

CA Service Desk Manager

Administrationshandbuch

r12.5



Diese Dokumentation und die dazugehörigen Software-Hilfeprogramme (nachfolgend als die "Dokumentation" bezeichnet) dienen ausschließlich zu Informationszwecken des Nutzers und können jederzeit durch CA 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 ist vertraulich und geistiges Eigentum von CA und darf vom Benutzer weder veröffentlicht noch zu anderen Zwecken verwendet werden als solchen, die in einem separaten Vertraulichkeitsabkommen zwischen dem Nutzer und CA erlaubt sind.

Ungeachtet der oben genannten Bestimmungen ist der Nutzer, der über eine Lizenz verfügt, berechtigt, eine angemessene Anzahl an Kopien dieser Dokumentation zum eigenen Gebrauch für sich und seine Angestellten im Zusammenhang mit der betreffenden Software auszudrucken, vorausgesetzt, dass jedes kopierte Exemplar diesen Urheberrechtsvermerk und sonstige Hinweise von CA enthält.

Das Recht zum Anfertigen einer Kopie der Dokumentation beschränkt sich auf den Zeitraum der vollen Wirksamkeit der Produktlizenz. Sollte die Lizenz aus irgendeinem Grund enden, bestätigt der Nutzer 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 JEGLICHE 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 DEM NUTZER ODER DRITTEN FÜR VERLUSTE ODER UNMITTELBARE ODER MITTELBARE SCHÄDEN, DIE AUS DER VERWENDUNG 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 dieses Urheberrechtsvermerks in keiner Weise verändert.

Diese Dokumentation wurde von CA hergestellt.

Diese Dokumentation wird 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 Folgebestimmungen.

Copyright © 2010 CA. Alle Rechte vorbehalten. Alle Marken, Produktnamen, Dienstleistungsmarken oder Logos, auf die hier verwiesen wird, sind Eigentum der entsprechenden Rechtsinhaber.

CA-Produktreferenzen

Diese Dokumentation bezieht sich auf die folgenden CA-Produkte:

- CA Advantage™ Data Transformer (ADT)
- CA Asset Portfolio Management (CA APM)
- CA CMDB
- CA Business Intelligence
- Ca Cohesion® Application Configuration Manager (CA Cohesion ACM)
- CA Embedded Entitlements Manager (CA EEM)
- CA Enterprise Workload Automation (CA EWA)
- CA IT Process Automation Manager (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
- Unicenter Asset Portfolio Management (UAPM)

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
Server-Konfigurationstasks.....	28
Konfigurieren von TCP/IP	29
Ändern einer Serverkonfiguration	30
ITIL-Konfiguration.....	30
ITIL-Servicedisziplinen	31
Optionen für die Mitarbeiter- und Gastschnittstelle	32
Benachrichtigungen für Configuration Items	34
Aktivitätsprotokoll – Sicherheit	34
PDA-Schnittstelle.....	36
Starten von sekundären Servern	37
Starten des primären Servers	38
Server Status	40
Konfigurieren von SSL auf Tomcat.....	41
Bereitstellen von CMDBf-Webservices	42
Beenden eines Servers (Windows)	43
Beenden von Servern (UNIX).....	43

Kapitel 3: Definieren der Geschäftsstruktur 45

Definieren einer Geschäftsstruktur.....	45
Kontakte	46
Gruppen.....	46
Standorte	46
Positionen	47
Organisationen.....	47
Definieren der Unternehmensinfrastruktur	48
Objektdefinitionsreihenfolge	48
Configuration Item-Familien und -Klassen	49
Hersteller und Modelle.....	49
Dienststatus	49

Anbietertypen und Anbieter.....	50
Configuration Item.....	50
Externe Asset Management-Tools	51
Unterstützung für Multi-Site.....	52
Mehrere Standorte – Übersicht	52
Einrichten eines CA Service Desk Manager-Systems für mehrere Standorte.....	54
Mandantenfähig	68
Dienst-Provider	69
Wie Multi-Tenancy funktioniert	70
Auswirkung auf die Benutzerschnittstelle.....	78
Support-Automatisierung-Auswirkung.....	81
Auswirkung auf Knowledge-Management	82
Verwenden von Multi-Tenancy	84

Kapitel 4: Richtlinie zur Implementierung: 95

Implementieren von Richtlinien	95
Benachrichtigungen	95
Aktivitätszuordnungen.....	96
Aktivitätsbenachrichtigungen.....	97
Objektkontaktbenachrichtigungen	98
Benachrichtigungsmethoden	100
E-Mail-Benachrichtigungen.....	103
Benachrichtigungsregeln.....	107
Beispiel: Erstellen von Meldungsvorlagen	119
Artefakte in Meldungen.....	121
BenachrichtigungsCodes und -zeichenfolgen	122
Liste der Empfänger von manuellen Benachrichtigungen.....	126
Benachrichtigungen an vorherige Zuständige.....	127
Benachrichtigungen für Configuration Items	130
Umfragebenachrichtigungen.....	132
Hinzufügen von URL-Hyperlinks an Benachrichtigungen.....	133
Reader für Benachrichtigungsprotokoll.....	133
E-Mail-Administration	137
Postfächer	139
Postfachregeln	140
Postfachrichtlinien	146
Implementieren von Postfächern.....	148
Mehrere Postfächer	153
Konfigurieren von E-Mail-Antworten	155
Artefakte.....	157
Hinweise zur Verwendung von Artefakten.....	158
Schutz und Sicherheit von Artefakten	159

Service Level Agreements (Dienstverträge).....	161
Verwendung von SLAs.....	161
Klassische SLA-Behandlung.....	162
Servicetypen und Ereignisse.....	162
Implementieren von Servicetypen.....	163
Vordefinierte Servicetypen.....	164
Einrichten von Ereignissen.....	165
Serviceziele.....	167
Serviceverträge.....	168
Migration von Serviceverträgen.....	169
Verletzungszeitpunkt.....	170
Zeitzone und Schichten.....	171
Sicherheit.....	175
Konfigurationen für CA EEM- und CA Workflow-Benutzerdatenbanken.....	175
Sicherheitsempfehlungen.....	187
CA EEM-Authentifizierung für CA IT-PAM.....	187
Benutzerauthentifizierung.....	188
Authentifizierung von Benutzern durch CA Service Desk Manager.....	189
Externe Authentifizierung.....	189
Validierungstypen.....	190
Anzahl angemeldeter und lizenzierter Benutzer.....	191
Interne Protokolle.....	192
CA Service Desk Manager-Integration.....	192
Zuordnungen von Datenpartitionen.....	193
Datenaufteilungen.....	193
Einrichten von Datenaufteilungen.....	194
Angaben von Bedingungen.....	194
Einschränkungstypen.....	196
Erstellen einer Datenpartitionseinschränkung für CAB-Zuweisungen.....	198
Konfigurieren von Knowledge-Management-Datenpartitionseinschränkungen für rollenbasierte Berechtigungen.....	199
Umfragen.....	200
Konfigurieren Ihres Systems für Umfragen.....	200
Vorbereiten einer Umfrage.....	200
Definieren von Umfragebenachrichtigungen.....	201
Berichte zu Umfragen.....	202
Verwaltete Umfrage.....	203
Webservices.....	203

Kapitel 5: Konfiguration von Benutzerkonten	205
Kontakte.....	205
Kontaktdefinitionen.....	206

Gruppen	207
Kontakttypen	208
Bestimmen des Verhaltens auf der Basis des Kontakttyps	208
Einrichten von Benachrichtigungen auf der Basis von Kontakttypen	208
Auswählen von Kontakten auf der Basis des Kontakttyps	209
Spezielle Verarbeitungstypen	209
Konfigurieren von Kontakten zur speziellen Verarbeitung	210
Zuordnen von Kontakten zu bestimmten Verarbeitungstypen	211
LDAP-Verzeichnis-Daten	212
Konfigurieren von LDAP-Optionen	213
Überprüfen der LDAP-Integration	216
Automatisches Erstellen von Kontakten	219
Zugriffstypenzuweisungen von LDAP-Gruppen aus	219
Batch-Import von Kontakten anhand von LDAP-Daten	220
Batch-Aktualisierung von Kontakten anhand von LDAP-Daten	223
LDAP-Authentifizierung	225
Transport Layer Security	226
Attributzuordnung	226
Problembehandlung	228

Kapitel 6: Verwalten von Rollen 241

Rollen	241
Vordefinierte Rollen	241
Rollenbasierte Sicherheit	244
Funktionsweise von Zugriffstypen	244
Rollendatensätze	247
Funktionale Zugriffsbereiche	248
Datenaufteilungen	253
Rollenbasierte Navigation	253
Registerkarten	254
Vordefinierte Registerkarten	255
Webformulare	257
Formulargruppen	258
Menüstrukturen	258
Menüstrukturressourcen	259
Menüleisten	259
Symbolleisten	261
'Los'-Ressourcen	261
Hilfesätze	262
Implementieren einer benutzerdefinierten Menüstruktur	262
Implementieren einer benutzerdefinierten Menüstruktur	264
Erstellen von Rollendatensätzen	265

Erstellen von Registerkartendatensätzen	266
Erstellen von Menüleistendatensätzen	267
Erstellen von Webformular-Datensätzen	268
Kopieren von Menüstrukturen	270
Erstellen und Anpassen von Menüstrukturen	271
Erstellen und Veröffentlichen von Helpsets	272
Wechseln von Rollen	274

Kapitel 7: Einrichten einer Support-Struktur 275

Support-Struktur	275
Modelle	276
Internes Modell	276
Externes Modell	277
Kombiniertes Modell	278
CA Workflow	279
Workflow zur Laufzeit	280
Auswählen einer Workflow-Prozessdefinition	280
Workflow-Aufgaben	282
CA IT-PAM-Workflow-Integration	282
CA IT-PAM-Komponenten	283
CA IT-PAM Integration mit CA Service Desk Manager zur Laufzeit	284
Erstellen einer Prozessdefinition	285
Erstellen von Startauftragsformularen	286
Anhängen von CA IT-PAM-Prozessdefinitionen	288
Freigegebene Codes	289
Prioritätscodes	290
Schweregrad-Codes	290
Auswirkungscodes	291
Dringlichkeitscodes	291
Statuscodes	291
Anfragestatuscodes	292
Statuscodes von Changes	293
Statuscodes von Issues	295
Aufgabenstatuscodes	296
Aufgabentypen	296
Incident-Nachverfolgung	298
Installieren der Incident-Nachverfolgung	298
Anfrage-/Incident-/Problembereiche	299
Anfrage-/Incident-/Problembereich - Eigenschaften	300
Definieren von Anfrage/Zwischenfall-/Problembereichen für Self-Service	303
Change- und Issue-Kategorien	303
Vordefinierte Change-Kategorien	305

Vordefinierte Issue-Kategorien	305
Regeln zum Ändern von Kategorien in einem Ticket	305
Kategorieeigenschaften	306
Definieren von Change-Kategorien und Issue-Kategorien für Self-Service	309
Automatisches Schließen von Tickets	310
Definieren von Einstellungen zur automatischen Schließung von Tickets	311
Definieren einer Aktivitätsbenachrichtigung für die automatische Schließung	312
Aktivitäten zugehöriger Tickets	313
Definieren von Aktivitätsbenachrichtigungen für zugehörige Tickets	314
Definieren von Benachrichtigungen über die Aktivität zugehöriger Tickets	315
Prioritätsberechnung	315
Verwaltung von Ticketwerten durch Prioritätsberechnung	316
Einstellen der Prioritätsberechnung	319
Statusübergänge und abhängige Attributsteuerungen.....	332
Arbeiten mit Statusübergängen und abhängigen Attributsteuerungen.....	333
Konfigurieren der Statusübergänge	333
Konfigurieren abhängiger Attributsteuerelemente.....	335
Web-Service-Methoden	336
Vordefinierte Übergangsabläufe	337
Best Practices: Vordefinierte Statusübergänge	341
Statusübergänge für Self-Service	343
Funktionsweise der Übergänge für Self-Service.....	344
Erstellen oder Aktualisieren von Übergangstypen für Übergänge.....	345
Verknüpfen von Übergangstypen mit Übergängen	345
Vordefinierte Übergangstypen	346
Timer.....	348
Zeitzone	348
Auslöser für Servicetypereignisse.....	349
Verwenden einer Zeitzone.....	350
Festlegung der zu verwendenden Zeitzone	350
Dateianhänge.....	351
Hoch- und Herunterladen von Dateianhängen	352
Repositorys	353
Ankündigungen.....	356
Sichtbarkeit interner Ankündigungen	357
Angaben der Ankündigungsdringlichkeit.....	357
Einrichten von gespeicherten Abfragen.....	358
Sequenznummern.....	359
Verwenden des Audit-Protokolls	360
Integration in das CA-Netzwerk und Systemverwaltung	361

Kapitel 8: Steuerung des Systemverhaltens **363**

Verwendung des Optionsmanagers	363
Ändern der System-Umgebung	364
Ereignisse	365
Makros	365
Makrotypen	366
Verwenden von Makros in Verbindung mit Ereignissen	367
Verwenden von Makros in Verbindung mit dem Verhalten für Issues- und Change-Kategorien..	367
Verwenden von Makros mit mehreren Benachrichtigungen	368
Verwenden von Makros mit einer standortdefinierten Bedingung.....	369

Kapitel 9: Konfiguration der Web-Schnittstelle **371**

Konfiguration der Web-Schnittstelle	371
Funktionsweise der Web-Schnittstelle	372
WebDirector und Verteilen der Webauslastung	372
Web.cfg und CA Service Desk Manager	373
Zuweisen einer Web-Engine zu einem WebDirector.....	374
Definieren der Web-Engine-Rolle durch WebDirector-Parameter	375
Nicht-SSL-Umgebung mit grundlegendem Lastausgleich.....	375
Globale SSL-Umgebung mit grundlegendem Lastausgleich.....	376
Gezielte Anmeldung in einer Nicht-SSL-Umgebung mit optionalem Lastausgleich	376
Gezielte SSL-Anmeldung in einer gemischten Umgebung mit optionalem Lastausgleich.....	377
Konfiguration von WebDirectors und Web-Engines	377
Implementieren einer SSL-Anmeldeumgebung mit nur einem primären Server	379
Erstellen eines Systems, das nur einen primären Server umfasst	379
Prüfen der WebDirector-Parameterwerte	382
Prüfen der SSL-Anmeldeumgebung	384
Sekundäre Server und Webfunktionen	384
So bereiten Sie Webfunktionen vor:	385
Erstellen eines Systems mit sekundären Servern.....	386
Serverkonfiguration	389
Durchführen von Änderungen mit pdm_edit.pl	403
Starten des WebDirectors	409
Abwicklung von Benutzersitzungen durch WebDirector	410
Verbessern der Leistung mit Browser-Caching	412
Konfigurieren von Microsoft Internet Information Server	412
Konfigurieren von Apache	413
Löschen des Cache-Speichers.....	414
Verhalten für die Anzeige von Datensätzen in der Web-Schnittstelle	415
Drucken von CA Service Desk Manager-Webseiten	416
Änderung der Konfigurationsdatei.....	416

SchedExpMaximum.....	426
SelListCacheExclude.....	426
SelListCacheMax.....	426

Kapitel 10: Konfiguration der Option "Automatische Zuweisung" 433

Automatische Zuweisung.....	433
Beziehungen bei der automatischen Zuweisung	434
Methoden der automatischen Zuweisung	434
Implementieren von automatischen Zuweisungen	435
Bereiche und Kategorien.....	436
Analystengruppen.....	436
Analyst	437
Automatische Zuweisung nach Lokation	437
Automatische Zuweisung nach Schicht.....	439
Standardgruppe und -zuständiger	441
Aktivieren der automatischen Zuweisung	441
Überschreiben der automatischen Zuweisung	442
Zuweisungssteuerungen.....	443
Manuelle Zuweisung.....	443
Option „Assignee_set“	444
Iss assignee_set.....	444
Area_Defaults	444
Optionen, die einen Zuständigen/eine Gruppe erfordern	444
Vorlagen	446
CA Network and Systems Management-Schnittstelle.....	446
Aktivitätsprotokoll	446
Ablaufverfolgung der automatischen Zuweisung	447
Gespeicherte Abfragen.....	447
Automatisches Zuweisen von Tickets	448
Automatisches Zuweisen von Workflow-Aufgaben	454
Configuration Item-basierte automatische Zuweisungen	457
Funktionsweise der auf einem Configuration Item basierenden automatischen Zuweisungen	457
Aktivieren von Configuration Item-basierten automatischen Zuweisungen.....	461

Kapitel 11: Verwalten Sie Ihre Datenbank 463

Datenbankverwaltungsprogramme	463
Auswählen und Konfigurieren der Datenbank	463
Datenbanklader	464
Erstellen und Nutzen einer Eingabedatei	465
Entfernen und Wiederherstellen von Bedingungen	466
Sichern von Datenbanken	467

Datenbankwiederherstellung.....	467
Datenbanktabellen-Ersatz	468
Extrahieren von Daten	468
Verwenden Datenextraktors unter UNIX.....	469
Auswählen von Daten für die Extraktion	469
Daten-Dereferenzierung.....	470
Beispiel für das Ausführen von "pdm_deref"	471
Verwenden des dbadmin-Modus	473
Archivierungs- und Lösungsregeln	474
Ausführen von Archivierungs- und Lösungsregeln	475
Anzeigen von Archivierungs- und Lösungsregeln	476
Starten der Archivierung und Löschung mit Hilfe des Schedulers eines Drittanbieters.....	477
Archivierungs- und Lösungsregeln - Definitionen	477
Archivierungs- und Lösungsverlauf.....	480
Verarbeitung von Anhängen (arcpur)	482
Wiederherstellen von archivierten Daten	483
Archivieren und Löschen von KPI-Daten.....	484
Archivieren und Löschen von Knowledge-Management-Foren	486
Archivieren und Löschen mit FAST ESP	486

