmn_dcon_tab.html
- edit_prop_dyn.html
- ed_image_pane.html
- evt_action_info.html
- evt_config_info.html

G

- generic.html
- get_comment.html
- g_profile_browser.html
- g_profile_browser2.html
- g_profile_browser3.html
- g_profile_browser_frameset.html
- g_profile_jump.html
- g_profile_scratchpad.html

N

- hierload_admin_tree.html
- hierload_KCAT.html
- hiersel_admin_tree.html
- hiersel_KCAT.html
- hourglass.html
- html_editor_create_change_order.html
- html_editor_create_ticket.html
- html_editor_frames.html
- html_editor_insert_image.html

- [html_editor_insert_link.htmlpl](#)
- [html_editor_insert_table.htmlpl](#)
- [html_editor_tabs.htmlpl](#)
- [html_editor_toolbar.htmlpl](#)
- I
- [insert_iss_wf.htmlpl](#)
- [insert_wf.htmlpl](#)
- [in_relreq_tab.htmlpl](#)
- [isscat_auto_assignment_tab.htmlpl](#)
- [isscat_prptpl_tab.htmlpl](#)
- [isscat_wftpl_tab.htmlpl](#)
- [issue_status_change.htmlpl](#)
- [iss_accumulate.htmlpl](#)
- [iss_close_all_child.htmlpl](#)
- [iss_custfld_tab.htmlpl](#)
- [iss_expedite.htmlpl](#)
- [iss_lr.htmlpl](#)
- [iss_reliss_tab.htmlpl](#)
- [iss_resol_tab.htmlpl](#)
- K
- [kd_action_forward.htmlpl](#)
- [kd_action_publish.htmlpl](#)
- [kd_action_reject.htmlpl](#)
- [kd_action_unpublish.htmlpl](#)
- [kd_action_unretire.htmlpl](#)
- [kd_attachments_tab.htmlpl](#)
- [kd_attributes_tab.htmlpl](#)
- [kd_categories_tab.htmlpl](#)
- [kd_content_tab.htmlpl](#)
- [kd_file_prop_tab.htmlpl](#)
- [kd_permissions_tab.htmlpl](#)
- [kd_qa_attributes_tab.htmlpl](#)

- kd_qa_content_tab.html
- keit_tmpl_export_fields_tab.html
- keit_tmpl_export_filter_tab.html
- keit_tmpl_import_settings_tab.html
- keit_tmpl_name_tab.html
- kt_admin_attachments.html
- kt_admin_automated_policies.html
- kt_admin_document_settings.html
- kt_admin_faq_options.html
- kt_admin_general_settings.html
- kt_admin_integration.html
- kt_admin_knowledge.html
- kt_admin_parse_settings.html
- kt_admin_report_card.html
- kt_admin_search_config_cr.html
- kt_admin_search_config_iss.html
- kt_admin_search_options.html
- kt_admin_survey_settings.html
- kt_admin_workflow_settings.html
- kt_architect.html
- kt_architect2.html
- kt_architect3.html
- kt_architect_delete_KCAT.html
- kt_architect_delete_KD.html
- kt_architect_frameset.html
- kt_architect_init.html
- kt_architect_javascript.html
- kt_architect_KCATs.html
- kt_architect_KCAT_path.html
- kt_architect_KDs.html
- kt_dtbuilder.html
- kt_dtbuilder2.html
- kt_dtbuilder3.html

- kt_dtbuilder_frameset.html
- kt_dtbuilder_node.html
- kt_dtbuilder_prompt_window.html
- kt_dtbuilder_save_dialog_window.html
- kt_dtbuilder_save_tree_form.html
- kt_dtbuilder_tree.html
- kt_email_document.html
- kt_faq_tree.html
- kt_main.html
- kt_main2.html
- kt_main3.html
- kt_main_role.html
- kt_permissions.html

L

- list.template
- list_acctyp.html
- list_act_type_assoc.html
- list_alg.html
- list_all_fmgrp.html
- list_all_lr.html
- list_architect_KDs.html
- list_architect_KDs_Pref.html
- list_arcpur_hist.html
- list_arcpur_rule.html
- list_atev.html
- list_atomic_cond.html
- list_atmnt.html
- list_attr_alias.html
- list_aty.html
- list_audlog.html
- list_bmcls.html
- list_bmhier.html

- list_bmrep.html
- list_bm_task.html
- list_bool.html
- list_ca_cmpny.html
- list_ca_logical_asset.html
- list_chg.html
- list_chgalg.html
- list_chgcat.html
- list_chgsched.html
- list_chgsched_config.html
- list_chgstat.html
- list_chgtype.html
- list_CI_ACTIONS.html
- list_CI_ACTIONS_ALTERNATE.html
- list_CI_DOC_TEMPLATES.html
- list_CI_STATUSES.html
- list_CI_WF_TEMPLATES.html
- list_cmth.html
- list_cnote.html
- list_cnt.html
- list_cost_cntr.html
- list_country.html
- list_cr.html
- list_crs.html
- list_crsq.html
- list_crs_cr.html
- list_crs_in.html
- list_crs_pr.html
- list_crt.html
- list_cr_kt.html
- list_ctab.html
- list_ctimer.html
- list_ctp.html