Kapitel 12: Verwenden der Text-API 489

Text-API	489
Befehlszeilenschnittstelle	489
CA Network and Systems Management-Schnittstelle	490
Eingabeformat	490
Keywords	492
Eingabekonventionen für Schlüsselwörter.....	494
Formatieren von E-Mail-Nachrichten zum Aktualisieren eines Tickets.....	495
Start- und Endtrennzeichen in E-Mail-Nachrichten	496
Text-API und Artefakte.....	496
Einrichten von Benachrichtigungsantworten zum Aktualisieren von Tickets.....	497
Konvertierungsmethoden	501
Die Konfigurationsdatei	503
Options	504
Standardwerte	504
Eingehende ignorieren.....	505
Beispieleingabe	506

Kapitel 13: Verwalten der Versionskontrolle 509

Funktionsweise der Versionskontrolle	509
Versionskontrolldateien.....	510

Versionskontrolldateien des primäre Servers	510
Sekundärer Server und Client-Steuerdateien.....	511
Versionskontrolle für die Anpassung von Installationen	511
Servermodi für Versionskontrolle.....	512
Syntax für Versionsverwaltungsdateien	514
Versionskontrollparameter	514
Aufheben der Kontrolle einer Komponente.....	519

Kapitel 14: Verwalten von Konfigurationselementen 521

Verwenden der Web-Schnittstelle	521
Anzeigen von Configuration Items	522
Erstellen von Configuration Items	522
Aktualisieren von Configuration Items	523
Zuordnen eines Wartungsfensters zu einem CI.....	524
Anzeigen von zugeordneten Change-Fenstern.....	524
Anzeigen des Konfigurationselement-Verlaufs	525
Deaktivieren von Konfigurationselementen	525
Neu aktivieren von Konfigurationselementen	526
Konfigurationselemente: Kontakt, Standort und Organisation	526
Erstellen eines CI für ein Basisobjekt	527
Wählen eines Basisobjekts für ein Konfigurationselement	527
Bearbeiten von Configuration Item-Details für ein Basisobjekt.....	528
Bearbeiten von Konfigurationselement-Attributen für ein Basisobjekt	529
Erstellen eines Basisobjekt-Konfigurationselements mit Hilfe von GRLoader	529
CI-Beziehungen	530
CI-Beziehungstypen.....	531
Erstellen eines Beziehungstyps	531
Verwalten von CI-Beziehungen	532
Erstellen von CI-Beziehungen.....	533
Anzeigen von Beziehungen für ein Konfigurationselement.....	534
Deaktivieren von CI-Beziehungen	534
Neuaktivieren einer CI-Beziehung	534
Deaktivieren von CI-Beziehungen (Listenbearbeitung)	535
Deaktivieren von CI-Beziehungen mit Hilfe von GRLoader.....	536
Erneutes Aktivieren von CI-Beziehungen mit Hilfe von GRLoader	537
Löschen von CI-Beziehungen aus der Datenbank.....	538
CI-Beziehungs-Verlauf und -Vergleich.....	538
Versionskontrolle	539
Verwenden von Versionskontrolle.....	540
Datensätze für gemeinsame Assets und CI-Audit-Kontrolle	541
Terminologie der Versionskontrolle.....	541
Datenquellen für Versionskontrollen	545

CA SDM Change Management-Integration	546
CA APM-Integration	547
CI-Versionsmanagement	548
CA SDM Change Management	568
Anzeigen von CI-Attributen in anderen CA-Produkten	569
Verwenden des CMDBf-Viewers	570
CMDB Visualizer.....	570
Durchführen der Ursachenanalyse.....	572
Visualizer-Administration	573
Hinzufügen von ermittelten Assets.....	574
Asset- und CI-Markierungen	575
Abstimmung von CIs	576
MDR-basierte Abstimmung.....	577
Identifizieren und Lösen von mehrdeutigen CIs.....	579
Überprüfen und Ändern von eingehenden Daten mit dem Transaktionsarbeitsbereich (TWA)....	592
Verwalten bereitgestellter Transaktionen	598
Transaktionsarbeitsbereich.....	599
Auffüllen des Transaktionsarbeitsbereichs	601
Aktualisieren von Daten im TWA über die Web-Schnittstelle.....	613
Verwalten von Beziehungstransaktionen	616
Laden von Transaktionen in die CMDB	617
TWA-Administration	619
CA CMDB-Datenwartung	624
CA CMDB-Strukturen für Familie und Klasse	624
Ändern der Familie/Klasse eines einzigen Konfigurationselements.....	625
Ändern der Familie/Klasse einer Liste von Konfigurationselementen	625
Ändern von Konfigurationselement-Familien oder Konfigurationselement-Klassen mit GRLoader	626
Erweitern von CA CMDB.....	627

Kapitel 15: Verwalten von MDRs

641

Was ist ein MDR?	641
MDR-Klassen und MDR-Namen	642
Wie ergänzt ein MDR CA Service Desk Manager?	642
Definition eines MDR für CA Service Desk Manager	643
MDR Launcher	643
Definieren einer URL zum Starten eines MDR	644
Einrichten eines CA APM-MDR-Providers	646
Starten im Kontext von CA CMDB an CA APM	647
Eigenschaften von Configuration Items, die MDR-Zusammenschluss unterstützen.....	647
Föderierte Anlagen-ID	647
MDR Name	648
MDR Class	648

MDR-Definition bei der Installation von CA Cohesion ACM	649
CA Cohesion ACM MDRs	650
Manuelles Verknüpfen eines MDR mit einem CI	651
Automatischer Import aus CA Cohesion	652
Zuordnung von CI zu MDR	652
Verwalten der MDR-Definition.....	653
CA Cohesion ACM-Bericht	654
CI-Import in CA CMDB mit GRLoader	654
Namenskonventionen und Einschränkungen für Configuration Items.....	655
Namenskonventionen für system_name	656
Verwenden des CMDBf-Viewers	657
Aktualisieren von Metadaten Dateien für die CMDBf-Zuordnung.....	658
Anzeigen von MDR-Attributwerten mit CA CMDB-Attributnamen	659
Ausblenden von Attributen des MDR-Providers	660
Definieren von MDR-Attributen ohne CA CMDB-Entsprechungen	661
Definieren von Metadaten des CMDBf-Datenanbieters	661

Kapitel 16: Change Management 663

Change Management in CA Service Desk Manager	663
Change-Management-Komponenten	664
Anzeigen des Change-Kalenders.....	665
CAB-Zuständigkeiten	666
Funktionsweise der CAB-Prozessdefinitionen	667
Zuständigkeiten des Change Managers.....	667
Funktionsweise der Rolle des Changes Managers	668
Definieren der Aufgaben für die Rolle des Change Managers	669
Change-Kategorien, Status und Risikoebenen.....	670
Anzeigen des Change-Scoreboards	671
Definieren von gespeicherten Abfragen für Changes	671
Konfigurieren von Change Manager-Optionen	673
Change-Kalender	673
Hinzufügen von Ablaufplaninformationen zu einem Change – CA	674
iCalendar-Ereignis-Vorlagen	674
Exportieren von Ablaufplänen in iCalendar.....	675
Ablaufplan-Ansichten	676
Konfigurieren von Planungsansichten.....	678
So planen Sie Changes:	688
Beispiel: Verwenden des Change-Schedulers	689
So planen Sie Change-Fenster:	693
Anzeigen von Change-Fenstern.....	694
Zuordnen eines CIs zu einem Wartungsfenster.....	695
Anzeigen von zugeordneten CIs	695

Erstellen eines Beispiel-Ausfallfensters.....	696
Erstellen eines globalen Wartungsfensters.....	697
Konfliktanalyse und Konflikterkennung.....	697
CA Workflow-Visualisierung.....	698
So visualisieren Sie den Workflow:.....	698
Change-Management-Prozessdefinition für CA Workflow.....	700
Komponenten der Change-Management-Prozessdefinition.....	701
Einrichten der Change Management-Vorgangsdefinition.....	702
Funktionsweise der Change Management-Prozessdefinitionen.....	708
ActivityNode Actor not found: Update Object -Service Desk r12 ("ActivityNode"-Akteur nicht gefunden: Objekt -Service Desk r12 aktualisieren").....	720
Change wird nicht geschlossen.....	721
CAB-Konsole und Berichterstattung.....	721
Verwalten von CAB-Gruppen.....	722
Zuweisen von CAB-Gruppen.....	724
CAB-Genehmigungen.....	724
Ändern der CAB-Konsoleneigenschaften.....	725
Change Management-Berichterstellung.....	726
Risikobewertung.....	727
So implementieren Sie die Risikoumfrage:.....	728
Zugreifen auf eine Risikoumfrage direkt über eine URL.....	730
Auswirkungs-Explorer.....	731
Starten von Auswirkungs-Explorer.....	732
Untersuchen von angehängten CIs.....	732
Anzeigen von CIs in Auswirkungs-Explorer.....	733
Hinzufügen von verwandten CIs zu Changes.....	733
Anzeigen der Liste der nachfolgenden Elemente des CI.....	734
Starten von CMDB Visualizer im Auswirkungs-Explorer.....	734
Konfigurieren von Auswirkungs-Explorer.....	735

Kapitel 17: Verwalten von CA Business Intelligence-Berichten 737

CA Business Intelligence-Berichte.....	737
Berichterstellungsszenarios.....	738
Berichtskomponenten.....	739
Berichtsdatenflussdiagramm.....	742
Anzeigen von Berichten in InfoView.....	743
Sicherheit und Autorisierung.....	743
Gruppen und Benutzer.....	744
Universum und Verbindungen mit einem Universum.....	744
Berichtsordner.....	745
Zugriffsebenen.....	747

Verweisen eines vorhandenen CA Business Intelligence-Servers auf einen CA Service Desk Manager-Server	748
Erstellen einer ODBC-Datenquelle	749
Konfigurieren des Universums	750
Exportieren des Universums	750
Einrichten der Datenaufteilungssicherheit für die Berichterstellung	751
Hinzufügen von berechtigten CA Service Desk Manager-Benutzern zur CMC	752
Definieren der Universe-Datenbank-Anmeldeinformationen	752
Einrichten von Datenaufteilungen	753
Replizierte Datenbank für Offline-Berichterstellung	754
Rollenbasierte Berichte	754
Definieren rollenbasierter Berichte für die Rolle	754
Anzeigen neuer Berichte auf der Registerkarte 'Berichte'	756
Webbasierte Berichte	764
Business Objects InfoView-Schnittstelle	764
Navigieren zu Berichten	765
InfoView-Voreinstellungen	765
Planen von Berichten	766
Einrichten der Datenanalyse	767
Speichern und Verteilen von Berichten	767
Dashboard-Berichte	768
Anzeigen von Berichten im Dashboard für den Einsatz im Unternehmen (Operational Dashboard)	769
Ad-hoc-Berichte	769
Web Intelligence-Schnittstelle	770
Funktionsweise der Ad-hoc-Berichterstellung	770
Ad-hoc-Beispielberichte	771
KPIs (Kritische Prozess-Indikatoren)	777
KPI-Typen	778
Vordefinierte KPIs	778
KPI-Daemon	779
System-KPIs	779
Gespeicherte Abfrage-KPI	781
SQL KPIs	782
KPI - Felder	783
Abrufen von Ticket-Daten	784
Problembehandlung	787
Schreiben von CA Business Intelligence-Berichten	789
CA Service Desk Manager-ODBC-Treiber	790
Schreiben von SQL für BusinessObjects-Berichte	791
PDM-Funktionen	792
Attributaliasnamen	794
pdm_isql - interaktives SQL	795

Kapitel 18: Generieren von Berichten in USDK **797**

Berichte erzeugen	797
Datenbankansichten	797
Grundlegende Ansichten	798
Erweiterte Ansichten	800
Einrichten von Berichtsmethoden	801
Berichtsformatierung	801
Ändern der Sortierreihenfolge der Spalten	802
Zusammengefasste Berichte und Detailberichte	802
Analyseberichte	803
Generieren von Berichten zu Anfragen und Issues	803
Generieren von Berichten zu Anfragebereichen und Issue-Kategorien	804
Erstellen von Berichten zur Priorität von Anforderungsbereichen und zur Priorität von Issue-Kategorien	804

Kapitel 19: Verwalten von Knowledge **805**

Knowledge-Management	805
Suchen von Prozeduren für das Knowledge Management	806
Knowledge und Mandantenfähigkeit	806
So richten Sie eine Knowledge Base ein:	807
Importieren von Knowledge-Beispieldaten	808
Überwachen der Knowledge Base	808
Neuindizierung der Knowledge Base	808
Indizieren der Warteschlangeneinstellungen für Batch-Verarbeitung und sofortige Verarbeitung bzw. Entfernen der Indizierung	809
So verwenden Sie Dokumente in der Knowledge Base:	810
Knowledge-Einreichung in CA Service Desk Manager	812
Knowledge-Einreichung über Self-Service	813
Dokument-Attribute	813
Dokumentberechtigungen	813
Bearbeiten der Lösung	814
Vorbereiten der Dokumentveröffentlichung	814
Dokumentveröffentlichung	815
Versionsdokumente	815
Dokumentablauf	816
Archivieren und Bereinigen von Dokumenten	817
Knowledge-Dateien	817
Knowledge-Suche	818
Foren	818
Knowledge-Baumstrukturdokumente	818
Knowledge-Dokument-Ablaufplan	819
Knowledge - Ablaufplanfilter	820

Ansichten von Knowledge-Ablaufplänen	822
Konfigurieren von Planungsansichten.....	823
Zugreifen auf Export/Import	830
So exportieren/importieren Sie Knowledge:	831
Exportieren/Importieren von Dokumenten.....	834
Exportieren/Importieren von Paketen	834
Anzeigen von Export-/Importvorlagen	835
Hilfsprogramm "pdm_ket": Knowledge-Export-Tool	842
Hilfsprogramm "pdm_kit": Knowledge- Import-Tool	843
Exportieren oder Importieren von Knowledge durch Benutzer.....	844
Webservices.....	845

Kapitel 20: Verwalten von Knowledge-Management 847

Knowledge-Verwaltung	847
Suchen von Prozeduren für die Knowledge-Administration.....	848
Rollen und Funktionen von Knowledge-Management	848
Knowledge-Management-Benutzeroberflächen	850
Konfiguration und Verwaltungsfunktionen von Knowledge-Management.....	850
Optionen für Self-Service-Knowledge.....	851
Dokumente und Benutzer	857
So verwalten Sie Rollenberechtigungen und die Dokumentsichtbarkeit:.....	862
Aktionsinhalte	862
Anzeigen von Aktionsinhalten	864
Erstellen von Aktionsinhalten (Aktions-URL)	865
Erstellen von Aktionsinhalt (interner HTML)	866
Bearbeiten von Aktionsinhalten.....	866
Suchen nach Aktionsinhalten	867
Genehmigungsvorgang für Dokumente.....	868
Manager für den Genehmigungsvorgang	869
Festlegen eines Genehmigungsvorgangs für die Dokumentbearbeitung	870
Erstellen einer Genehmigungsprozessvorlage.....	871
Definitionen für den Dokumentstatus.....	874
Automatisierungsrichtlinien	876
Anzeigen von Automatisierungsrichtlinien.....	876
Einrichten von Automatisierungsrichtlinien	878
Erstellen von Automatisierungsrichtlinien	878
Bearbeiten von Automatisierungsrichtlinien	879
Planen von Automatisierungsrichtlinien	880
Anzeigen von Berichten zu Lebenszyklusrichtlinien für Dokumente	880
Knowledge-Dokumentsteuerung	881
Kommentartypen.....	882
Dokumentvorlagen	887

Erstellen von Verknüpfungen für Knowledge-Dokumente	895
Knowledge-Kategorien	898
Erstellen von Knowledge-Kategorien.....	898
Ändern einer Kategorie.....	902
Löschen einer Kategorie	903
Verschieben von Kategorien	905
Kopieren von Kategorien mit Dokumentverknüpfungen	905
Kopieren von Kategorien ohne Dokumentverknüpfungen	906
Verwalten von Kategorieberechtigungen	906
Berichte und Indikatoren	909
Knowledge-Berichtskarte	909
Webbasierte Berichte	911
Rollenbasierte Berichts-Webformulare	911
Suchen.....	911
KT-Such-Engine	912
FAST ESP-Suche.....	925
Empfohlene Dokumente.....	929
Einrichten von Standard-Sucheinstellungen	933
Optionen zur Integration von CA Service Desk Manager	935
Definieren von Feldzuordnungen	935
Definieren der Issue-Suchkonfiguration.....	938
Definieren der Suchkonfiguration für Anfragen/Incidents/Probleme	939
Knowledge-Vorschläge	940
Definieren von Issue-Kategorien	941
Definieren von Anfrage-/Incident-/Problembereichen	942
Konfigurieren von Self-Service-Richtlinien	943
Lösungsumfrage	944
Festlegen der FAQ-Einstellungen.....	945
Festlegen der Einstellungen für Lösungsumfragen	947
Knowledge-Management-Systemeinstellungen	947
Konfigurieren von allgemeinen Einstellungen	948