- list_dcon.html
- list_dept.html
- list_dmn.html
- list_DOC_VERSIONS.html
- list_EBR_ACRONYMS.html
- list_EBR_LOG.html
- list_EBR_NOISE_WORDS.html
- list_EBR_SYNONYMS_ADM.html
- list_event_log.html
- list_evt.html
- list_evtdly.html
- list_grc.html
- list_grpmem.html
- list_g_chg_queue.html
- list_g_cnt.html
- list_g_cr_queue.html
- list_g_iss_queue.html
- list_g_loc.html
- list_g_org.html
- list_g_prod.html
- list_g_qname.html
- list_g_srvrs.html
- list_g_tblmap.html
- list_g_tblrule.html
- list_g_tenant.html
- list_help_item.html
- list_help_set.html
- list_ical_event_template.html
- list_imp.html
- list_in.html
- list_iss.html
- list_issalg.html
- list_isscat.html

- list_issstat.html
- list_iss_kt.html
- list_iss_wf.html
- list_kc.html
- list_KCAT_LINKED.html
- list_KCAT_QA.html
- list_KCAT_tree.html
- list_KD.html
- list_kdsched.html
- list_kdsched_config.html
- list_KD_ATTMNT.html
- list_kd_CI_DOC_LINKS.html
- list_KD_FILE.html
- list_kd_INDEX_DOC_LINKS.html
- list_KD_QA.html
- list_KEIT_export_transactions.html
- list_KEIT_IMPORT_PACKAGES.html
- list_KEIT_import_transactions.html
- list_KEIT_TEMPLATES.html
- list_KT_ACT_CONTENT.html
- list_KT_BLC.html
- list_KT_FILE_TYPE.html
- list_KT_FLG_TYPE.html
- list_KT_FREE_TEXT.html
- list_KT_LIFE_CYCLE_REP.html
- list_ldap.html
- list_ldap_group.html
- list_loc.html
- list_LONG_TEXTS.html
- list_lr.html
- list_macro.html
- list_macro_type.html
- list_menu_bar.html

- list_menu_tree_name.html
- list_mfrmod.html
- list_mgs.html
- list_mgsalg.html
- list_mgsstat.html
- list_NOTIFICATION.html
- list_no_contract_sdsc.html
- list_nr.html
- list_nrf.html
- list_nr_com.html
- list_ntfl.html
- list_ntfm.html
- list_ntfr.html
- list_OA_TABLES.html
- list_options.html
- list_org.html
- list_O_EVENTS.html
- list_pcat.html
- list_pcat_cr.html
- list_pcat_in.html
- list_pcat_pr.html
- list_perscnt.html
- list_position.html
- list_pr.html
- list_pri.html
- list_prod.html
- list_prod_list.html
- list_prpval.html
- list_prpval_rule.html
- list_QUERY_POLICY.html
- list_QUERY_POLICY_ACTIONS.html
- list_rc.html
- list_rel_cat.html

- list_response.html
- list_role.html
- list_role_tab.html
- list_rptmeth.html
- list_rrf.html
- list_rss.html
- list_sapolicy.html
- list_saprobtyp.html
- list_sdsc.html
- list_sdsc_map.html
- list_seq.html
- list_sev.html
- list_showgrp.html
- list_site.html
- list_srvr_aliases.html
- list_srvr_zones.html
- list_state.html
- list_svc_contract.html
- list_svy_atpl.html
- list_svy_qtpl.html
- list_svy_tpl.html
- list_tab.html
- list_tenant.html
- list_tenant_group.html
- list_tskstat.html
- list_tskty.html
- list_tspan.html
- list_typecnt.html
- list_tz.html
- list_urg.html
- list_usp_servers.html
- list_vpt.html
- list_web_form.html

- list_wf.html
- list_wrkshft.html
- load_properties.html
- load_wait.html
- loc_address_tab.html
- loc_auto_assignment_tab.html
- log_reader.html
- log_reader_banner.html
- log_reader_fs.html
- log_sol_4itil.html

M

- macro_atomic_cond_tab.html
- macro_cnt_tab.html
- macro_ctp_tab.html
- macro_ntfl_tab.html
- macro_rrf_tab.html
- mactyp_exescript_tab.html
- mactyp_valscript_tab.html
- mapped_contracts_tab.html
- menubar.template
- menubar_admin.html
- menubar_architect.html
- menubar_chg_sched.html
- menubar_dtbuilder.html
- menubar_html_editor.html
- menubar_kt.html
- menubar_no.html
- menubar_sd.html
- menubar_sd_chg_manager.html
- menubar_sd_cust_mgr.html
- menubar_sd_cust_rep.html
- menubar_sd_hd_manager.html