Kapitel 21: Verwalten von Support-Automatisierung 951

Automatisieren des Supports in Ihrer Umgebung	951
Live-Unterstützung	952
Verwalten von Support-Automatisierung-Analysten.....	954
Starten der Live-Unterstützung durch Analysten.....	955
Konfigurieren von Live-Unterstützung für Analysten.....	957
Verbinden von Endbenutzern mit Unterstützungssitzungen	958
Wie Analysten die Unterstützung für Endbenutzer automatisieren	959
Bereitstellen der Live-Unterstützung durch Analysten.....	959
Support-Automatisierung-Benutzerverwaltung.....	960

Konfigurieren von Rollenberechtigungen	961
Support-Automatisierung anonyme und registrierte Benutzer	962
Konfigurieren von Support-Automatisierung für Gastbenutzer	962
Verwalten der Support-Automatisierung-Zugriffsebenen	964
Support-Automatisierung-Aktivitätsbenachrichtigungsverwaltung	965
Support-Automatisierung-Seitenanpassungen	966
Branding-Verwaltung	967
Verwalten der Lokalisierung	968
Seitenlayoutkonfiguration	968
Support-Automatisierung-Systemeigenschaften	969
Support-Automatisierung-Warteschlangenverwaltung	969
Warteschlangenverwaltung	970
Verwalten von Warteschlangen-Zusammenfassungen	971
Verwalten der Warteschlangen-Stunden	971
Verwaltung von Ticket-Vorlagen	972
Administrationseinstellungen	972
So konfigurieren Sie die Support-Automatisierung-Einstellungen:	972
Anpassen von Support-Automatisierung-Tools	975
Automatisierte Aufgaben	975
Verwalten von Chat-Voreinstellungen	981
Standardanmeldeinformationen	982
Disclaimer	983
Sitzungsprotokoll-Verwaltung	983
Anzeigen des Sitzungsprotokolls	983
Support-Automatisierung-Berichte	984

Anhang A: Beschreibungen der Felder in Ansichten 985

Beschreibungen der Felder in Ansichten	986
View_Act_Log	986
View_Audit_Assignee	988
View_Audit_Group	988
View_Audit_Priority	989
View_Audit_Status	990
View_Change_Act_Log	990
View_Change	992
View_Change_to_Assets	997
View_Change_to_Change_Act_Log	997
View_Change_to_Change_WF	999
View_Change_to_Properties	1001
View_Contact_Full	1002
View_Contact_to_Environment	1005
View_Group	1006

View_Group_to_Contact.....	1007
View_Issue	1007
View_Issue_Act_Log.....	1012
View_Issue_to_Assets	1014
View_Issue_to_Issue_Act_Log	1014
View_Change_to_Request	1016
View_Issue_to_Issue_WF.....	1019
View_Issue_to_Properties	1021
View_Request.....	1022
View_Request_to_Act_Log	1028
View_Request_to_Properties.....	1028

Anhang B: LDAP-Ergebniscodes von RFC 2251 **1031**

LDAP-Rückgabecodes	1031
Rückgabecodes des LDAP-Servers	1031
Rückgabecodes des LDAP-Clients	1037
LDAP-spezifische RFC-Standards	1039

Anhang C: Referenzbefehle **1043**

bop_sinfo – Systeminformationen anzeigen	1045
dbmonitor_nxd – Daemon zur Überwachung von Datenbanken	1046
pdm_backup – Exportieren der Datenbank in eine ASCII-Datei	1048
pdm_cache_refresh – Aktualisieren der Datenbank	1049
pdm_configure – Öffnen des Konfigurationsfensters	1051
pdm_d_refresh – Starten fehlgeschlagener Daemons	1052
pdm_deref – Dereferenzieren von ASCII-Daten	1053
pdm_discimp – Importieren ermittelter Assets	1056
pdm_discupd – Asset-Aktualisierung ermittelt	1058
pdm_edit – Konfigurieren von Serverprozessen	1059
pdm_extract – Extrahieren von Daten aus der Datenbank	1061
pdm_halt – Beenden von Daemons oder Anhalten von Diensten	1064
pdm_init – Starten von Daemons	1065
pdm_key_refresh – Aktualisieren von im Cache gespeicherten Schlüsselinformationen	1066
"pdm_lexutil" – CA Service Desk Manager-Lexika ändern	1066
"pdm_k_reindex" – Dienstprogramm zur Knowledge-Neuindizierung.....	1067
Verwenden von pdm_k_reindex.....	1069
Verfolgen der Neuindizierung.....	1069
Importieren und Neuindizieren	1070
Verwenden von "pdm_k_reindex" mit FAST ESP.....	1070
Indizieren der Warteschlangeneinstellungen für Batch-Verarbeitung und sofortige Verarbeitung bzw. Entfernen der Indizierung.....	1073

pdm_listconn – Auflisten der aktiven Verbindungen.....	1074
pdm_load – Hinzufügen, Aktualisieren und Löschen von Datenbank-Datensätzen	1076
pdm_logfile – Ändern der Cutover-Größe von STDLog	1078
pdm_proctor_init – Starten von Proctor auf sekundären Servern.....	1079
pdm_replace – Ersetzen einer Datenbanktabelle	1079
pdm_restore – Wiederherstellen einer Datenbank	1081
pdm_status – Anzeigen des Status von Daemons oder Prozessen.....	1083
pdm_task – Einstellen der Umgebungsvariablen	1083
pdm_text_cmd – Befehlszeilenschnittstelle für Text-API.....	1084
Beispiele für Eingaben	1086
pdm_uconv – Konvertiert den lokalen Zeichensatz in UTF-8	1087
pdm_userload – Hinzufügen, Aktualisieren und Löschen von Datenbank-Datensätzen	1090
pdm_webstat – Zurückgeben von Webnutzungsstatistiken	1093
report – Generieren von Berichten.....	1097
rpt_srv – Generieren von Berichten	1098
uniconv – Starten des UNIX CA NSM-Event Converter-Daemons	1100

Anhang D: Formulargruppen **1101**

Formulargruppe "Kunden"	1101
Formulargruppe "Mitarbeiter"	1102
Formulargruppe "Analysten"	1104

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, d. h. die Person, die die gesamte Verantwortung für die Verwaltung des Produkts hat. Zu den Aufgaben des Administrators zählen:

- Starten und Anhalten der für den CA Service Desk Manager-Server erforderlichen Dienste
- Einrichten verschiedener Systemkomponenten
- Festlegen der Optionen, die Benutzern 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 Service Desk Manager 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 Service Desk Manager sollten Sie mit Folgendem vertraut sein:

- Betriebsumgebung, auf der CA Service Desk Manager 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 Service Desk Manager beschriebenen Prozesse umfassen:

- Incident Management
- Problemverwaltung
- Change Management
- Anforderungsverwaltung
- Konfigurationsverwaltung
- 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)

[Server-Konfigurationstasks](#) (siehe Seite 28)

[Konfigurieren von TCP/IP](#) (siehe Seite 29)

[Ändern einer Serverkonfiguration](#) (siehe Seite 30)

[ITIL-Konfiguration](#) (siehe Seite 30)

[Starten von sekundären Servern](#) (siehe Seite 37)

[Starten des primären Servers](#) (siehe Seite 38)

[Server Status](#) (siehe Seite 40)

[Konfigurieren von SSL auf Tomcat](#) (siehe Seite 41)

[Bereitstellen von CMDBf-Webservices](#) (siehe Seite 42)

[Beenden eines Servers \(Windows\)](#) (siehe Seite 43)

[Beenden von Servern \(UNIX\)](#) (siehe Seite 43)

Anzahl der Server

Ihre CA Service Desk Manager-Installation hat eine oder mehrere Serverkomponenten, die Sie als Administrator verwalten müssen. Die Anzahl der Server hängt von Ihrem Unternehmen ab. Jede Installation hat einen Primärserver, der die gesamte Funktionsweise von CA Service Desk Manager verwaltet. Installationen können optional einen oder mehr sekundäre Server haben, um bestimmte Funktionen zu verwalten. Nach der Installation von CA Service Desk Manager müssen Sie jeden Computer, auf dem Produktkomponenten ausgeführt werden, konfigurieren.

Zum Beispiel kann Ihre spezielle Konfiguration einen einzelnen Computer umfassen, der als primärer Server fungiert und auf dem alle erforderlichen Services installiert sind. Ihre Installation kann auch über mehrere Computer verteilt sein, von denen jeder eine bestimmte Funktion übernimmt. Ein Computer kann zum Beispiel als Primärserver und als Datenbankserver dienen, während die Web-Schnittstelle auf einem separaten Webserver ausgeführt wird und ein weiterer Computer für die Authentifizierung von Benutzern zuständig ist.

Sie können die Server-Konfiguration als Teil des Installationsprozesses ausführen oder später ausführen. Sie ändern die Konfiguration, wenn Änderungen in Ihrer Umgebung auftreten.

Hinweis: Weitere Informationen zur Architektur dieses Produkts und zu den Konfigurationsoptionen finden Sie im *Implementierungshandbuch*.

Server-Konfigurationstasks

Sie sollten jeden Computer konfigurieren, der zum Ausführen von CA Service Desk Manager vorgesehen ist. Als Administrator konfigurieren Sie den Primärserver, den Sekundärserver und die Client-Installationen. Die anfängliche Konfiguration ist Teil des CA Service Desk Manager-Installationsprozesses.

In CA Service Desk Manager-Umgebungen führen Sie die nachfolgenden Aufgaben aus:

- Konfigurieren der Server
- Starten, Stoppen und Überwachen des Primärservers
- Starten, Stoppen und Überwachen des Sekundärservers (sofern definiert)

Hinweis: CA Service Desk Manager verwendet Ihren Datenbankserver, um Informationen zu speichern und abzurufen. Der Datenbankserver wird als separater Service ausgeführt. Administrative Informationen finden Sie in der Dokumentation zu Ihrem Datenbankserver.

Eine Änderung in der Systemumgebung kann eine Änderung der Serverkonfiguration erforderlich machen. Zum Beispiel können Sie die CA Service Desk Manager-Serverkonfiguration aus den folgenden Gründen ändern:

- Änderungen im Datenbank-Management-System
- Mit "pdm_edit.pl" an der CA Service Desk Manager-Startvorlagendatei durchgeführte Änderungen (ein Feature, mit dem Funktionen hinzugefügt und die Leistung des Unternehmenssystems erhöht werden kann)
- Integration mit einem Webserver wie Tomcat
- Integration mit CA EEM

Konfigurieren von 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. Der Mixed-Modus ist für Clients mit sekundären Servern gedacht, die ein anderes Internetprotokoll als der Primärserver (oder untereinander) 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
```

Ändern einer Serverkonfiguration

Mit dem Konfigurationsdienstprogramm können Sie Änderungen an einer Serverkonfiguration vornehmen.

So ändern Sie eine Serverkonfiguration:

1. Wählen Sie im Windows-Startmenü "Programme", dann "CA", dann "CA CMDB" und anschließend "Konfiguration".
Das Dienstprogramm für die CA Service Desk Manager-Konfiguration wird angezeigt.
2. 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.
3. Folgen Sie den Anweisungen auf dem Bildschirm, um die Installation abzuschließen, und klicken Sie auf "Fertig stellen".
Die Serverkonfiguration wurde geändert.

ITIL-Konfiguration

Information Technology Infrastructure Library (ITIL) ist eine Sammlung der Best Practices für die Verwaltung von Computerrechenzentren. Zusätzlich zur Definition empfohlener Prozesse hat das ITIL-Framework einen weiteren wichtigen Vorteil: die klare Definition von in Rechenzentren gebräuchlicher Terminologie. In der IT-Welt wird der gleiche Begriff oft für verschiedene Dinge verwendet. Manchmal wird ein bestimmter Begriff von unterschiedlichen Personen mit leicht abweichender Bedeutung gebraucht. Mit ITIL lässt sich diese Art von Problem vermeiden.

Folgende Tickettypen stehen zur Verfügung:

- Anforderung
- Change (Änderungsauftrag)
- Issue
- Incident (Störung)
- Problem

Wichtig: CA Service Desk Manager unterstützt nur eine ITIL-Schnittstelle.

Die ITIL-Schnittstelle 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:

- Sie erstellt eine ITIL-Schnittstelle für Ihre CA Service Desk Manager-Installation.
- Sie macht es möglich, dass Ihre CA Service Desk Manager-Datenbank, -Formulare und -Felder von einer Standardinstallation abweichen und stattdessen ITIL-Konventionen entsprechen.

Wichtig! Wenn Sie ein Upgrade für Ihr bestehendes System durchführen, deaktivieren Sie dieses Kontrollkästchen, um die Datenbanktabellen und die Daten beizubehalten. Andernfalls gehen all Ihre bestehenden Daten verloren.

ITIL-Service Disziplinen

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:

- Incident Management
- Problemverwaltung
- Change Management
- Versionsverwaltung
- Konfigurationsverwaltung

CA Service Desk Manager 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 Service Desk Manager behandelt im besonderen das Service Management.

Optionen für die Mitarbeiter- und Gastschnittstelle

Sie können CA Service Desk Manager 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 "Verwaltung".
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 "Verwaltung".

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.

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 Service Desk Manager-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.

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:

- Anforderung
- 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 "Verwaltung".
Die Administrationskonsole wird angezeigt.

2. Klicken Sie auf "Optionsmanager" > "Anfrage-Change-Issue".

Die Liste der Optionen wird angezeigt.

3. Klicken Sie auf "activity_log_security".

Die Seite "Optionsdetails" 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 Auswahl 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_SECURITY { ON_NEW DEFAULT NOW ; } ;  
description STRING $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.

PDA-Schnittstelle

CA Service Desk Manager unterstützt ITIL-Terminologie für die PDA-Schnittstelle (persönlicher digitaler Assistent). Die PDA-Schnittstelle zeigt die folgenden Tickettypen an:

- Incidents
- Probleme
- Anfragen
- Changes
- Issues

Sie können die PDA-Schnittstelle deaktivieren, indem Sie die Zeile
"PDAHtmlPath" in der Konfigurationsdatei auskommentieren. Wenn die PDA-Schnittstelle deaktiviert ist, erhalten Benutzer entsprechend die Web-Schnittstelle für Analysten oder Kunden.

Anfragen nach der PDA-Schnittstelle sind nur für Benutzer vom Typ "Analyst" gültig. Wenn Sie sich an der PDA-Schnittstelle anmelden, wird Ihre Rolle auf die Rolle gesetzt, die Sie verwendet haben, als Sie zuletzt von der standardmäßigen CA Service Desk Manager-Web-Analystenschnittstelle abmeldeten.

Alle Benutzer, die sich typischerweise an der CA Service Desk Manager-Web-Analystenschnittstelle anmelden, können die PDA-Schnittstelle anfordern, indem Sie auf der Anmeldeseite vor ihre *Benutzer-ID* folgendermaßen "pda" setzen:

pda:userid

Zum Beispiel können Sie von einem Nicht-PDA-Gerät wie z. B. ein Desktop-Rechner oder ein Laptop auf die PDA-Schnittstelle zugreifen, indem Sie **pda:Benutzer-ID** und das Kennwort angeben.

Starten von sekundären Servern

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

In einer UNIX-Umgebung starten Sie jeden CA Service Desk Manager-Sekundärserver mit "pdm_proctor_init" über die Befehlszeile.

In einer Windows-Umgebung starten Sie jeden CA Service Desk Manager-Sekundärserver mit Hilfe des Remote-Überwachungsservers.

So starten Sie einen Sekundärserver in Windows:

1. Wählen Sie in der Systemsteuerung die Option "Services" aus.
Das Fenster "Systemsteuerung" wird angezeigt.
2. Wählen Sie den Dienst CA Service Desk Manager-Remote-Proctor und klicken Sie auf "Starten".
Der Service wird gestartet.

Weitere Informationen:

[pdm_proctor_init – Starten von Proctor auf sekundären Servern](#) (siehe Seite 1079)

Starten des primären Servers

Jede CA Service Desk Manager-Installation hat einen Primärserver, der die grundlegende Produktfunktionalität abwickelt.

Wichtig! Wenn Ihre Installation einen oder mehr sekundäre Server einschließt, müssen Sie die sekundären Server vor dem Primärserver starten.

Wählen Sie in der Systemsteuerung den Service "CA Service Desk Manager-Server" aus, und klicken Sie auf "Starten", um den CA Service Desk Manager-Primärserver in einer Windows-Umgebung zu starten. Sie können den Dienst jederzeit starten, oder Sie können ihn so konfigurieren, dass er wie jeder andere Windows-Dienst automatisch gestartet wird.

Starten Sie den CA Service Desk Manager-Server in einer UNIX-Umgebung mit "pdm_init" über die Befehlszeile.

Die folgende Tabelle beschreibt die Prozesse, die automatisch starten, wenn Sie den CA Service Desk Manager-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.
BOP Virtual DB (bpvrtdb_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

Prozess	Beschreibung
Event Manager (ehm_nxd)	Ereignis-Manager
License Manager (license_nxd)	Dient der Sicherheitsverwaltung.
Message Dispatcher (sslump_nxd)	Stellt Meldungen zu.
Notification Manager (nur Windows) (bpnotify_nxd)	Verwaltet Benachrichtigungen in der Windows-Umgebung.
Object Engine (domsrvr)	CA Service Desk Manager-Server
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)	Zeitereignisse und Benachrichtigungen
User Validation (boplgln)	Anmeldung für Anfrageverwaltung
Web Engine (webengine)	Führt die Webservice-Engine 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
EBR Idx Daemon (bpeid_nxd)	Wickelt die EBR-Neuindizierung ab
Multi-site SD Daemon (global_nxd)	Verwaltet die Replikation im Hintergrund für die Verarbeitung an mehreren Standorten
KRC Daemon (krc_daemon)	Verwaltet statistische Berechnungen und Benachrichtigungen für die Knowledge-Berichtskarte

Prozess	Beschreibung
KT Daemon (kt_daemon)	Verwaltet Knowledge-Dokumente (KD-Genehmigungsvorgang, Berechtigungen, Benachrichtigungen usw.)
LDAP virtddb (ldap_virtddb)	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 KTLC (pdm_ktlc)	Verwaltet die Lizenzierung für Knowledge-Management
PDM RPC (PDM_RPC)	Verwaltet Anfragen nach Webservices
Repository Daemon (rep_daemon)	Verarbeitet Repositories 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.

Server Status

Verwenden Sie das Dienstprogramm "pdm_status", um den Status eines in einem beliebigen Betriebssystem ausgeführten primären oder sekundären CA Service Desk Manager-Servers anzuzeigen.

Konfigurieren von SSL auf Tomcat

Sie können Ihr System so konfigurieren, dass es Secure Sockets Layer (SSL) auf einem Tomcat-Webserver verwendet.

So konfigurieren Sie SSL auf einem Tomcat-Server:

1. Wechseln Sie über die Befehlszeile zum JRE-Installationsverzeichnis, und geben Sie den folgenden Befehl ein:

```
bin\keytool -genkey -alias tomcat -keyalg RSA
```

Im Stammverzeichnis des angemeldeten Benutzers wird standardmäßig eine .keystore-Datei erstellt. Sie können während der Erstellung der .keystore-Datei ein anderes Verzeichnis angeben. Stellen Sie bei UNIX sicher, dass das Verzeichnis, in dem die Datei ".keystore" erstellt wird, ausreichende Berechtigungen für den Zugriff von CA Service Desk Manager hat.

Hinweis: Weitere Informationen zum Angeben eines anderen Speicherorts für die .keystore-Datei finden Sie in der Tomcat-Dokumentation.

2. Beantworten Sie die Fragen in den Eingabeaufforderungen entsprechend. Das Standardkennwort ist *changeit*.

Hinweis: Sie können ein vom Standardwert abweichendes Kennwort eingeben. Weitere Informationen finden Sie in der Tomcat-Dokumentation.

3. Bearbeiten Sie die Datei "server.xml", die sich im folgenden Verzeichnis befindet:

```
"NX_ROOT\bopcfg\www\CATALINA_BASE\conf"
```

4. Entfernen Sie die Kommentarsymbole im SSL-Abschnitt, und fügen Sie den Speicherort der .keystore-Datei hinzu, die in Schritt 1 generiert wurde:

```
<!-- Define a SSL Coyote HTTP/1.1 Connector on port 8443 -->
<Connector className="org.apache.coyote.tomcat4.CoyoteConnector"
port="8443" minProcessors="5" maxProcessors="75"
enableLookups="true"
acceptCount="100" debug="0" scheme="https" secure="true"
useURISValidationHack="false" disableUploadTimeout="true">
<Factory className="org.apache.coyote.tomcat4.CoyoteServerSocketFactory"
clientAuth="false" protocol="TLS" keystoreFile="C:\Documents and
Settings\user\.keystore" />
</Connector>
```

5. Verwenden Sie die folgenden Befehle, um den Tomcat-Server neu zu starten:

```
pdm_tomcat_nxd -c stop
pdm_tomcat_nxd -c start
```

6. Verwenden Sie `https://computer_name:8443/CAisd/pdmweb.exe`, um mit SSL auf die CA Service Desk Manager-Web-Schnittstelle zuzugreifen. Sie können die URL des Webservice auf ähnliche Weise ableiten.

Hinweis: Sie können in der Datei "server.xml" einen anderen Port als 8443 angeben.

7. Zeigen Sie das SSL-Zertifikat an, und installieren Sie es, um auf CA Service Desk Manager zuzugreifen.

Das System wird für die Verwendung von Secure Sockets Layer (SSL) auf einem Tomcat-Webserver konfiguriert.

8. (Optional) Wenn Sie auf CA Service Desk Manager mit Internet Explorer zugreifen, und Windows Server 2003 für SSL konfiguriert ist benötigt der Browser zusätzliche Konfiguration und einen Neustart. Deaktivieren Sie unter "Internetoptionen" auf der Registerkarte "Erweitert" die folgenden Optionen im Abschnitt "Sicherheit":

- Auf zurückgezogene Serverzertifikate überprüfen (Neustart erforderlich)
- Verschlüsselte Seiten nicht auf der Festplatte speichern

Nachdem Sie den Browser neu gestartet haben, können Sie auf CA Service Desk Manager über den SSL-aktivierten Tomcat-Server zugreifen.

Bereitstellen von CMDBf-Webservices

Nach der Installation von CA Service Desk Manager können Sie CMDBf-Webservices einsetzen.

So stellen Sie CA CMDB-Webservices bereit:

1. Stellen Sie sicher, dass der Webserver aktiv ist.
2. Navigieren Sie zum Verzeichnis "CMDBHOME\sdk\websvc\CMDBf".
3. Führen Sie die Datei "deploy_cmdbws.bat" aus.

Die CMDBf-Webservices werden bereitgestellt und gestartet.

Beenden eines Servers (Windows)

Sie können einen CA Service Desk Manager-Primär- oder Sekundärserver in einer Windows-Umgebung beenden.

So beenden Sie CA Service Desk Manager-Server in einer Windows-Umgebung:

1. Wählen Sie in der Systemsteuerung die Option "Services" aus.
Das Fenster „Dienste“ wird angezeigt.
2. Wählen Sie den Service aus, den Sie beenden möchten, und klicken Sie auf "Anhalten":

CA Service Desk Manager-Server

Steuert den primären Server.

CA Service Desk Manager Remote Proctor

Steuert einen sekundären Server.

Der Server wird beendet.

Beenden von Servern (UNIX)

Sie können einen CA Service Desk Manager-Primär- oder Sekundärserver in einer UNIX-Umgebung beenden.

So beenden Sie CA Service Desk Manager-Server in einer UNIX-Umgebung:

1. Schließen Sie alle CA Service Desk Manager-Clients.
2. Beenden Sie den Server durch Ausführen des Dienstprogramms "*pdm_halt*".

Der Server wird beendet.

Weitere Informationen:

[pdm_halt – Beenden von Daemons oder Anhalten von Diensten](#) (siehe Seite 1064)

Kapitel 3: Definieren der Geschäftsstruktur

Dieses Kapitel enthält folgende Themen:

[Definieren einer Geschäftsstruktur](#) (siehe Seite 45)

[Definieren der Unternehmensinfrastruktur](#) (siehe Seite 48)

[Unterstützung für Multi-Site](#) (siehe Seite 52)

[Mandantenfähig](#) (siehe Seite 68)

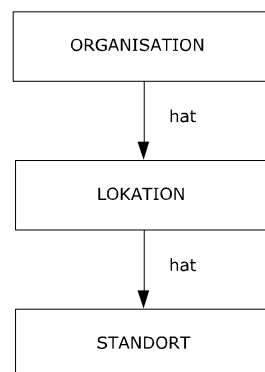
Definieren einer Geschäftsstruktur

Die *Geschäftsstruktur* ist eine logische Darstellung der Organisation, in der CA Service Desk Manager verwendet wird. Sie können die Geschäftsstrukturobjekte Ihren Anforderungen entsprechend einrichten und die Installation so nach Bedarf anpassen.

Sie erstellen die folgenden Objekte, um die Geschäftsstruktur zu definieren:

- Standorte
- Positionen
- Organisationen

Das folgende Diagramm veranschaulicht die Beziehung zwischen den Objekten in der Geschäftsstruktur:



Weil eine Organisation eine Lokation hat bzw. dieser zugeordnet ist und diese Lokation wiederum einen Standort hat, müssen Sie die Objekte in der folgenden Reihenfolge definieren:

1. Standorte
2. Positionen
3. Organisationen

Auf diese Weise können Sie beim Definieren jedes Objekts eine Auswahl aus vorhandenen Objekten auf niedrigeren Ebenen in der Hierarchie treffen.

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

Kontakte

Sie können jede Person definieren, die Ihr System regelmäßig benutzt, z. B. Analysten und Kunden. Diese Personen werden als Kontakte bezeichnet.

Gruppen

Eine Gruppe ist eine Sammlung von Kontakten, die einen bestimmten Verantwortungsbereich innerhalb Ihres Service Desk darstellt. Durch die Definition von Gruppen können Sie Verantwortung zum Lösen eines Tickets zuweisen, wenn diese Verantwortung von mehreren Personen geteilt wird.

Zum Beispiel können Sie die Gruppe "Dallas Personal" einrichten, die für PersonalIssues im Büro in Dallas Ihrer Organisation verantwortlich ist. Wenn ein Mitarbeiter in diesem Büro ein Problem hat, können Sie es zur Lösung der Gruppe „Dallas Personal“ zuordnen.

Sie können einer Gruppe Anfragebereiche, Lokationen und eine Schicht zuweisen, um zu bestimmen, ob und wann die Kontakte in der Gruppe die automatische Zuweisung einer Anfrage annehmen können.

Standorte

Ein *Standort* ist eine Gruppierung von Lokationen. Ein Beispiel für einen Standort ist eine Stadt, in der Ihr Unternehmen eine oder mehrere physische Lokationen hat, oder eine Region, in der Sie einen Kundenstamm haben, für den Sie Unterstützung bieten. Da sich Standorte auf Positionen beziehen, sollten Sie Standorte vor Positionen definieren. Somit können Sie den neuen Standort innerhalb der Lokation verwenden.

Positionen

Lokationen geben einen bestimmten physischen Ort an; mit ihm können Sie Bereiche nachverfolgen und verwalten, die Ihr Unternehmen betreffen, wie z. B. die Adresse eines bestimmten Unternehmens, den Ort eines Büros, ein Universitätsgelände, ein Gebäude, oder sogar eine Etage eines Gebäudes.

Lokationen sind die einzigen Objekte, denen Sie eine physische Adresse zuweisen können. Alle anderen Objekte, wie Organisationen, Configuration Items und Kontakte, leiten ihre Adressen von den zugehörigen Lokationen ab.

Sie sollten Lokationen vor Organisationen definieren; in dieser Reihenfolge können Sie die neue Lokation in der Organisation benutzen.

Sie können Lokationen benutzen, um Anfragen automatisch zuzuweisen. Um die automatische Zuweisung auf der Basis von Lokationen zu aktivieren, weisen Sie Anfragebereichen und Gruppen Lokationen zu. Lokationen für Anfragebereiche stimmen mit einer Anfrage zu einer Lokation überein, die auf der Lokation des Configuration Items der Anfrage oder der Lokation des betroffenen Endbenutzers basiert. Gruppenpositionen werden anschließend verwendet, um eine Gruppe zu wählen, die für die automatische Zuweisung von Anfragen an dieser Position zulässig ist.

Hinweis: Auf der Registerkarte "Administration" werden Tickets als Anfrage-/Incident-/Problembereiche bezeichnet. Sie werden hier einfach kurz als Anfragebereiche bezeichnet.

Organisationen

Organisationen beschreiben interne Abteilungen und Geschäftsbereiche oder externe Firmen, die Tickets, Configuration Item-Klassen und Kontakten zugewiesen werden können (zum Beispiel dienen sie zur Identifizierung des Unternehmens, dem ein Kunde angehört).

Sie können einer Organisation einen Standardservicetyp zuweisen, der bei Angabe der Organisation Tickets automatisch zugewiesen wird. Auf diese Weise können Sie einem Ticket einen bestimmten Service Level auf der Basis der zugewiesenen Organisation zuordnen.

Sie können Configuration Items für Organisationen definieren. Somit können Sie die Hardware, die Software und die Services angeben, die von der Organisation verwendet werden. Durch Verknüpfen von Configuration Items mit einer Organisation (gemeinsame CIs) wird die Funktion ergänzt, mit der Sie CIs direkt mit einem Kontakt verknüpfen können (private CIs). Wenn Sie einen Kontakt als betroffenen Endbenutzer einer Anfrage bestimmen, können Sie anschließend ein CI für die Anfrage aus separaten Listen von gemeinsamen und privaten CIs auswählen.

Definieren der Unternehmensinfrastruktur

Ein wichtiger Aspekt bei der Implementierung Ihres Service Desk mit CA Service Desk Manager 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 Item

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 Diensttyp, 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.

Externe Asset Management-Tools

Sie können Ihre CA Service Desk Manager-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 Service Desk Manager-Tools:

- CA NSM stellt das pdm_nsmimp-Dienstprogramm (nur für Windows) bereit, mit dem CA Service Desk Manager Asset-Informationen hinzugefügt werden können.
- CA Asset Management bietet einen vollständigen Satz von Hardware und Software-Bestandsfunktionen. Wird ein CI im CA Service Desk Manager-Client angezeigt, können Sie auf die Schaltfläche "Asset-Viewer" klicken, um Zusatzinformationen zu dem Asset anzuzeigen.

Die Integration zwischen CA Service Desk Manager 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 Service Desk Manager-Client angezeigt, können Sie auf die Schaltfläche "Asset-Viewer" klicken, um Zusatzinformationen zu dem Asset anzuzeigen.

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

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

Unterstützung für Multi-Site

CA Service Desk Manager kann für den globalen Zugriff konfiguriert werden, so dass Daten für mehrere CA Service Desk Manager-Installationen freigegeben werden können. Beachten Sie dabei die folgenden Situationen:

- Globale Service Desks erfordern mehrere regionale CA Service Desk Manager-Installationen, die unter Umständen nicht dasselbe Ausmaß an Anpassungen oder nicht dieselbe Version aufweisen. Diese regionalen Installationen umspannen oft die ganze Welt und die Analytiker in einer Region bieten auch außerhalb der Geschäftszeit einen Support für Kunden, die in einer anderen Region beheimatet sind. Dies wird auch als "following the sun" (der Sonne folgend) bezeichnet: Analysten müssen zum Service am Kunden in der Lage sein, unabhängig davon, wo der Kunde "beheimatet" ist.
- Zu mehreren regionalen CA Service Desk Manager-Installationen gehören Gruppen von Analytiken, die in mehr als einer regionalen Installation Warteschlangen bearbeiten müssen. Ein Analytiker in einer spezialisierten Gruppe muss die Warteschlange für eine bestimmte Gruppe über alle Installationen hinweg sehen können.

In beiden Fällen müssen die Regeln der Geschäftstätigkeit, die sich zwischen den Installationen manchmal widersprechen, beibehalten werden. Die Unterstützung für mehrere Standorte ermöglicht die Überbrückung dieser getrennten Installationen (Regionen), während die Geschäftsregeln für jede Region beibehalten werden.

Ein Supportanalytiker, der globale Anforderungen behandelt, kann Kontakte über alle Regionen hinweg suchen und sich von einem einzigen Fenster aus den Zugang zu Tickets verschaffen und diese öffnen. Wenn das Ticket tatsächlich erstellt wurde, kann der Analyst auf die entsprechende Region (lokal oder ortsfern) übertragen werden, wo die zutreffenden Geschäftsregeln angewendet werden.

Analytiker, die Tickets mehrerer Regionen behandeln, können außerdem eine Liste von all ihrer Tickets in einem Fenster anzeigen. Beim Zugriff auf Details eines bestimmten Tickets wird ein Analytiker auf die entsprechende Region (in der Nähe oder entfernt) übertragen, wo die zutreffenden Geschäftsregeln verwendet werden.

Mehrere Standorte – Übersicht

Der Service-Support für mehrere Standorte ermöglicht einen globalen (verteilten) Support. Sie können lokale Benutzer über lokale Server unterstützen, aber den Zugriff auf Ihren Server von einer beliebigen Lokation aus ermöglichen.

Der Support für mehrere Standorte bietet die folgenden Möglichkeiten:

- Telefonische Erreichbarkeit des Managements außerhalb der Geschäftszeiten und überregional.
- Support für globale Experten, die mehrere Regionen betreuen.
- Herunterfahren des CA Service Desk Manager-Primärservers bei Wartungsfenstern, ohne dass sich dies auf die übrigen Elemente der Architektur an mehreren Standorten auswirkt

Funktionen von "Mehrere Standorte":

- Durchsetzen von regionalen Geschäftsregeln
- Support für das Öffnen und Überprüfen von Tickets
- Support für globale Analysten bei der Bearbeitung von Warteschlangen über mehrere Regionen hinweg.
- Replizieren von minimalen Daten
- Erlaubt es Regionen, unterschiedliche Wartungsebenen zu haben
- Erlaubt es Regionen, unterschiedliche Sprachversionen zu verwenden

Wichtig! Die Codepage muss auf allen Primärservern identisch sein, um die Verfälschung von Daten zu vermeiden.

Diese Funktionen gehören nicht zu der Option "Mehrere Standorte":

- keine Übertragung von Tickets zwischen Regionen
Support-Tickets verbleiben an dem Standort, an dem sie erstellt wurden.
- keine globale Berichterstellung möglich
Eine eingeschränkte Berichterstellung kann über Globale Warteschlagentabellen erfolgen.
- keine Bearbeitung von replizierten Daten möglich, z. B. Knowledge-Dokumente
replizierte Daten sind schreibgeschützt.

Was Sie wissen müssen

Wenn Sie Unterstützung für mehrere Standorte unter Berücksichtigung der folgenden Information benutzen wollen:

- Führen Sie beim Ändern der IP-Adresse einer teilnehmenden Region eine der folgenden Maßnahmen durch:
 - Führen Sie den Service Desk der Region zurück.
 - Deaktivieren Sie den Datensatz "Globale Region" für diese Region und aktivieren Sie ihn danach wieder.

- Globale Analysten müssen bei allen Regionen die gleiche Anmelde-ID haben.
- Server-Zonen und Aliasnamen ermöglichen es Ihnen, globale Analysten zur Verarbeitung von Issues, wie z. B. Internet, Intranet, DMZ usw., heranzuziehen.
- Sie können kopierte Daten anpassen.
Hinweis: Für diese Anpassung muss eventuell die Datei "global_sd.xml" in "\$NX_ROOT/site/cfg" geändert werden.
Wichtig! Testen Sie Ihre veränderte Datei "global_sd.xml" durch Ausführen von "pdm_global_nxd -x".
- CI-Daten werden nicht kopiert.
- Knowledge-Dokumente werden nicht kopiert.
- Sie müssen die "Lös"-Ressourcen einer Rolle bei der Implementierung an mehreren Standorten aktualisieren.

Wichtig! Konfigurationen mit mehreren Standorten unterscheiden sich von Installationen für mehrere Mandanten. Weitere Informationen zur Mandantenfähigkeit finden Sie unter [Mandantenfähigkeit](#) (siehe Seite 68).

Einrichten eines CA Service Desk Manager-Systems für mehrere Standorte

Sie können auf der Registerkarte "Administration" im Optionsmanager ein System für mehrere Standorte einrichten.

So richten Sie ein System für mehrere Standorte ein:

1. Legen Sie fest, welche Installation die Masterregion bilden soll.
2. (Alle Regionen) Setzen und installieren Sie in "Optionsmanager" > "Mehrere Standorte" die Option "global_name".
3. Wiederverwerten Sie die Services.
Wichtig! Der Wert muss über alle Regionen hinweg eindeutig sein, und darf, nachdem er festgelegt wurde, nicht mehr geändert werden.
4. (Alle Regionen) Definieren Sie in "Service Desk" > "Sequenznummern" Präfixe für Anforderungen, Changes und Issues.

Das Präfix muss für alle Regionen für jeden Tickettyp (z. B. Anfragen) eindeutig sein. Mit eindeutigen Präfixen können Sie auf einfache Weise über alle Regionen hinweg nach Tickets suchen.

5. (Masterregion) Erstellen Sie einen Datensatz für eine Masterregion in "Service Desk" > "Unterstützung für mehrere Standorte" > "Einstellungen für Masterregion" > "Globale Regionen" und markieren Sie das Kontrollkästchen "Master". Führen Sie dann die folgenden Schritte aus:
 - a. Legen Sie einen benutzerfreundlichen Namen fest.
 - b. Stellen Sie die Option "Globaler Name" auf den Wert ein, der in der Option "global_name" festgelegt ist.
 - c. Stellen Sie die Präfixwerte auf den in Schritt 3 festgelegten Wert ein.
 - d. Stellen Sie die Adresse des Primärservers auf den Namen oder die IP-Adresse des Primärservers in der Region ein.
 - e. Stellen Sie die Adresse des Webserver auf den Namen oder die IP-Adresse des Servers ein, zu dem andere Regionen die Verbindung herstellen.
 - f. Bestätigen Sie die URL des Webserver — diese URL sollte sich nicht ändern.
 - g. Stellen Sie den Port des Webserver auf die Portnummer des oben genannten Webserver ein. Bei einer Tomcat-Verbindung kann dies der Wert 8080 sein. Wenn Sie keinen Wert eintragen, ist dies der Standardport für das Webserverprotokoll.
 - h. Stellen Sie das Webserverprotokoll auf die zuvor festgelegte Webserver-Adresse (http oder https) ein.
 - i. Markieren Sie das Kontrollkästchen "Master" (nur beim Masterserver).
6. (Masterregion) Erstellen Sie andere entfernte Regionen ("Service Desk" > "Unterstützung für mehrere Standorte" > "Einstellungen für Masterregion" > "Globale Regionen"). Zur Einstellung von Masterregionen befolgen Sie die Schritte oben.