- menubar_sd_inc_manager.html
- menubar_sd_know_analyst.html
- menubar_sd_know_manager.html
- menubar_sd_l1_analyst.html
- menubar_sd_l2_analyst.html
- menubar_sd_prb_manager.html
- menubar_sd_vendor_analyst.html
- menu_frames.html
- menu_tree_editor.html
- menu_tree_editor2.html
- menu_tree_editor3.html
- mgs_cnt_tab.html
- mgs_ctp_tab.html
- mgs_ini_tab.html
- mgs_ntfl_tab.html
- mgs_rem_tab.html
- multiframe.template
- multiframe_reports_admin.html
- multiframe_reports_chg_manager.html
- multiframe_reports_cust_mgr.html
- multiframe_reports_inc_mgr.html
- multiframe_reports_know_analyst.html
- multiframe_reports_know_mgr.html
- multiframe_reports_prb_mgr.html
- multiframe_reports_sd_mgr.html

N

- new_lr.html
- nf.html
- nosession.html
- nr_bm_tab.html
- nr_chg_tab.html
- nr_contact_tab.html

- nr_inc_tab.html
- nr_inv_tab.html
- nr_iss_tab.html
- nr_loc_tab.html
- nr_log_tab.html
- nr_org_tab.html
- nr_prb_tab.html
- nr_projex_tab.html
- nr_rel_tab.html
- nr_reqitil_tab.html
- nr_req_tab.html
- nr_serv_tab.html
- ntfl_ntfr_tab.html
- ntfr_aty_tab.html
- ntfr_cnt_tab.html
- ntfr_ctp_tab.html
- ntfr_ntfl_tab.html

O

- order_status_change.html
- org_address_tab.html
- org_env_tab.html

P

- pcat_auto_assignment_tab.html
- pcat_prptpl_tab.html
- pcat_wftpl_tab.html
- power_user_tips.html
- profile_browser.html
- profile_browser2.html
- profile_browser3.html
- profile_browser_frameset.html
- profile_envcnt.html
- profile_envorg.html

- profile_histcnt_chg.html
- profile_histcnt_cr.html
- profile_histcnt_in.html
- profile_histcnt_iss.html
- profile_histcnt_pr.html
- profile_historg_chg.html
- profile_historg_cr.html
- profile_historg_in.html
- profile_historg_iss.html
- profile_historg_pr.html
- profile_infocnt.html
- profile_infoorg.html
- profile_menu.html
- profile_qtemplate.html
- pr_attinc_tab.html
- pr_relreq_tab.html

R

- reports.html
- reports.html.tpl
- request_status_change.html
- role_auth_tab.html
- role_fnacc_tab.html
- role_goform_tab.html
- role_kt_ct_tab.html
- role_kt_docs_tab.html
- role_webform_tab.html
- role_web_interface_tab.html

S

- sapolicy_ac_tab.html
- sapolicy_pt_tab.html
- saprobtyp_dh_tab.html
- saprobtyp_rd_tab.html

- scoreboard.html
- scratchpad.html
- screen_reader_usage.html
- sdsc_chg_slatpl_tab.html
- sdsc_chg_wf_slatpl_tab.html
- sdsc_cr_slatpl_tab.html
- sdsc_iss_slatpl_tab.html
- sdsc_iss_wf_slatpl_tab.html
- sdsc_map_cnt_tab.html
- sdsc_map_grp_tab.html
- sdsc_map_nr_tab.html
- sdsc_map_pri_tab.html
- sdsc_map_urg_tab.html
- sd_kt_admin.html
- sd_main.html
- sd_main_role.html
- search_child_KCATs_filter.html
- show_error.html
- show_main_detail.html
- std_body.html
- std_body_site.html
- std_footer.html
- std_footer_site.html
- std_head.html
- std_head_site.html
- suggest_knowledge_isscat.html
- suggest_knowledge_list_isscat.html
- suggest_knowledge_list_pcat.html
- suggest_knowledge_pcat.html
- suggest_knowledge_search_options.html
- T
- tab_detail.template

- tenant_address_tab.html
- tenant_groups_tab.html
- tenant_group_members_tab.html
- tskty_tskstat_tab.html

U

- update_lrel_bmrep.html
- update_lrel_chg.html
- update_lrel_chgcat.html
- update_lrel_cnt.html
- update_lrel_cr.html
- update_lrel_ctp.html
- update_lrel_goform.html
- update_lrel_help_content.html
- update_lrel_in.html
- update_lrel_iss.html
- update_lrel_isscat.html
- update_lrel_loc.html
- update_lrel_macro.html
- update_lrel_nr.html
- update_lrel_ntfl.html
- update_lrel_ntfr.html
- update_lrel_org.html
- update_lrel_pcat.html
- update_lrel_pr.html
- update_lrel_role.html
- update_lrel_tab.html
- update_lrel_tenant.html
- update_lrel_tenant_group.html
- update_lrel_tskstat.html
- update_lrel_webform.html
- update_lrel_wrkshft.html
- upd_chg_sched.html

- upload_file.html
- upload_success.html
- usq_update.html
- usq_update_control.html
- usq_update_fin.html
- usq_update_select.html
- usq_update_tree.html

V

- v30_date_helper.html

W

- wfdef.html
- wftpl_auto_assignment_tab.html
- wftpl_bhvtpl_tab.html
- working.html
- workitems.html
- wrkshft_auto_assignment_tab.html
- wrkshft_schedule_tab.html
- wspmain.html

X

- xfer_esc_chg.html
- xfer_esc_cr.html
- xfer_esc_iss.html
- xx_attmnt_tab.html
- xx_candp_tab.html
- xx_nr_tab.html
- xx_prop_tab.html
- xx_solnalg_tab.html
- xx_stype_tab.html
- xx_template_tab.html
- xx_wf_tab.html

Anhang D: LDAP-Ergebniscodes von RFC 2251

Dieses Kapitel enthält folgende Themen:

[LDAP-Rückgabecodes](#) (siehe Seite 1283)

[Rückgabecodes des LDAP-Servers](#) (siehe Seite 1283)

[Rückgabecodes des LDAP-Clients](#) (siehe Seite 1289)

[LDAP-spezifische RFC-Standards](#) (siehe Seite 1291)

LDAP-Rückgabecodes

LDAP verfügt über eine Reihe von Operationsergebniscodes, die vom LDAP-Server als Antwort auf verschiedene LDAP-Anfragen generiert werden können. Diese Codes geben den Status der Protokolloperation an und sind in Server- und Client-Rückgabecodes unterteilt.

Rückgabecodes des LDAP-Servers

In der folgenden Tabelle werden die Server-Rückgabecodes aufgeführt.

Hex	Dezimal	Beschreibung
0x00	0	LDAP_SUCCESS Zeigt an, dass die angeforderte Clientoperation erfolgreich beendet wurde.
0x01	1	LDAP_OPERATIONS_ERROR Zeigt an, dass ein interner Fehler aufgetreten ist. Der Server kann nicht mit einem spezifischeren Fehlercode antworten und ist auch nicht in der Lage, auf eine Anfrage zu antworten. Dies gibt nicht an, dass der Client eine fehlerhafte Meldung gesendet hat.
0x02	2	LDAP_PROTOCOL_ERROR Zeigt an, dass der Server eine ungültige oder falsch formatierte Anfrage vom Client empfangen hat.
0x03	3	LDAP_TIMELIMIT_EXCEEDED Zeigt an, dass die vom Client oder Server angegebene Frist für die Operation überschritten wurde. Bei Suchvorgängen werden unvollständige Ergebnisse zurückgegeben.

Hex	Dezimal	Beschreibung
0x04	4	LDAP_SIZELIMIT_EXCEEDED Zeigt an, dass bei einem Suchvorgang, die vom Client oder Server angegebene Größenbeschränkung überschritten wurde. Es werden unvollständige Ergebnisse zurückgegeben.
0x05	5	LDAP_COMPARE_FALSE Zeigt keine Fehlerbedingung an. Zeigt an, dass die Ergebnisse einer Vergleichsoperation falsch sind.
0x06	6	LDAP_COMPARE_TRUE Zeigt keine Fehlerbedingung an. Zeigt an, dass die Ergebnisse einer Vergleichsoperation wahr sind.
0x07	7	LDAP_AUTH_METHOD_NOT_SUPPORTED Zeigt an, dass während eines Verbindungsvorgangs vom Client eine Authentifizierungsmethode angefordert wurde, die vom LDAP-Server nicht unterstützt wird.
0x08	8	LDAP_STRONG_AUTH_REQUIRED Zeigt eine der folgenden Situationen an: ■ Bei Verbindungsanfragen akzeptiert der LDAP-Server nur die erweiterte Authentifizierung. ■ Bei einer Clientanfrage hat der Client eine Operation angefordert, wie zum Beispiel einen Löschvorgang, der die erweiterte Authentifizierung erfordert. ■ Bei der Meldung einer nicht beabsichtigten Trennung erkennt der LDAP-Server, dass die Sicherheit, die die Kommunikation zwischen dem Client und dem Server schützt, unvorhergesehen fehlschlug oder beeinträchtigt war.
0x09	9	Reserved.
0x0A	10	LDAP_REFERRAL Zeigt keine Fehlerbedingung an. Zeigt bei LDAP v3 an, dass der Server den Zieleintrag der Anfrage nicht enthält, dass dies aber für die Server im Verweisungsfeld der Fall sein kann.
0x0B	11	LDAP_ADMINLIMIT_EXCEEDED Zeigt an, dass eine LDAP-Serverbegrenzung, die durch eine administrative Autorität festgelegt wurde, überschritten wurde.
0x0C	12	LDAP_UNAVAILABLE_CRITICAL_EXTENSION Zeigt an, dass der LDAP-Server unfähig war, eine Anfrage zu erfüllen, weil eine oder mehrere kritische Erweiterungen nicht verfügbar waren. Entweder unterstützt der Server das Steuerelement nicht, oder das Steuerelement ist für die Art der Operation nicht zutreffend.