Nachdem die anderen entfernten Regionen erstellt worden sind, führen Sie "pdm_extract" mit der Tabelle "Global_Servers" aus, um eine Datei zu erstellen (z. B. "pdm_extract" "Global_Servers" > "gservers.dat"), und kopieren Sie diese Datei in die neue(n) entfernte(n) Region(en).
7. (Entfernte Region) Führen Sie "pdm_load" für die Daten der Tabelle "Global_Servers" der aktuellen Masterregionen aus, um die Daten in die Datenbanken der entfernten Regionen zu laden (z. B. "pdm_load" -f "gservers.dat"). Dieses muss für jede entfernte Region nur einmal durchgeführt werden. Nach Herstellen der Verbindung behält die globale Region diese Tabelle bei.
8. (Masterregion) Definieren Sie globale Warteschlangennamen ("Service Desk" > "Unterstützung für mehrere Standorte" > "Einstellungen für Masterregion" > "Globale Regeln").

9. (Alle Regionen) Starten Sie alle globalen Regeln ("Service Desk" > "Unterstützung für mehrere Standorte" > "Einstellungen für lokale Region" > "Globale Regeln").
 - a. Markieren Sie die Schaltflächen "Filter anzeigen", Ändern Sie "Aktiv" zu "Inaktiv", und klicken Sie auf die Schaltfläche "Suche".
 - b. Klicken Sie auf die Schaltfläche "In Liste bearbeiten", um die entsprechenden Felder anzuzeigen.
 - c. Ändern Sie "inaktiv" in "aktiv", klicken auf die Schaltfläche "Alle ändern", um die Aktion für alle Datensätze durchzuführen.
 - d. Klicken Sie auf die Schaltfläche "Speichern", um alle Regeln zu aktivieren.
 - e. Nun beginnt die Datenreplikation zwischen dieser Region und der Masterregion.
10. (Alle Regionen) Ordnen Sie alle lokalen Gruppen den globalen Warteschlangen zu (Registerkarte "Administration" > "Sicherheit" > "Gruppen"). Markieren Sie die zutreffende Gruppe oder erstellen diese und stellen das Feld "Globale Warteschlange" auf den Namen der "Globalen Warteschlange" für diese Gruppe ein.

Das standortübergreifende Festlegen der Einstellungen ist nun abgeschlossen.

Definieren von beteiligten Regionen

Globale Regionen definieren eine Sammlung von Regionen in einem System für mehrere Standorte. Sie können nur eine Region als die Masterregion und die Masterregion als die erste Region definieren.

Hinweis: Wenn Sie in einer Umgebung mit mehreren Standorten die Präfixeinstellungen verwenden möchten, müssen Sie ein Präfix/Suffix für alle Regionen definieren, die zu dem Verbund gehören. Wenn Sie nur für einen der teilnehmenden regionalen Server einen Präfix definieren, ist die globale Ticketsuche anhand des Präfixwertes nicht möglich. Sie müssen daher entweder Präfixwerte für alle teilnehmenden Regionen definieren oder die Definition der Präfixwerte für die teilnehmenden regionalen Server ganz unterlassen.

Die Masterregion überwacht aus Sicherheitsgründen, welche Regionen mit der Masterregion kommunizieren können. Wenn eine nicht definierte Region versucht, eine Verbindung zur Masterregion herzustellen, wird die Anfrage ignoriert. Entfernte Regionen können nur mit der Masterregion und nicht untereinander kommunizieren. Wenn eine Remote-Region versucht, mit einer anderen Remote-Region zu kommunizieren, z. B für einen Authentifizierungs-Bypass, wird die Anforderung zuerst an die Masterregion geschickt. Die Masterregion leitet die Anforderung an die andere Remote-Region weiter. Die Antwort folgt dem umgekehrten Weg zurück zum Anforderer.

Wichtig! Alle Regionen einer Konfiguration für mehrere Standorte müssen auf jedem Primärserver dieselbe Codepage verwenden. Andernfalls ist mit der Verfälschung von Daten zu rechnen.

So definieren Sie beteiligte Regionen

1. Geben Sie in "Optionsmanager" für die Option "global_name" den Namen für diese Region ein. Beispielsweise ist "NA_REGION" der "global_name" für die Region Nordamerika. Dieser Wert muss allen anderen Regionen einmalig sein. Er wird in das Feld "Globaler Name" eingegeben, wenn Sie Regionen definieren, die CA Service Desk Manager für mehrere Standorte angehören. Verändern Sie diese Option nach dem Definieren nicht mehr.
2. Installieren Sie die Option und starten Sie den CA Service Desk Manager-Server neu (erforderlich).
3. Melden Sie sich an der Web-Schnittstelle der Masterregion als Administrator an, und erstellen Sie mit Hilfe der im Optionsmanager definierten Option "global_name" eine globale Region.
4. Bei jeder neuen Region, die nicht als Masterregion definiert ist, müssen Sie eine Kopie der Datendatei "Global_Servers" der Masterregion anlegen und diese Datei wie folgt lokal laden:
 - Führen Sie "pdm_extract Global_Servers > gs.dat" auf dem Server der Masterregion aus, nachdem Sie die Remote-Region zu den globalen Regionen hinzugefügt haben.
 - Kopieren Sie "gs.dat" an die Remote-Region, und laden Sie sie lokal über den Befehl "pdm_load gs.dat". Sie müssen den CA Service Desk Manager-Server nicht neu starten, damit die Änderungen wirksam werden.

Nachdem die Tabelle "Global_Servers" zum ersten Mal geladen wurde, werden die an der Masterregion vorgenommenen Änderungen mit Hilfe der Regel "Pull Global_Servers" auf die Remote-Regionen übertragen, so dass Sie nur einmal eine Kopie der Datendatei "Global_Servers" anlegen müssen.

5. Sie können überprüfen, ob die beiden Regionen miteinander kommunizieren, indem Sie "stdlog" auf einem der beiden Systeme kontrollieren. Suchen Sie nach einem Protokolleintrag wie "Region (region_name) has joined." oder "Connected to Master Region (master_region_name)".

Regeln aktivieren

Globale Tabellenregeln werden verwendet, um Regel zu definieren, welche Tabelle repliziert werden sollen, sofern die Replikation zulässig ist, wie oft die Daten repliziert werden sowie zur Definition einer optionalen Abfrage, um Daten zu filtern, die repliziert werden sollen. Entfernte Regionen definieren, wann und wie oft Daten zur und von der Masterregion repliziert werden. Die Masterregion selbst definiert, welche Regionen zur Kommunikation mit der Masterregion zugelassen werden.

Die Regeln werden entweder als Push- und Pull-Regeln definiert.

- Mit Hilfe der Push-Regel werden die Daten in die betreffende globale Tabelle der Masterregion geschrieben.
- Mit Hilfe der Pull-Regel werden die Daten aus der entsprechenden Tabelle der Masterregion in lokalen Kopien der Tabelle gespeichert.

Jede Push-Regel hat eine entsprechende Pull-Regel, mit zwei Ausnahmen: Globale Server und globale Warteschlangennamen sind nur in der Masterregion definiert und haben daher keine Push-Regeln.

Im Allgemeinen sollten alle mitgelieferten Regeln aktiviert werden. Die Masterregion, in der nur die Push-Regeln aktiviert sein müssen, bildet eine Ausnahme. Die Aktivierung der Pull-Regeln in der Masterregion führt lediglich zu einem Eintrag im Fehlerprotokoll. Die Regel wird nicht gestartet. Wenn die Masterregion keine laufende CA Service Desk Manager-Installation ist, müssen Sie keine Regeln auf dem Master aktivieren.

Um den Replikationsumfang bei globalen Warteschlangen zu verringern, können Sie nur die Daten von "Global_Request_Queue", "Global_Change_Queue" und "Global_Issue_Queue" zur Masterregion und nicht zurück zu den Remote-Regionen replizieren. Analysten, die an globalen Warteschlangen arbeiten, melden sich dann bei der Masterregion an, um sich einen Überblick über die Inhalte ihrer globalen Warteschlangen zu verschaffen.

Standardmäßig sind alle Regeln als "inaktiv" markiert. Dadurch kann ein Administrator festlegen, wann und wie oft Regeln gestartet und ob die Daten zusätzlich gefiltert werden sollen. Bei globaler Datenreplikation laufen die Abfragen mit niedrigerer Priorität als der übrige CA Service Desk Manager, so dass die Replikation während der normalen CA Service Desk Manager-Verarbeitung nur eine geringe Auswirkung hat.

Führen Sie für jede Region, die einer Konfiguration für mehrere Standorte angehört, die folgenden Schritte aus:

1. Melden Sie sich in jeder Region als Administrator an. Navigieren Sie auf der Registerkarte "Administration" unter dem Buch "Unterstützung für mehrere Standorte" zum Buch "Einstellungen für lokale Region"
2. Legen Sie die Suchkriterien "Aktiv" auf "Inaktiv" fest, und wählen Sie "Suche" aus.
3. Überprüfen Sie die Standardeinstellungen für jede Regel in der Liste, legen Sie den Status auf "Aktiv" fest, und klicken Sie auf "Speichern". Wenn der Ablaufplan den Start der Regel vorsieht, startet die Regel unverzüglich.

Das Aktivieren oder Deaktivieren einer Regel wird sofort wirksam. Damit die Regeln ausgeführt werden können, muss eine Verbindung zur Masterregion bestehen. Bei einer Unterbrechung der Verbindung zur Masterregion wird die Replikation ausgesetzt, bis die Verbindung wiederhergestellt ist.

Einrichten von globalen Gruppen

Um den Benutzern Informationen von allen an einer globalen Konfiguration beteiligten Systemen anzuzeigen, wird eine Teilmenge der Daten aus Kontakt-, Organisations-, Lokations-, Produkt-, Anfrage-, Change- und Issue-Tabellen in neueren, kleineren Tabellen erfasst. Diese Zusammenfassungen werden regelmäßig unter den teilnehmenden Systemen repliziert, um die Effizienz und Leistung zu verbessern. Wenn Analytiker die übrigen Daten ansehen müssen, können zu dem jeweiligen System navigieren, um Zugang zu diesen Daten zu erlangen.

Globale Gruppen müssen definiert werden, damit die Replikation von Daten die globalen Warteschlangen (Anfrage, Change oder Issue) unterstützen kann. Es werden nur Tickets repliziert, die globalen Gruppen zugewiesen sind. Nachdem eine Masterregion definiert wurde, können Sie in dieser nur globale Gruppen definieren.

So definieren Sie eine globale Gruppe:

1. Navigieren Sie auf der Registerkarte "Administration" der Masterregion zu "Unterstützung für mehrere Standorte" > "Einstellungen für Masterregion" > "Globale Warteschlangennamen".
2. Klicken Sie auf "Neu erstellen".

3. Geben Sie den Namen ein, den Sie dieser Warteschlange zuweisen wollen, und klicken Sie auf "Speichern".

Die globale Gruppe wird erstellt.

So weisen Sie eine Gruppe einer globalen Warteschlange zu:

1. Navigieren Sie auf der Registerkarte "Administration" zu "Sicherheit" > "Kontakte".
2. Suchen Sie die Gruppe, die Sie mit der globalen Warteschlange verknüpfen möchten, und klicken Sie auf "Bearbeiten".
3. Wählen Sie den Wert "Globale Warteschlange" aus, und klicken Sie auf "Speichern".

Alle zukünftig erstellten Tickets, die dieser Gruppe zugewiesen werden, sind in die Replikation einbezogen.

Anpassen des Replikationsvorgangs

Sie können den Replikationsvorgang anpassen, um weitere Spalten bei vorhandenen Tabellen oder auch neue Tabellen hinzuzufügen.

Führen Sie für alle Anpassungen für Datenreplikation die folgenden Aufgaben durch:

1. [Ändern der Datei "global_sd.xml"](#) (siehe Seite 61)
2. [Testen der Datei "global_sd.xml"](#) (siehe Seite 64)

Führen Sie für neue Tabellen die folgenden Schritte durch:

1. [Hinzufügen von neuen globalen Zuordnungen](#) (siehe Seite 64)
2. [Hinzufügen von neuen globalen Regeln](#) (siehe Seite 65)

Ändern der Datei "global_sd.xml"

In der Datei "global_sd.xml" werden die Tabellen definiert, die für die Replikation zur Verfügung stehen und wie sie zwischen den Regionen zugeordnet werden. Diese Datei befindet sich in "\$NX_ROOT/site/cfg/global_sd.xml" und wird vom Prozess "pdm_global_nxd" verwendet. Nach Änderungen in dieser Datei müssen Sie die CA Service Desk Manager-Services neu starten, damit die Änderungen in Kraft treten.

Die Datei "global_sd.xml" enthält die folgenden Hauptabschnitte:

Tabellen

Definiert alle Tabellen, die Daten im Rahmen des Replikationsvorgangs bereitstellen oder annehmen.

Zuordnungen

Definiert Zuordnungen der Tabellen, die Daten bereitstellen, und der Tabelle, die die Daten speichert.

Tabellenzuordnungen zwischen Regionen müssen nicht in derselben Weise definiert werden, obwohl es dann leichter ist, Unterschiede zu erkennen.

Hinweis: Sie müssen sich mit XML auskennen, bevor Sie Anpassungen vornehmen, denn falsch ausgeführte Änderungen an der Datei "global_sd.xml" können dazu führen, dass die Replikation hängen bleibt.

Verfahren Sie wie folgt, um die Datei "global_sd.xml" zu ändern:

1. Legen Sie eine Sicherungskopie der Datei an, bevor Sie Änderungen durchführen.
2. Verwenden Sie einen Standardtexteditor, z. B. Notizblock unter Windows oder vi unter UNIX.
3. Verwenden Sie eine vorhandene Definition als Beispiel.
4. Speichern Sie Änderungen im Nur-Text-Format, nicht als UNICODE oder formatiert.

Aufbau der Datei "global_sd.xml"

Die Datei "global_sd.xml" enthält die folgenden Abschnitte:

<GlobalMaps>

(Erforderlich) Kennzeichnet, dass diese XML-Datei der globalen Zuordnung dient. Ändern Sie diesen Eintrag nicht.

<Tables>

Führt die Tabellendefinitionen auf, die an der Replikation beteiligt sind.

<Table name="xx" factory="xx">

Definiert eine Tabellendefinition und besteht aus mehreren Spaltendefinitionen.

Name

(Erforderlich) Muss den Wert aufweisen, der in der Datei "ddict.sch" definiert ist.

Factory

(Erforderlich) Der Objektname, der in den .maj- oder .mod-Dateien dieser Tabelle definiert ist.

<Column name="xx" [primary_key="true"] [update_key="true"] [last_mod_date="true"] [map_to_name="yy"] [set_system_id="true"] [set_id="true"]>

Definiert eine Spalte in der Tabellendefinition.

Name

(Erforderlich) Der tatsächliche Name der Spalte gemäß der Definition für diese Tabelle in der Datei "ddict.sch".

Primary_key

(Optional) Legt fest, dass diese Spalte der Primärschlüssel für diese Tabelle ist. Es kann nur eine Spalte als "primary_key" definiert werden.

Update_key

(Optional) Kennzeichnet, dass diese Spalte in der Zielregion verwendet wird, um zu bestimmen, ob eine Zeile bereits existiert. Es können bis zu zwei Spalten pro Tabelle als "update_key" definiert werden.

Last_mod_date

(Optional) Legt fest, dass diese Spalte das Datum der letzten Änderung dieser Zeile enthält. Alle Tabellen müssen eine Spalte mit der Definition "last_mod_date" enthalten, da hauptsächlich anhand dieser Spalte bestimmt wird, ob eine Zeile repliziert wurde.

Map_to_name

(Optional) Ermöglicht das Umbenennen (oder Zuordnen) von Spalten in der Definition der Zieltabelle.

Set_system_id

(Optional) Beim "Push"-Vorgang zur Masterregion wird diese Spalte, gemäß der Definition in der Tabelle "Global_Servers" für die Region, auf die "remote_system_id" der Quelle gesetzt.

Set_id

(Optional) Beim "Push"-Vorgang zur Masterregion enthält diese Spalte einen neuen, auf den Master zugewiesenen, ID-Wert.

<Maps>

Führt die in der Replikation verwendeten Zuordnungsdefinitionen auf.

<Map name="xx" direction="ToMaster | FromMaster">

Definiert eine Replikationszuordnung.

Name

(Erforderlich) Definiert den Namen dieser Zuordnung. Auf diesen Namen wird in der Tabelle "Global_Table_Map" " map_definition" verwiesen.

Richtung

(Erforderlich) Legt die Richtung fest, die in dieser Zuordnung zum Replizieren von Daten verwendet wird. "ToMaster" fügt Daten in der Masterregion ein. "FromMaster" ruft Daten aus der Masterregion ab.

<From_Table table_name="xx">

Definiert die Quelltabellen, aus denen Daten kopiert werden. In einer Zuordnung können zwei "From_Table"-Definitionen vorhanden sein. Zwei Definitionen ermöglichen die Kombination von Daten aus zwei Tabellen in einer Zieltabelle.

Table_name

(Erforderlich) Definiert den Namen der Tabellendefinition. Diese Tabelle muss im Abschnitt "Tabellen" oben definiert werden.

<To_Table table_name="xx">

Definiert die Zieltabelle, in die die Daten kopiert werden. Pro Zuordnung muss eine der Einheiten vorhanden sein.

Table_name

(Erforderlich) Definiert den Namen der Tabellendefinition. Diese Tabelle muss im Abschnitt "Tabellen" oben definiert werden.

<Where_Clause clause="xx">

Wenn zwei Tabellen eine Quelle definieren, wird durch diese Einheit die Where-Klausel zum Verbinden der beiden Tabellen definiert. Pro Zuordnung muss eine der Einheiten vorhanden sein.

Clause

(Erforderlich) Mit dieser SQL-Klausel werden zwei Tabellen verbunden. Diese Eigenschaft muss existieren, kann aber eine leere Zeichenfolge sein.

<Order_By table_name="xx" column_name="yy">

Definiert die Reihenfolge, in der die Zeilen repliziert werden. Dies muss das Datum der letzten Änderung in der "From_Table" sein. Pro Zuordnung muss eine der Einheiten vorhanden sein.

Table_name

(Erforderlich) Der Tabellename aus einer der "From_Table"-Einheiten.

Column_name

(Erforderlich) Der Name der Spalte aus "Table_name", die das Datum der letzten Änderung angibt.

Testen der Datei "global_sd.xml"

Nach den Änderungen an der Datei "global_sd.xml" können Sie die Datei testen, um sich zu vergewissern, ob die Änderungen korrekt sind. Starten Sie den folgenden Befehl von der Befehlszeile auf dem Primärserver:

```
pdm_global_nxd -X
```

Für die Ausführung des Befehls ist es unerheblich, wenn die CA Service Desk Manager-Dienste laufen.

Wenn keine Fehler entdeckt werden, wird eine Meldung ausgegeben, dass keine Fehler in XML-Konfigurationsdatei aufgetreten sind. Wenn Fehler entdeckt werden, wird eine Meldung ausgegeben, dass Fehler in XML-Konfigurationsdatei aufgetreten sind. Eine Liste aller Fehler ist im aktuellen Protokoll *stdlog* enthalten.

Sind in der Datei "global_sd.xml" 2 Fehler enthalten, wenn die CA Service Desk Manager-Dienste gestartet werden, dann findet keine Datenreplikation statt. Starten Sie die Dienste nach der Korrektur der Datei "global_sd.xml" wieder, um die Datenreplikation erneut zu starten.

Hinzufügen von neuen globalen Zuordnungen

Um neue Zuordnungen in Regeln definieren zu können, müssen sie außerdem in der Tabelle "Global_Table_Map" definiert werden. Diese Tabelle enthält die in der Datei "global_sd.xml" definierten Zuordnungen, die für Regeln zur Verfügung stehen.

So erstellen Sie eine neue globale Zuordnung:

1. Wählen Sie auf der Registerkarte "Administration" die Option "Service Desk" > "Unterstützung für mehrere Standorte" > "Einstellungen für lokale Region" > "Globale Zuordnungen" aus.
2. Markieren Sie "Neu erstellen", um einen neuen Eintrag zu erstellen.

3. Geben Sie in einem Namen und eine optionale Beschreibung ein.

Hinweis: Das Feld "Zuordnungsdefinition" muss denselben Namen enthalten wie der Zuordnungsname in der Datei "global_sd.xml".

4. Klicken Sie auf "Speichern".

Die globale Zuordnung wird der Tabelle "Global_Table_Map" hinzugefügt.

Globale Regeln

Wenn eine "Global_Table_Map" sowohl in der Datei "global_sd.xml" als auch in der Tabelle "Global_Table_Map" definiert ist, kann sie in einer globalen Regel verwendet werden. Zu einer globalen Zuordnung können mehrere globale Regeln definiert sein. Mehrere Definitionen können in den folgenden Situationen nützlich sein:

- Eventuell möchten Sie in Spitzenzeiten des Tages die Anzahl der Abfragen nach Änderungen reduzieren. Sie möchten beispielsweise zwischen 7:00 Uhr und 10:00 Uhr eine längere Wiederholung als während des restlichen Tages benötigt. In diesem Fall würden Sie zwei Regeln mit zwei verschiedenen Schichten und zwei verschiedenen Intervallen erstellen.
- Eventuell möchten verschiedene Filter (weitere Abfrage) auf die verschiedenen Regeln anwenden. Sie möchten zum Beispiel, dass Anforderungen mit der Priorität 1 schnell und solche mit anderen Prioritäten in größerem Zeitabstand repliziert werden. In diesem Fall können Sie zwei Regeln mit einer jeweils anderen "Zusätzlichen Abfrage" und unterschiedlichen Zeitabständen erstellen.

Sie können neue Regeln erstellen oder vorhandene Regeln aktualisieren, wenn Sie auf der Registerkarte "Administration" die Option "Service Desk" > "Unterstützung für mehrere Standorte" > "Einstellungen für lokale Region" > "Globale Regeln" auswählen.

Konfigurieren von Serverzonen und Server-Aliasnamen

Mithilfe von Server-Zonen und Server-Aliasnamen können globale Analysten auf Web-Schnittstellen in verschiedenen Regionen zugreifen. Netzwerkkonfigurationen und Firewalls können Servernamen oder IP-Adressen von allen Standorten aus unerreichbar machen. Zur Verringerung dieses Problems können Sie einen Server-Aliasnamen erstellen, um einen Servernamen in einen anderen Namen oder eine IP-Adresse umzuwandeln. Ist ein Aliasname in einer bestimmten Server-Zone nicht definiert, verwendet das System den für die globale Region definierten Namen des Webserver.

Mithilfe von Server-Zonen können Sie Sammlungen von Server-Aliasnamen für unterschiedliche Situationen definieren. Die Internet- oder Intranet-Server-Zonen sind der verfügbare Standard. Sie können diese entweder umbenennen oder neue erstellen. Beispielsweise können Sie eine Sammlung von Aliasnamen für den Intranet-Zugang zu CA Service Desk Manager und eine andere für den Internet-Zugang zu CA Service Desk Manager erstellen. Ein globaler Analyst kann dann eine Server-Zone ändern, indem er die Einstellung "Aktive Zone" in seinen Web-Voreinstellungen ändert (Service Desk-Menü: "Ansicht" > "Voreinstellungen").

Hinweis: Server-Zonen und Server-Aliasnamen werden lokal für die Region definiert. Änderungen an diesen Tabellen stehen anderen Regionen nicht zur Verfügung.

So erstellen Sie eine Server-Zone:

1. Wählen Sie "Unterstützung für mehrere Standorte" > "Einstellungen für lokale Region" > "Server-Zonen" aus.
2. Klicken Sie auf "Neu erstellen".
3. Geben Sie den Namen der Zone ein, die Sie definieren.
4. (Optional) Wählen Sie die Standardeinstellung, um eine Standard-Server-Zone festzulegen.
5. Klicken Sie auf "Speichern".

Das System erstellt die Server-Zone.

So erstellen Sie einen Server-Alias:

1. Wählen Sie "Unterstützung für mehrere Standorte" > "Einstellungen für lokale Region" > "Server-Aliasnamen" aus.
2. Klicken Sie auf "Neu erstellen".

3. Geben Sie unter "Aliasname" den Namen des Servers ein, den Sie überschreiben möchten.
4. Markieren Sie die Zone, der Sie diesen Aliasnamen zuordnen möchten.
5. Geben Sie unter "Hostadresse" den neuen Hostnamen oder die IP-Adresse ein, dem bzw. der Sie die umgewandelte Zone zuordnen möchten, und klicken Sie dann auf "Speichern".

Das System erstellt den Server-Aliasnamen.

Aktualisieren von Rollen für Los: Ressourcen

Sie müssen die Los: Ressourcen Ihrer Rollen aktualisieren, wenn Sie die Unterstützung für mehrere Standorte implementieren. Dies gibt Ihnen die Möglichkeit, nur bestimmten Rollen das Verwenden von globalen Tickets zu gestatten.

So aktualisieren Sie eine Rolle für Los: Ressourcen:

1. Navigieren Sie zu "Sicherheits- und Rollenmanagement" > "Rollenmanagement" > "Rollenliste".
Die Rollenliste wird angezeigt.
2. Klicken Sie auf einen Rollennamen. Z. B auf "Administrator".
Die Seite "Rolle - Detail" wird angezeigt.
3. Klicken Sie auf die Registerkarte "Los: Ressourcen" und anschließend auf "Los: Ressourcen aktualisieren".
4. Fügen Sie der Rolle die geeigneten Los: Ressourcen hinzu.
5. Klicken Sie auf "Speichern".

Beispiele für den Einsatz von Multi-Site

Beispiel 1: Globaler Annehmer von Anrufen - Neue Anforderung

Während der Anzeige des globalen Ad-hoc-Profiles erhält der Analyst einen Anruf von einem Kunden. Der Analytiker gibt die Suchkriterien ein, um den Kunden ausfindig zu machen und klickt auf "Suche". Mithilfe der in der Liste enthaltenen Informationen markiert der Analytiker die entsprechende Kontaktzeile. Die Felder "Ausgewählter Kontakt" und "Remote-System" werden automatisch ausgefüllt, und die Schaltfläche "Zum System des Kontakts wechseln" wird aktiv. Der Analyst füllt das Notizblock Feld nach Bedarf aus und klickt auf "Anfrage erstellen". Ein neues Anfrageformular wird geöffnet, in dem der Name des Kontakts und die Beschreibung aus den Notizblock-Informationen ausgefüllt werden. Der Analyst bearbeitet dann ganz normal die Anfrage und klickt auf "Speichern", um die neue Anfrage zu erstellen.

Beispiel 2: Globaler Annahmer von Anrufen - Vorhandene Anforderung

Während der Anzeige eines beliebigen Formulars, einschließlich des globalen Ad-hoc-Profiles, erhält der Analyst einen Rückruf zu Anfrage "NA: 1234". Der Analyst gibt neben der Schaltfläche "Los" "NA:1234" ein, wählt "Globale Anfragen" und klickt auf "Los". Die Anfrage entweder von der Remote- oder der lokalen Region wird angezeigt, und der Analyst kann die Anfrage auf normale Weise verarbeiten.

Beispiel 3: Globaler Analytiker - Globale Anforderungswarteschlange verarbeiten

Ein Analytiker, der einer Globalen Gruppe zugeordnet ist, richtet sein Scoreboard mit einer gespeicherten Abfrage ein, die nur seine globalen Anforderungen zeigt. Durch Markieren des Scoreboards-Elements werden die Anforderungen zu der gespeicherten Abfrage im rechten Fenster des Browsers aufgeführt. Durch Markieren eines der Elemente in der Liste werden die Anforderungsdetails über das System angezeigt, in dem die Anforderung erstellt wurde.

Mandantenfähig

Mit *Mandantenfähigkeit* können mehrere unabhängige Mandanten (und ihre Benutzer) eine einzige Implementierung von CA Service Desk Manager gemeinsam nutzen. Mandantenbenutzer 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 Service Desk Manager-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*.

Dienst-Provider

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

CA Service Desk Manager 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 Service Desk Manager-Aufgaben ausführen:

- Festlegen von CA Service Desk Manager-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 70)

[Mandantenzugriff](#) (siehe Seite 73)

[Erstellen eines Mandanten](#) (siehe Seite 85)

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 Service Desk Manager-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 Service Desk Manager, nicht der DBMS, durchgesetzt). Alle Daten in diesen Objekten sind mit individuellen Mandanten verbunden. Es gibt keine öffentlichen Daten.

Beispiele: Tickettabellen (Anfrage, 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 Service Desk Manager 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 Service Desk Manager, 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 Benutzer, der ein Objekt erstellt, Aktualisierungszugriff auf mehrfache Mandanten hat, muss der Benutzer 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 Service Desk Manager-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 Mandantenvalidierungsregeln 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-Benutzer steuert diese Autorisierung.

Hinweis: Wenn CA Service Desk Manager 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 Service Desk Manager-Installation.
- **Aufbau:** Mandantenfähigkeits-Merkmale bestehen für Administratoren, so dass mandantenbezogene Objekte und Attribute sichtbar und editierbar sind. CA Service Desk Manager 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 Service Desk Manager zu beeinträchtigen.
- **Aktiviert** - Die Mandantenfähigkeit ist voll einsatzbereit. Alle Benutzer sehen die für Sie geltenden Änderungen der Benutzeroberfläche, und CA Service Desk Manager 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.

Dienst-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. Dieses 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 Service Desk Manager-Benutzers bestimmt sowohl die Zugriffsautorisierung als auch die Anwenderschnittstelle. Der Satz an Rollen, die Benutzern zur Verfügung stehen, hängt von deren Zugriffstyp ab. Mit Mandantenfähigkeit können Sie den Mandanten oder die Mandantengruppe steuern, auf die ein Benutzer 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 Service Desk Manager erlaubt einem Benutzer 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 Benutzer mit "Alle Mandanten"-Zugriff ein Objekt erstellen, müssen sie für CA Service Desk Manager 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 Service Desk Manager beschränkt einen Benutzer 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 gilt sowohl für Mandantenzugriff als auch für Mandantenschreibzugriff.

Mandantengruppe

Legt den Mandantenzugriff einer Rolle auf eine benutzerdefinierte oder vom System gepflegte Mandantengruppe fest. Wenn die Mandantengruppen-Möglichkeit ausgewählt ist, erscheint ein zweites Feld auf der Web-Oberfläche, mit der eine bestimmte Mandantengruppe ausgewählt werden kann. CA Service Desk Manager beschränkt einen Benutzer 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 Benutzer mit Mandantengruppenzugriff ein Objekt erstellt, muss er für CA Service Desk Manager den Mandanten für das neue Objekt auswählen. Diese Auswahl gilt sowohl für Mandantenzugriff als auch für Mandantenschreibzugriff.

Mandant des Kontakts

Legt den Mandantenzugriff einer Rolle auf den Mandanten des benutzenden Kontakts fest. CA Service Desk Manager beschränkt einen Benutzer 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 Benutzer 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 Service Desk Manager beschränkt einen Benutzer 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 Service Desk Manager beschränkt einen Benutzer 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 Service Desk Manager beschränkt einen Benutzer 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 Benutzer können öffentliche Daten ungeachtet der Zugriffsrechte ihrer gegenwärtigen Rolle anzeigen. Das Kontrollkästchen "Öffentlich aktualisieren" steuert, ob ein Benutzer des Service Providers in der Rolle öffentliche Daten erstellen oder aktualisieren darf. Mandantenbenutzer (Benutzer, 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 76)

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 Service Desk Manager 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 Service Desk Manager 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 77)

So konfigurieren Sie die Nutzungsbedingungen

Wenn sich der Endbenutzer bei CA Service Desk Manager 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 Service Desk Manager fortfahren kann. Wenn der Endbenutzer die Nutzungsbedingungen akzeptiert, fährt CA Service Desk Manager mit der Anmeldung fort und zeigt das Hauptformular an. Wenn der Benutzer die Nutzungsbedingungen nicht akzeptiert, weist CA Service Desk Manager 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 Service Desk Manager die Nutzungsbedingungen der direkt und indirekt übergeordneten Elemente des Mandanten an. Wenn auf diese Weise keine Nutzungsbedingungen gefunden werden, fährt CA Service Desk Manager mit der Anmeldung fort. Wenn Sie einen Mandanten mit leeren Nutzungsbedingungen konfigurieren, fährt CA Service Desk Manager 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-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 Service Desk Manager-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 Mandanten 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 Service Desk Manager 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 Service Desk Manager 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 Service Desk Manager-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 Service Desk Manager-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.

Dienst-Provider

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

Mandantennummer

(Nur zur Information) Zeigt die Mandantennummer an. Dieses Feld ist wird nicht von CA Service Desk Manager 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 benutzerdefinierten 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".
2. Klicken Sie auf "Mandanten".
Die Liste der Mandanten 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 Liste der Mandanten 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 Service Desk Manager 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 Liste der Mandanten 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 Service Desk Manager 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".

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".
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 Service Desk Manager 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 Service Desk Manager 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 Service Desk Manager automatisch alle Mandanten implizierende Felder, die Verweise auf Objekte enthalten, welche zum vorherigen Mandanten gehören.

CA Service Desk Manager 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 einen 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-Produkt (z. B. CA APM) oder aus der Befehlszeilenschnittstelle erstellen, ist das Objekt öffentlich.

Weitere Informationen:

[Erstellen eines Mandantenobjekts](#) (siehe Seite 93)

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 94)

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 4: Richtlinie zur Implementierung:

Dieses Kapitel enthält folgende Themen:

[Implementieren von Richtlinien](#) (siehe Seite 95)
[Benachrichtigungen](#) (siehe Seite 95)
[E-Mail-Administration](#) (siehe Seite 137)
[Service Level Agreements \(Dienstverträge\)](#) (siehe Seite 161)
[Sicherheit](#) (siehe Seite 175)
[Benutzerauthentifizierung](#) (siehe Seite 188)
[Interne Protokolle](#) (siehe Seite 192)
[CA Service Desk Manager-Integration](#) (siehe Seite 192)
[Zuordnungen von Datenpartitionen](#) (siehe Seite 193)
[Umfragen](#) (siehe Seite 200)
[Webservices](#) (siehe Seite 203)

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 Service Desk Manager 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 Ereignissen (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 Ereignis auftritt, erzeugt CA Service Desk Manager eine Benachrichtigungsmeldung, die Folgendes ausführt:

- Identifizieren der Ticketaktivität oder des Ereignisses
- 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.

Aktivitätszuordnungen

Sie können Aktivitätstypen mit einem Attribut eines Objekts verknüpfen. Aktivitätstypen ermöglichen Folgendes:

- Nachverfolgen und Berichten über Änderungen an einem Objektattribut.
- Markieren von Aktivitätszuordnung als intern.

Interne Aktivitätszuordnungen beschränken Benachrichtigungen auf jene Kontakte, deren Zugriffstyp es erlaubt, interne Protokolle anzuzeigen. Kontakte, die interne Protokolle nicht anzeigen dürfen, werden nicht benachrichtigt, selbst wenn sie ansonsten als Empfänger der Benachrichtigung aufgeführt sind. Alle zukünftigen mit der zugeordneten Aktivität erstellten Aktivitätsprotokolle werden so als intern markiert.

Hinweis: Ein Objektattribut kann nur eine Aktivitätszuordnung erhalten.

Aktivitätsbenachrichtigungen

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. Aktivitätsbenachrichtigungen identifizieren die Arten von Aktivitäten, die automatische Benachrichtigungen für Tickets verursachen können. Sie können eine Benachrichtigung definieren, die für eine bestimmte Aktivität gesendet wird. Zum Beispiel können Sie zur zusätzlichen Information eine E-Mail-Benachrichtigung an einen betroffenen Benutzer senden. Der Benutzer kann auf die E-Mail mit den durch ein Gerät wie ein PDA angeforderten Informationen antworten. Sogar tägliche Aktivitäten wie zum Beispiel ein Rückruf, Abbrechen oder Schließen eines Datensatzes, Erhöhen der Priorität oder Aktualisieren eines Status können dazu führen, dass eine Benachrichtigung gesendet wird.

In der Regel geben diese Aktivitätsbenachrichtigungen den Beginn oder Abschluss einer Aktion an, wovon Sie Mitarbeiter in Schlüsselpositionen benachrichtigen möchten, zum Beispiel, wenn Tickets eskaliert, übertragen oder überwacht werden. Wenn eine Ticketaktivität stattfindet, prüft CA Service Desk Manager, ob die automatische Benachrichtigung für die Aktivität konfiguriert ist. Wenn ja, definiert die Aktivitätsbenachrichtigung, welche Nachricht an den Benachrichtigungsprozess zu senden ist.

Sie können auch folgende Aktionen für eine Aktivitätsbenachrichtigung durchführen:

- Mit Benachrichtigungsregeln können Sie Richtlinien für das Senden von Benachrichtigungen festlegen. Richten Sie zum Beispiel eine Aktivitätsbenachrichtigung ein, die den vorherigen Zuständigen (oder die Gruppe) benachrichtigt, wenn sich etwas an einem Ticket ändert.
- Richten Sie eine manuelle Aktivitätsbenachrichtigung ein, die ein Ticket aktualisiert, wenn der Benutzer antwortet.

Hinweis: Sie können keine unterschiedlichen Aktivitätsbenachrichtigungen für manuelle Benachrichtigungen pro Mandant oder eine Kopie einer Aktivitätsbenachrichtigung für manuelle Benachrichtigungen pflegen.

- Hängen Sie Ereignisse an.

Weitere Informationen:

[Interne Protokolle](#) (siehe Seite 192)

[Benachrichtigungsregeln](#) (siehe Seite 107)

[Benachrichtigungen an vorherige Zuständige](#) (siehe Seite 127)

[Benachrichtigungen für Configuration Items](#) (siehe Seite 34)

[Funktionsweise von Aktivitätsbenachrichtigungen](#) (siehe Seite 98)

Funktionsweise von Aktivitätsbenachrichtigungen

Sie können eine Benachrichtigung definieren, die für eine bestimmte Aktivität gesendet wird. Aktivitätsbenachrichtigungen können für Anfragen, Incidents, Probleme, Changes, Issues, verwaltete Umfragen, Knowledge-Dokumente, Knowledge-Dokumentkommentare, Knowledge-Berichtskarten, Unterstützungssitzungen, Kontakte und Configuration Items definiert werden.

Wenn Sie eine Aktivitätsbenachrichtigung definieren, können Sie Folgendes konfigurieren:

Ereignisse

Definiert die Ereignisse-Liste für diese Aktivitätsbenachrichtigung. Ereignisse sind Prozeduren, die nach Ablauf einer bestimmten Zeitspanne durch die Issue-Verwaltung abgearbeitet werden.

Benachrichtigungsregeln

Definiert neue Benachrichtigungsregeln für Anfragen/Incidents/Probleme, Changes, Issues. Sie können auch die Standardregeln ändern, die in der Liste der Benachrichtigungsregeln angezeigt werden.

Survey

Definiert eine Umfragebenachrichtigung, die dem Empfänger der Aktivitätsbenachrichtigung ermöglicht, auf eine URL zu klicken, um eine Umfrage anzuzeigen. Mit Umfragen können Sie Kunden-Feedback erfassen und analysieren.

Hinweis: Weitere Informationen zum Erstellen von Aktivitätsbenachrichtigungen für Anfragen, Changes, Issues, verwaltete Umfragen, Knowledge-Dokumente, Knowledge-Dokumentkommentare, Knowledge-Berichtskarten, Unterstützungssitzungen, Kontakte und Configuration Items finden Sie in der *Online-Hilfe*.

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.

So erstellen Sie eine Objektkontaktbenachrichtigung:

1. Wählen Sie auf der Registerkarte "Administration" die Option "Benachrichtigungen" > "Objektkontaktbenachrichtigungen".

Die Seite "Objektkontaktbenachrichtigung - Liste" wird angezeigt.

2. Klicken Sie auf "Neu erstellen".

Das Fenster "Neue Objektkontaktbenachrichtung erstellen" wird angezeigt.

3. Füllen Sie die folgenden Felder aus:

Symbol

Definiert ein eindeutiges Kennzeichen für die Objektkontaktbenachrichtung.

Status

Gibt an, ob die Objektkontaktbenachrichtung derzeit aktiv oder inaktiv ist.

Objekttyp

Zeigt den Namen des Objekts an, für das Attribut gilt.

Objektattributname

Gibt den Namen der Objektkontaktbenachrichtung (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 Problemanfragenaktivitätsprotokoll, 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 Objektkontaktbenachrichtung.

4. Klicken Sie auf "Speichern".