Hex	Dezimal	Beschreibung
0x0D	13	LDAP_CONFIDENTIALITY_REQUIRED Zeigt an, dass die Sitzung nicht durch ein Protokoll geschützt ist, wie zum Beispiel Transportschichtssicherheit (Transport Layer Security, TLS), das für die Vertraulichkeit von Sitzungen sorgt.
0x0E	14	LDAP_SASL_BIND_IN_PROGRESS Zeigt keine Fehlerbedingung an, sondern zeigt an, dass der Server für den nächsten Schritt im Prozess bereit ist. Zur Fortsetzung des Prozesses muss der Client dem Server den gleichen SASL-Mechanismus senden.
0x0F	15	Nicht verwendet.
0x10	16	LDAP_NO_SUCH_ATTRIBUTE Zeigt an, dass das in der Änderungs- oder Vergleichsoperation angegebene Attribut im Eintrag nicht existiert.
0x11	17	LDAP_UNDEFINED_TYPE Zeigt an, dass das in der Änderungs- oder Hinzufügungsoperation angegebene Attribut im Schema des LDAP-Servers nicht existiert.
0x12	18	LDAP_INAPPROPRIATE_MATCHING Zeigt an, dass die im Suchfilter angegebene Vergleichsregel keiner Regel entspricht, die für die Syntax des Attributs definiert wurde.
0x13	19	LDAP_CONSTRAINT_VIOLATION Zeigt an, dass der Attributwert, der in einer Änderungs-, Hinzufügungs- oder Änderungs-DN-Operation angegeben wurde, für das Attribut festgelegte Bedingungen verletzt. Die Bedingung kann sich auf die Größe oder den Inhalt beziehen (nur Zeichenfolge, keine Binärdarstellung).
0x14	20	LDAP_TYPE_OR_VALUE_EXISTS Zeigt an, dass der Attributwert, der in einer Änderungs- oder Hinzufügungsoperation angegeben wurde, bereits als Wert für das Attribut existiert.
0x15	21	LDAP_INVALID_SYNTAX Zeigt an, dass es sich bei dem Attributwert, der in einer Änderungs-, Vergleichs- oder Hinzufügungsoperation angegeben wurde, um eine unerkannte oder ungültige Syntax für das Attribut handelt.
	22-31	Nicht verwendet.
0x20	32	LDAP_NO_SUCH_OBJECT Zeigt an, dass das Zielobjekt nicht gefunden werden kann. Dieser Code wird bei folgenden Operationen nicht zurückgegeben: ■ Suchvorgänge, die die Suchbasis finden, aber keine Einträge finden können, die dem Suchfilter entsprechen ■ Verbindungsvorgänge

Hex	Dezimal	Beschreibung
0x21	33	LDAP_ALIAS_PROBLEM Zeigt an, dass ein Fehler aufgetreten ist, als ein Aliasname dereferenziert wurde.
0x22	34	LDAP_INVALID_DN_SYNTAX Zeigt an, dass die Syntax des DN falsch ist. Wenn die DN-Syntax jedoch korrekt ist, aber die Strukturregeln des LDAP-Servers die Operation nicht zulassen, gibt der Server Folgendes zurück: LDAP_UNWILLING_TO_PERFORM
0x23	35	LDAP_IS_LEAF Zeigt an, dass die angegebene Operation für einen Blatteintrag nicht durchgeführt werden kann. (Dieser Code ist derzeit nicht in den LDAP-Spezifikationen enthalten, ist aber für diese Konstante reserviert).
0x24	36	LDAP_ALIAS_DEREF_PROBLEM Zeigt an, dass während eines Suchvorgangs entweder der Client keine Zugriffsrechte zum Lesen des Objekt-Aliasnamens hat oder die Dereferenzierung nicht erlaubt ist.
	37-47	Nicht verwendet.
0x30	48	LDAP_INAPPROPRIATE_AUTH Zeigt an, dass während eines Verbindungsvorgangs, der Client die Verwendung einer Authentifizierungsmethode versuchte, die er nicht korrekt verwenden kann. Zum Beispiel kann dieser Fehler eine der folgenden Ursachen haben: ■ Der Client gibt einfache Identifikationsdaten zurück, wenn erweiterte Identifikationsdaten erforderlich sind. ■ Der Client gibt einen eindeutigen Namen und ein Kennwort für eine einfache Verbindung zurück, wenn für den Eintrag kein Kennwort definiert ist.
0x31	49	LDAP_INVALID_CREDENTIALS Zeigt an, dass während eines Verbindungsvorgangs einer der folgenden Fehler aufgetreten ist: ■ Vom Client wurde entweder ein falscher eindeutiger Name oder ein falsches Kennwort übergeben. ■ Das Kennwort ist falsch, weil es abgelaufen ist; das Erkennungssystem für Eindringversuche hat das Konto gesperrt; oder es liegt eine andere ähnliche Ursache vor.
0x32	50	LDAP_INSUFFICIENT_ACCESS Zeigt an, dass der Teilnehmer keine ausreichenden Rechte hat, um die angeforderte Operation durchzuführen.

Hex	Dezimal	Beschreibung
0x33	51	LDAP_BUSY Zeigt an, dass der LDAP-Server zu ausgelastet ist, um die Clientanfrage zurzeit zu bearbeiten; aber wenn der Client wartet und die Anfrage erneut übermittelt, kann der Server sie dann gegebenenfalls bearbeiten.
0x34	52	LDAP_UNAVAILABLE Zeigt an, dass der LDAP-Server die Verbindungsanfrage des Client nicht bearbeiten kann, normalerweise weil er heruntergefahren ist.
0x35	53	LDAP_UNWILLING_TO_PERFORM Zeigt an, dass der LDAP-Server die Anfrage aufgrund serverdefinierter Einschränkungen nicht bearbeiten kann. Dieser Fehler wird aus den folgenden Gründen zurückgegeben: ■ Die Anfrage zum Hinzufügen von Einträgen verletzt die Strukturregeln des Servers. ■ Die Anfrage zur Änderung von Attributen gibt Attribute an, die Benutzer nicht ändern können. ■ Kennworteinschränkungen verhindern die Aktion. ■ Verbindungseinschränkungen verhindern die Aktion.
0x36	54	LDAP_LOOP_DETECT Zeigt an, dass der Client einen Aliasnamen oder eine Verweisungsschleife erkannt hat und folglich nicht in der Lage ist, diese Anfrage abzuschließen.
	55-63	Nicht verwendet.
0x40	64	LDAP_NAMING_VIOLATION Zeigt an, dass die Operation zum Hinzufügen oder Ändern von eindeutigen Namen die Strukturregeln des Schemas verletzt. Beispiel: ■ Die Anfrage ordnet den Eintrag einem Aliasnamen unter. ■ Die Anfrage ordnet den Eintrag einem Container unter, was aufgrund der Containment-Regeln unzulässig ist. ■ Der relative eindeutige Name (RDN) für den Eintrag verwendet einen unzulässigen Attributtyp.

Hex	Dezimal	Beschreibung
0x41	65	LDAP_OBJECT_CLASS_VIOLATION Zeigt an, dass die Hinzufügings- oder Änderungsoperation oder die Operation zur Änderung eines eindeutigen Namens die Objektklassenregeln für den Eintrag verletzt. Zum Beispiel geben die folgenden Arten von Anfragen diesen Fehler zurück: ■ Die Hinzufügings- oder Änderungsoperation versucht, einen Eintrag hinzuzufügen, der keinen Wert für ein erforderliches Attribut enthält. ■ Die Hinzufügings- oder Änderungsoperation versucht, einen Eintrag mit einem Wert für ein Attribut hinzuzufügen, das die Klassendefinition nicht enthält. ■ Die Änderungsoperation versucht, ein erforderliches Attribut zu entfernen ohne die Hilfsklasse zu entfernen, die das Attribut als erforderlich definiert.
0x42	66	LDAP_NOT_ALLOWED_ON_NONLEAF Zeigt an, dass die angeforderte Operation nur für Blatteinträge zulässig ist. Zum Beispiel geben die folgenden Arten von Anfragen diesen Fehler zurück: ■ Der Client fordert einen Löschvorgang für einen übergeordneten Eintrag an. ■ Der Client fordert eine Operation zur Änderung des eindeutigen Namens für einen übergeordneten Eintrag an.
0x43	67	LDAP_NOT_ALLOWED_ON_RDN Zeigt an, dass die Änderungsoperation versucht hat, einen Attributwert zu entfernen, der den relativen eindeutigen Namen des Eintrags bildet.
0x44	68	LDAP_ALREADY_EXISTS Zeigt an, dass die Hinzufügingsoperation versucht hat, einen Eintrag hinzuzufügen, der bereits existiert, oder dass die Änderungsoperation versucht hat, einen Eintrag in einen Namen umzubenennen, der bereits existiert.
0x45	69	LDAP_NO_OBJECT_CLASS_MODS Zeigt an, dass die Änderungsoperation versucht hat, die Strukturregeln einer Objektklasse zu ändern .
0x46	70	LDAP_RESULTS_TOO_LARGE Reserviert für CLDAP
0x47	71	LDAP_AFFECTS_MULTIPLE_DSAS Zeigt an, dass die Operation zur Änderung des eindeutigen Namens den Eintrag von einem LDAP-Server zu einem anderem bewegt und dass somit mehr als ein LDAP-Server erforderlich ist.
	72-79	Nicht verwendet.

Hex	Dezimal	Beschreibung
0x50	80	LDAP_OTHER Zeigt eine unbekannte Fehlerbedingung an. Dies ist der Standardwert für NDS-Fehlercodes, die keinen anderen LDAP-Fehlercodes entsprechen.

Rückgabecodes des LDAP-Clients

In der folgenden Tabelle werden verschiedene Rückgabecodes aufgeführt.

Hex	Dezimal	Beschreibung
0x51	81	LDAP_SERVER_DOWN Zeigt an, dass die LDAP-Bibliotheken keine anfängliche Verbindung mit dem LDAP-Server herstellen können. Entweder ist der LDAP-Server heruntergefahren, oder der angegebene Hostname oder die angegebene Anschlussnummer ist falsch.
0x52	82	LDAP_LOCAL_ERROR Zeigt einen Fehler beim LDAP-Client an. Dies ist gewöhnlich ein dynamischer Speicherzuweisungsfehler.
0x53	83	LDAP_ENCODING_ERROR Zeigt an, dass der LDAP-Client Fehlern beim Kodieren einer LDAP-Anfrage für den LDAP-Server begegnet.
0x54	84	LDAP_DECODING_ERROR Zeigt an, dass der LDAP-Client Fehlern beim Dekodieren einer LDAP-Antwort vom LDAP-Server begegnet.
0x55	85	LDAP_TIMEOUT Zeigt an, dass die Frist des LDAP-Clients überschritten wurde, während er auf ein Ergebnis wartete.
0x56	86	LDAP_AUTH_UNKNOWN Zeigt an, dass die Funktion ldap_bind oder ldap_bind_s mit einer unbekannten Authentifizierungsmethode aufgerufen wurde.
0x57	87	LDAP_FILTER_ERROR Zeigt an, dass die Funktion ldap_search mit einem ungültigen Suchfilter aufgerufen wurde.
0x58	88	LDAP_USER_CANCELLED Zeigt an, dass der Benutzer die LDAP-Operation abgebrochen hat.

Hex	Dezimal	Beschreibung
0x59	89	LDAP_PARAM_ERROR Zeigt an, dass eine LDAP-Funktion mit einem ungültigen Parameterwert aufgerufen wurde (zum Beispiel der ID-Parameter ist NULL).
0x5A	90	LDAP_NO_MEMORY Zeigt an, dass eine dynamische Speicherzuweisungsfunktion beim Aufrufen einer LDAP-Funktion fehlgeschlagen ist.
0B	91	LDAP_CONNECT_ERROR Zeigt an, dass der LDAP-Client entweder seine Verbindung verloren hat oder keine Verbindung zum LDAP-Server herstellen kann.
0x5C	92	LDAP_NOT_SUPPORTED Zeigt an, dass der Client die angeforderte Funktionalität nicht unterstützt. Wenn zum Beispiel der LDAP-Client als LDAPv2-Client eingerichtet ist, legen die Bibliotheken diesen Fehlercode fest, wenn der Client LDAPv3-Funktionalität anfordert.
0x5D	93	LDAP_CONTROL_NOT_FOUND Zeigt an, dass der Client ein Steuerelement angefordert hat, das die Bibliotheken in der vom LDAP-Server gesendeten Liste der unterstützten Steuerelemente nicht finden können.
0x5E	94	LDAP_NO_RESULTS_RETURNED Zeigt an, dass der LDAP-Server keine Ergebnisse gesendet hat. Bei Aufruf der Funktion ldap_parse_result wird kein Ergebniscode in die Antwort des Servers eingeschlossen.
0x5F	95	LDAP_MORE_RESULTS_TO_RETURN Zeigt an, dass mehrere Ergebnisse in der Ergebnismeldung verkettet sind. Die Bibliotheken legen diesen Code fest, wenn der Aufruf der Funktion ldap_parse_result ergibt, dass zusätzliche Ergebniscodes verfügbar sind.
0x60	96	LDAP_CLIENT_LOOP Zeigt an, dass die LDAP-Bibliotheken eine Schleife erkannt haben. Gewöhnlich geschieht dies beim Verfolgen von Verweisungen.

Hex	Dezimal	Beschreibung
0x61	97	LDAP_REFERRAL_LIMIT_EXCEEDED Zeigt an, dass die Verweisung das Hop-Limit überschreitet. Das Hop-Limit bestimmt, wie viele Server der Client durchlaufen kann, um Daten abzurufen. Angenommen, es liegen die folgenden Bedingungen vor: ■ Das Hop-Limit beträgt zwei. ■ Die Verweisung erfolgt zu Server D, der nur durch Server B kontaktiert werden kann (1 Hop), der Server C kontaktiert (2 Hops), der wiederum Server D kontaktiert (3 Hops) Bei diesen Bedingungen ist das Hop-Limit überschritten, und die LDAP-Bibliotheken legen diesen Code fest.

LDAP-spezifische RFC-Standards

Die folgende Tabelle beschreibt die verfügbaren LDAP-spezifischen RFC-Standards:

RFC	Beschreibung
1274	COSINE- und Internet X.500-Schema
1275	Replikationsanforderungen zur Bereitstellung eines Internet Directorys unter Verwendung von X.500
1276	Erweiterungen für Replikationen und verteilte Operationen zur Bereitstellung eines Internet Directorys unter Verwendung von X.500
1308	Einführung zu Directory Services unter Verwendung des Protokolls X.500
1309	Technische Übersicht über Directory Services unter Verwendung des Protokolls X.500
1430	Strategischer Plan zur Bereitstellung eines Internet X.500 Directory Service
1488	X.500-Zeichenfolgendarstellung von Standard-Attributsyntaxen
1558	Eine Zeichenfolgendarstellung der LDAP-Suchfilter
1617	Benennungs- und Strukturierungsrichtlinien für X.500 Directory Pilots
1777	Lightweight Directory Access Protocol v2
1778	Zeichenfolgendarstellung von Standard-Attributsyntaxen
1779	Eine Zeichenfolgendarstellung von eindeutigen Namen
1804	Schema-Veröffentlichung in X.500 Directory
1823	LDAP-API
1959	Ein LDAP-URL-Format

RFC	Beschreibung
1960	Eine Zeichenfolgendarstellung der LDAP-Suchfilter
2044	UTF-8, ein Umsetzungsformat von Unicode und ISO 10646
2164	Verwendung eines X.500/LDAP Directorys zur Unterstützung der MIXER-Adresszuordnung
2218	Allgemeines Schema für den Internet White Pages Service
2247	Verwendung von Domänen in eindeutigen Namen in LDAP/X.500
2251	Lightweight Directory Access Protocol (v3)
2252	Lightweight Directory Access Protocol (v3): Syntaxdefinitionen für Attribute
2253	Lightweight Directory Access Protocol (v3): UTF-8-Zeichenfolgendarstellung von eindeutigen Namen
2254	Zeichenfolgendarstellung der LDAP-Suchfilter
2255	LDAP-URL-Format
2256	Zusammenfassung des X.500(96)-Benutzerschemas für die Verwendung mit LDAP v3
2279	UTF-8, ein Umsetzungsformat von ISO 10646
2293	Darstellung von Tabellen und Unterbäumen im X.500 Directory
2294	Darstellung der O/R-Adresshierarchie im X.500 Directory Information Tree
2307	Ein Ansatz zur Verwendung von LDAP als Network Information Service
2377	Benennungsplan für Internet Directory-kompatible Anwendungen
2531	Content Feature-Schema für Internetfax
2559	Protokolle für Internet X.509 Public Key Infrastructure – LDAP v2
2587	Internet X.509 Public Key Infrastructure – LDAP v2-Schema
2589	Lightweight Directory Access Protocol (v3): Erweiterungen für dynamische Verzeichnis-Services
2596	Verwendung von Sprachencodes in LDAP
2649	Ein LDAP-Steuerelement und -Schema für die Haltung von Signaturen
2657	RFC 2657 – LDAP v2-Client gegenüber Indexraster
2696	LDAP-Steuerelementerweiterung für Simple Paged Results Manipulation
2713	Schema zur Darstellung von Java(tm)-Objekten in einem LDAP-Verzeichnis
2714	Schema zur Darstellung von CORBA-Objektreferenzen in einem LDAP-Verzeichnis
2739	Kalenderattribute für vCard und LDAP
2798	Definition der LDAP-Objektklasse „inetOrgPerson“
2820	Anforderungen für die Zugriffssteuerung für LDAP

RFC	Beschreibung
2829	Authentifizierungsmethoden für LDAP
2830	Lightweight Directory Access Protocol (v3): Erweiterungen für Transport Layer Security
2849	LDAP Data Interchange Format (LDIF) – Technische Spezifikation
2879	Content Feature-Schema für Internetfax (V2)
2891	LDAP-Steuerelementerweiterung für serverbasierte Sortierung von Suchergebnissen
3045	Speicherung von Anbieterinformationen in LDAP-Root-DSE
3062	Erweiterte Operation zur Änderung von LDAP-Kennwörtern
3112	LDAP-Schema zur Kennwortauthentifizierung
3296	Benannte untergeordnete Referenzen in Lightweight Directory Access Protocol-Verzeichnissen
3377	Lightweight Directory Access Protocol (v3): Technische Spezifikation
3384	Lightweight Directory Access Protocol (Version 3): Replikationsanforderungen