Die neue Objektkontaktbenachrichtung wird in der Liste der Objektkontaktbenachrichtungen aufgeführt, sobald Sie diese Liste erneut öffnen.

Benachrichtigungsmethoden

Benachrichtigungsmethoden beschreiben, wie Benachrichtigungsmeldungen Benutzern zugestellt werden. Benachrichtigungsmethoden sind Skripts, die auf der Basis von Aktivitätsbenachrichtigungen aufgerufen werden. Die Skripts benutzen Informationen, die als Variablen geliefert werden, um Mitarbeiter oder andere Systeme von etwas zu benachrichtigen, das stattgefunden hat. Sie können beispielsweise ein Skript erstellen, mit dem eine Sprachmeldung an den einer Anfrage zugewiesenen Analysten gesendet wird, um ihn zu informieren, dass die Anfrage eskaliert wurde.

Benachrichtigungsmethoden können für jeden Kontaktdatensatz zugewiesen werden. Das System sucht die Benachrichtigungsmethode, die für bestimmte Kontakte zu verwenden ist.

Die Standardbenachrichtigungsmethoden für CA Service Desk Manager lauten wie folgt:

- E-Mail sendet Nachrichten per elektronischer Post mithilfe des Simple Mail Transport Protocol (SMTP) direkt an den Empfänger. Die Nachrichten werden auch an das Benachrichtigungsprotokoll des Empfängers gesendet.
- Die Benachrichtigungsfunktion sendet Nachrichten an das Benachrichtigungsprotokoll des Empfängers, das der Empfänger aufrufen kann, wenn CA Service Desk Manager ausgeführt wird.
- Pager-E-Mail sendet eine E-Mail an eine Adresse, die von einem Pagingssystem-Anbieter verwaltet wird. Der E-Mail-Text müsste normalerweise auf einem alphanumerischen Pager angezeigt werden können.

Sie können auch Ihre eigenen Benachrichtigungsmethoden erstellen. Sie können zum Beispiel eine Benachrichtigung für die periodische Sammlung an einen bestimmten Drucker oder über einen Pager senden. Um eine Benachrichtigungsmethode zu erstellen, müssen Sie ein Shellskript erstellen, das Benachrichtigungsvariablen enthält. Anschließend müssen Sie die neue Benachrichtigungsmethode in CA Service Desk Manager eingeben.

Hinweis: Weitere Informationen zu Benachrichtigungsmethoden finden Sie im *Implementierungshandbuch*.

Weitere Informationen:

[Einrichten von Benachrichtigungen auf der Basis von Kontakttypen](#) (siehe Seite 208)

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 Anzeigeaufforderung 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 Service Desk Manager-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.

E-Mail-Benachrichtigungen

E-Mail-Benachrichtigungen helfen Analysten bei der Kommunikation mit Mitarbeitern und Endbenutzern.

Mitarbeiter und Endbenutzer innerhalb einer Umgebung sind manchmal mobil, und interagieren mit CA Service Desk Manager per E-Mail. Sie können CA Service Desk Manager so einrichten, dass diese Art von Benutzer Folgendes machen kann:

- Aktualisieren Sie Anfragen/Incidents/Probleme/Changes/Issues über eine Antwort auf eine von CA Service Desk Manager gesendete E-Mail-Benachrichtigung.
- Genehmigen Sie oder lehnen Sie eine Workflow-Aufgabe (klassisch oder CA Workflow) per E-Mail ab.

Mit Benachrichtigungen können Sie mit Beteiligten für ein Ticket folgendermaßen kommunizieren:

- E-Mail-Benachrichtigungen können alle Empfänger der Benachrichtigung zeigen, und weisen den Benutzer darauf hin, wer die interessierten Parteien sind.
- Analysten können eine manuelle Benachrichtigung an eine temporäre E-Mail-Adresse senden, die gegenwärtig keinem Kontakt zugeordnet ist. Eine temporäre Adresse ist zum Beispiel hilfreich, wenn ein Endbenutzer nicht im Büro ist oder Schwierigkeiten haben, auf sein Standard-E-Mail-Konto zuzugreifen.
- Analysten können Anhänge mit einer Benachrichtigung senden, um einem Benutzer zusätzliche Details mitzuteilen.

Temporäre 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:

1. Ein Endbenutzer ist nicht im Büro oder hat Schwierigkeiten, auf sein Standard-E-Mail-Konto zuzugreifen.
2. Der Analyst möchte E-Mail verwenden, um Interaktionen mit dem Benutzer nachzuverfolgen.

3. Der Analyst sendet eine manuelle Benachrichtigung an eine *temporäre* E-Mail-Adresse für den Benutzer.
4. Der Analyst kann das Aktivitätsprotokoll anzeigen, das mit der manuellen Benachrichtigung aktualisiert wird.

Hinweis: Informationen zum Einrichten von temporären E-Mail-Adressen finden Sie in der *Online-Hilfe*.

Zulassen von temporären E-Mail-Adressen

Sie können Benutzer manuelle Benachrichtigungen an temporäre E-Mail-Adressen senden lassen. Zum Beispiel können Analysten E-Mails an eine Adresse senden, die keinem Kontaktdatensatz zugeordnet ist. 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.

So ermöglichen Sie die Verwendung von temporären E-Mail-Adressen:

1. Wählen Sie auf der Registerkarte "Administration" die Option "Optionsmanager" > "Benachrichtigungen".
Das Fenster "Optionen - Liste" wird angezeigt.
2. Klicken Sie auf "notification_allow_temp_address".
Die Seite "Optionen - Details" für "notification_allow_temp_address" wird mit den jeweiligen Standardwerten angezeigt.
3. Klicken Sie auf "Bearbeiten".
Die Seite "Optionen aktualisieren" für "notification_allow_temp_address" wird mit den jeweiligen Standardwerten angezeigt. Sie können die Beschreibung bearbeiten.
4. Klicken Sie auf "Installieren".
Die Seite mit den Optionsdetails zu "notification_allow_temp_address" wird angezeigt.
5. Klicken Sie auf "Fenster schließen".
6. Starten Sie den CA Service Desk Manager-Server neu.
Temporäre E-Mail-Adressen werden jetzt für manuelle Benachrichtigungen erlaubt.

Verbieten temporärer E-Mail-Adressen

Standardmäßig können Benutzer keine manuellen Aktivitätsbenachrichtigungen an temporäre E-Mail-Adressen senden. Zum Beispiel können Analysten keine E-Mails an eine Adresse senden, die keinem Kontaktdatensatz zugeordnet ist. Administratoren können die Option "notification_allow_temp_address" installieren, um temporäre E-Mail-Adressen zu erlauben. Wenn die Option installiert ist und Sie manuelle Benachrichtigungen an temporäre E-Mail-Adressen verbieten möchten, können Sie diese Option deinstallieren.

Hinweis: Temporäre E-Mail-Adressen verwenden SMTP-E-Mail-Adressen und die Benachrichtigungsmethode "Bevorzugte Methode".

So verbieten Sie die Verwendung von temporären E-Mail-Adressen:

1. Wählen Sie auf der Registerkarte "Administration" die Option "Optionsmanager" > "Benachrichtigungen".
Das Fenster "Optionen - Liste" wird angezeigt.
2. Klicken Sie auf "notification_allow_temp_address".
Die Seite mit den Optionsdetails zu "notification_allow_temp_address" wird angezeigt.
3. Klicken Sie auf "Bearbeiten".
Die Seite "Optionen aktualisieren" für "notification_allow_temp_address" wird angezeigt.
4. Klicken Sie auf "Deinstallieren".
Die Seite mit den Optionsdetails zu "notification_allow_temp_address" wird angezeigt.
5. Klicken Sie auf "Fenster schließen".
6. Starten Sie den CA Service Desk Manager-Server neu.
Die Option wird deinstalliert und temporäre E-Mail-Adressen sind nun für manuelle Aktivitätsbenachrichtigungen nicht mehr zulässig.

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 Service Desk Manager versucht nicht, E-Mail-Nachrichten erneut zu senden, wenn der ausgehende Mail-Server die Nachricht erhalten hat, diese jedoch nicht vom Benutzer 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.

So legen Sie das Wiederholungsintervall für E-Mails fest:

1. Navigieren Sie auf dem Server zu dem Verzeichnis "\$NX_ROOT".
2. Öffnen Sie die Datei "NX.env" in einen Texteditor wie WordPad.
3. 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.

4. Speichern und schließen Sie die Datei.
5. Starten Sie den CA Service Desk Manager-Service neu.
Die Änderung wird übernommen.

Benachrichtigungsregeln

Mit Benachrichtigungsregeln werden Richtlinien festgelegt, denen das System beim Senden von Benachrichtigungen folgen soll. Mit Hilfe der Benachrichtigungsregeln geben Sie an, wer unter welchen Umständen automatisch benachrichtigt werden soll.

Sie können Benachrichtigungsregeln für Anfragen, Incidents, Probleme, Changes, Issues, Kontakte, Configuration Items und globale und spezifische Mandanten definieren. Jede Benachrichtigungsregel enthält die folgenden Komponenten:

Bedingungs makro

Nehmen Sie die Konfiguration vor, um die gewünschten Werte eines oder mehrerer Felder auf einem Service Desk-Ticket darzustellen. Die Bedingung wird an unterschiedlichen Punkten während der Verarbeitung ausgewertet, um zu entscheiden, ob eine Aktion stattfindet.

Meldungsvorlage

Enthält einen Prototypen der Meldung, die erzeugt und an Kontakte geschickt wird, wenn die Benachrichtigung geschickt wird. Eine Benachrichtigungsregel muss eine Meldungsvorlage enthalten und kann wieder benutzt werden.

Objektkontakte

Zeigt den Objektkontakt an, der von den Ticketinformationen wie z. B. Zuständiger, Endbenutzer, Gruppe usw. abgeleitet wird. Wenn die Bedingung erfüllt wird, erhalten diese Objektkontakte eine Benachrichtigung.

Kontakte

Wenn die Bedingung erfüllt wird, erhalten diese Kontakte eine Benachrichtigung. Kontakte sind die Datenbankdatensätze, die die Benutzer des Systems darstellen.

Kontakttypen

Zeigt den Kontakttyp an, für den Sie die Benachrichtigung standardmäßig erhalten möchten, z. B. Analysten, Mitarbeiter, Kunde usw.

Verwandte Aktivitätsbenachrichtigungen

Zeigt eine Liste mit verwandten Aktivitätsbenachrichtigungen an, die die Benachrichtigungsregel verwenden.

Hinweis: Bei Aktivitätsbenachrichtigungen, die mehrere Regeln enthalten, deren Bedingungen erfüllt sind, können Benutzer mehrere Benachrichtigungen erhalten.

Konfigurationsoptionen für Benachrichtigungsregeln

Sie können die folgenden Optionen angeben, wenn Sie eine Benachrichtigungsregel definieren:

- **Standardbenachrichtigungsregel** - Sie können eine Standardbenachrichtigungsregel, die automatisch alle im referenzierten Feld auf dem Ticket bezeichneten Kontakte benachrichtigt, angeben. Um die Liste von Standardbenachrichtigungsregeln anzuzeigen, die Sie ändern können, wählen Sie die Registerkarte "Administration" und dann "Benachrichtigungen" und "Benachrichtigungsregeln" aus.
- **Standortdefiniertes Bedingungs makro** - Sie können ein *standortdefiniertes Bedingungs makro* implementieren, um Ihre eigene Bedingung zu erstellen, die nur bestimmte Kontakte unter gewissen Umständen benachrichtigt. Um ein Bedingungs makro von der Registerkarte "Administration" aus zu erstellen, wählen Sie "Ereignisse und Makros", "Makrotypen" und dann "Standortdefinierte Bedingung" in der Liste "Makrotyp".

- **Neue Kontakte** - Wenn Sie eine Benachrichtigungsregel definieren, können Sie auf den folgenden Registerkarten neue Kontakte festlegen, die Benachrichtigungen erhalten sollen:
 - **Objektkontakte** - Zeigt die verfügbaren Organisationen, Anbieter und Configuration Items für den markierten Objekttyp an, die eine Benachrichtigung zu Tickets erhalten sollen.
 - **Kontakte** - Zeigt die Personen an, die der Benachrichtigungsregel hinzugefügt sind, unabhängig von ihrer Zugehörigkeit zum Ticket.
 - **Kontakttypen** - Zeigt die Benutzer an, die innerhalb der Benachrichtigungsregel mit der gleichen Klassifizierung definiert sind, z. B. Analysten oder Kunden.

Mit der Schaltfläche "Aktualisieren" auf jeder Registerkarte können Sie nach neuen Kontaktdatensätzen suchen, die Sie der Regel zuordnen möchten.

Hinweis: Bevor Sie eine Benachrichtigungsregel implementieren, müssen Sie die geeigneten Kontakte für Ihre Geschäftsstruktur konfigurieren.

- **Meldungsvorlage** - Jede Benachrichtigungsregel muss eine Meldungsvorlage enthalten. Sie können Ihre eigene Meldungsvorlage definieren oder eine der verfügbaren Standardmeldungsvorlagen auf der Listenseite "Meldungsvorlage" angeben. Um diese Seite anzuzeigen, wählen Sie die Registerkarte "Administration" und dann "Benachrichtigungen" und "Meldungsvorlagen" aus.
- **Configuration-Item-Benachrichtigungen** - Wenn Sie eine Benachrichtigungsregel definieren, können Sie die Person festlegen, die für die Pflege eines Configuration Items verantwortlich ist, um Benachrichtigungen zu empfangen, wenn ein Ticket erstellt wird.
- **Benachrichtigungen des vorherigen Zuständigen** - Wenn Sie eine Aktivitätsbenachrichtigung definieren, können Sie Werte in der Benachrichtigungsregel angeben, die den bisherigen Zuständigen oder die vorherige Gruppe benachrichtigen, wenn eine Ereignisaktivität auftritt.

Weitere Informationen:

[Definieren einer Geschäftsstruktur](#) (siehe Seite 45)

[Beispiel: Erstellen von Meldungsvorlagen](#) (siehe Seite 119)

[Benachrichtigungen an vorherige Zuständige](#) (siehe Seite 127)

[Objektkontaktbenachrichtigungen](#) (siehe Seite 98)

[Überblick über standortdefinierte Bedingungs makros](#) (siehe Seite 110)

Überblick über standortdefinierte Bedingungs makros

Ein Manager möchte über alle Ticket-Aktivitäten informiert werden, die für Issues der Priorität 2 auftreten, die zu seiner Abteilung gehören. Der Administrator fügt den Manager auf ausgewählten Aktivitätsbenachrichtigungstypen, z. B. "Anfang" und "Protokollkommentar", als spezifischen Kontakt hinzu. Mit dieser Implementierung erhält der Manager alle ausgewählten Aktivitätsbenachrichtigungen für das gesamte System.

In einer Abteilung mit hohem Datenverkehr, z. B. beim technischen Support, könnte dies zu einer bedeutenden Menge an unerwünschtem E-Mail-Datenverkehr führen. Zum Steuern seines Postfachs muss der Manager Postfachregeln implementieren, um die Benachrichtigungen zu filtern, und hoffen, dass keine wichtigen Benachrichtigungen übersehen werden.

Der Administrator definiert ein standortdefiniertes Bedingungs makro, das den Manager nur benachrichtigt, wenn die Priorität auf 2 gesetzt ist und der Anfragebereich auf "Anwendungen" (Abteilung des Managers) gesetzt ist. Die neue Bedingung ist in der Benachrichtigungsregel angegeben, und der Manager wurde als Kontakt hinzugefügt. Eine Meldungsvorlage, die die Ticketaktivität beschreibt, wird definiert und die Regel der Aktivitätsbenachrichtigung hinzugefügt.

Die Aktivität tritt auf, wenn für die Priorität eines Tickets "2" und für den Anfragebereich "Anwendungen" festgelegt wurde. Wenn diese Aktivität auftritt, wird die Regel implementiert und die Bedingung bewertet. Wenn die Bedingung "True" ist, wird eine Benachrichtigungsmeldung, die die Ticketaktivität beschreibt, an den Manager gesendet. Unerwünschte Benachrichtigungen werden nicht mehr an den Manager gesendet.

Beispiel-Benachrichtigungsregel

Beispiele für Benachrichtigungsregeln bieten einleitende Informationen, die Ihnen bei folgenden Aktivitäten helfen:

- Standortdefiniertes Bedingungs makro erstellen
- Benachrichtigungsregel erstellen
- Regel zur Aktivitätsbenachrichtigung hinzufügen

Wenn die Aktivität erfolgt, wird die entsprechende Bedingung implementiert, die mit der Regel verknüpft ist. Wenn die Bedingung erfüllt ist (wird als *wahr* ausgewertet), wird eine Benachrichtigungsmeldung mit der Beschreibung der Ticket-Aktivität an alle Kontakte gesendet.

Weitere Informationen:

[Beispiel: Erstellen eines standortdefinierten Bedingungs makros](#) (siehe Seite 111)

[Beispiel: Erstellen neuer Benachrichtigungsregeln](#) (siehe Seite 112)

[Beispiel: Hinzufügen der Regel zu der Aktivitätsbenachrichtigung](#) (siehe Seite 113)

Beispiel: Erstellen eines standortdefinierten Bedingungs makros

In diesem Beispiel erstellen Sie ein standortdefiniertes Bedingungs makro, das die angegebene Bedingung überprüft.

1. Navigieren Sie auf der Registerkarte "Administration" zu "Ereignisse und Makros", "Makros".

Die Seite "Makroliste" wird angezeigt.

2. Klicken Sie auf "Neu erstellen".

Die Seite "Neues Makro erstellen" wird angezeigt.

3. Füllen Sie die folgenden Felder aus:

- Symbol: Geben Sie Folgendes ein: *Anwendung P1*.
- Makrotyp: Wählen Sie "Standortdefinierte Bedingung" aus.
- Objekttyp: Wählen Sie "Anfrage" aus.

4. Klicken Sie auf "Fortsetzen".

Die Seite "Neues Makro erstellen – AnwendungenP1" wird angezeigt.

5. Füllen Sie die folgenden Felder aus:

- Makrobeschreibung: Geben Sie Folgendes ein: *Makro=Anfrage, Priorität=1, Anfragebereich=Anwendungen*.
- Wenn alle Bedingungen erfolgreich sind, erfolgt Rückgabe-Code: WAHR auswählen.
- Datensatz-Status: "Aktiv" auswählen.

6. Klicken Sie auf "Speichern".

Die Detailseite des Makros "Anwendungen 1" wird angezeigt.

7. Klicken Sie auf "Bedingung hinzufügen".

Die Seite "Neue atomare Bedingung erstellen" wird angezeigt.

8. Erstellen Sie eine atomare Bedingung, um "Priorität=2" zu überprüfen, und füllen Sie die folgenden Felder aus:
 - Sequenz: Geben Sie Folgendes ein: *10*.
 - Beschreibung: Geben Sie Folgendes ein: *Überprüfen Sie die Priorität*.
 - Attribut auswählen: Wählen Sie "Priorität".
 - Operator auswählen: Wählen Sie "Gleich".
 - Attribut- oder Datenwert auswählen: Wählen Sie "Datenwert".
9. Wählen Sie "2" für den Datenwert aus, und klicken Sie auf "Speichern".
10. Klicken Sie auf der Makro-Detailseite auf "Bedingung hinzufügen" und füllen Sie die folgenden Felder aus:
 - Sequenz: Geben Sie Folgendes ein: *20*.
 - Beschreibung: Geben Sie Folgendes ein: *Anfragebereich überprüfen=Anwendungen*.
 - Attribut auswählen: Wählen Sie "Anfragebereich" aus.
 - Operator auswählen: Wählen Sie "Gleich".
 - Attribut- oder Datenwert auswählen: Wählen Sie "Datenwert".
11. Wählen Sie "Anwendungen" für den Datenwert aus, und klicken Sie auf "Speichern".

Die neue Bedingung wird auf der Registerkarte "Bedingungen" des standortdefinierten Bedingungs makros angezeigt.

Beispiel: Erstellen neuer Benachrichtigungsregeln

In diesem Schritt verknüpfen Sie das standortdefinierte Bedingungs makro mit der Benachrichtigungsregel, hängen eine Meldungsvorlage an und fügen den Manager als Kontaktyp hinzu.

1. Wählen Sie auf der Registerkarte "Administration" die Option "Benachrichtigungen" > "Benachrichtigungsregeln".

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: "App1 Manager benachrichtigen" eingeben.
 - Objekttyp: Anfrage auswählen.
 - Beschreibung: *"Manager über Anwendungsausfälle der Priorität 1 informieren"* eingeben.
4. Klicken Sie auf "Speichern & fortfahren".
5. Klicken Sie auf die Bedingungsverknüpfung, und wählen Sie das neue standortdefinierte Bedingungs makro mit dem Namen "Application P1" aus.
6. Klicken Sie auf "Meldungsvorlage".

Die Seite "Meldungsvorlagen - Liste" wird geöffnet.
7. Wählen Sie eine Meldungsvorlage aus der Liste aus. Stellen Sie sicher, dass die Option "Automatische Benachrichtigung" in der Vorlage aktiviert ist.
8. Klicken Sie auf der Registerkarte "Kontakttypen" auf die Schaltfläche "Kontakttyp aktualisieren".

Die Seite "Kontakttypen – Suche" wird angezeigt.
9. Klicken Sie auf "Suche".

Die Liste der Empfänger von Benachrichtigungsaktualisierungen wird angezeigt.
10. Wählen Sie "Manager" in der Liste links aus, und klicken Sie auf die Schaltfläche zur Kontaktauswahl ($\geq$).
11. Sobald der Kontakt in der rechten Liste aufgeführt wird, klicken Sie auf "OK".
12. Speichern Sie die Benachrichtigungsregel.

Die neue Benachrichtigungsregel wird in der Liste der Benachrichtigungsregeln aufgeführt, sobald Sie diese Liste erneut öffnen.

Beispiel: Hinzufügen der Regel zu der Aktivitätsbenachrichtigung

In diesem Beispiel aktivieren Sie die Option "Auto-Benachrichtigung" in der Meldungsvorlage, und fügen der Aktivitätsbenachrichtigung die Benachrichtigungsregel hinzu.

1. Wählen Sie auf der Registerkarte "Administration" die Option "Benachrichtigungen" > "Aktivitätsbenachrichtigungen" aus.

Die Seite "Aktivitätsbenachrichtigungen - Liste" wird angezeigt.
2. Wählen Sie die Aktivitätsbenachrichtigung "Anfang" in der Liste.

Die Seite "Initial Activity Notification Detail" wird angezeigt.

3. Überprüfen Sie, ob der Objekttyp auf "Anfragen" gesetzt ist, so dass das Notizbuch in den Konfigurationsinformationen für Anfragen angezeigt wird.

4. Klicken Sie auf der Registerkarte "Benachrichtigungsregeln" auf "Benachrichtigungsregeln aktualisieren".

Die Seite "Benachrichtigungsregeln – Suche" wird angezeigt.

5. Geben Sie *App P1 Manager benachrichtigen* in das Symbolfeld ein, und klicken Sie auf "Suchen".

Die aktualisierte Seite der zugewiesenen Benachrichtigungsregeln wird angezeigt.

6. Wählen Sie *Anw P1 benachrichtigt Manager* in der Liste links aus, und klicken Sie auf die Schaltfläche "Kontaktauswahl" ($\geq$).

Die Benachrichtigungsregel wird in der rechten Liste aufgeführt.

7. Klicken Sie auf "OK".

8. Klicken Sie auf die Bedingungsverknüpfung, und wählen Sie die neue Benachrichtigungsregel "App P1 Manager benachrichtigen" aus. (Sie können zusätzliche Regeln durch Klicken auf die Schaltfläche "Benachrichtigungsregeln aktualisieren" hinzufügen.)

Die Seite "Aktivitätsbenachrichtigung" wird angezeigt.

9. Stellen Sie sicher, dass die Option "Automatische Benachrichtigung" in der Meldungsvorlage aktiviert ist.

- a. Klicken Sie auf der Registerkarte "Benachrichtigungsregeln" der Aktivitätsbenachrichtigung auf die Verknüpfung der Benachrichtigungsregel.

Die Seite "Benachrichtigungsregel" wird angezeigt.

- b. Klicken Sie auf die Verknüpfung der Meldungsvorlage.

Die Seite "Meldungsvorlage - Detail" wird angezeigt.

- c. Klicken Sie auf "Bearbeiten".

Die Seite "Meldungsvorlage aktualisieren" wird angezeigt.

- d. Überprüfen Sie, ob "Automatische Benachrichtigung" aktiviert ist.

10. Klicken Sie auf "Speichern".

Wenn die Aktivität erfolgt, wird die entsprechende Bedingung implementiert, die mit der Regel verknüpft ist. Wird die Bedingung erfüllt (d. h., sie hat den Wert TRUE), wird eine Benachrichtigung mit einer Beschreibung der Ticketaktivität an alle Manager gesendet.

Beispiel-Standardbenachrichtigungsregeln

CA Service Desk Manager enthält mehrere Standardbenachrichtigungsregeln. Sie können die Standardbenachrichtigungsregeln anzeigen, indem Sie auf der Registerkarte "Administration" zu "Benachrichtigungen" und dann zu "Benachrichtigungsregeln" gehen.

Weitere Informationen:

[Beispiel: Verwenden der Regel "Anfrage mit Priorität 1"](#) (siehe Seite 115)

[Beispiel: Verwenden der Regel "Aktuellen und vorherigen Zuständigen eines Change benachrichtigen"](#) (siehe Seite 116)

[Beispiel: Verwenden der Regel "Tatsächliche Priorität - Eskalation"](#) (siehe Seite 117)

[Beispiel: Verwenden der Regel "Aktive Anfrage/Incident/Problem"](#) (siehe Seite 118)

Beispiel: Verwenden der Regel "Anfrage mit Priorität 1"

Die Benachrichtigungsregeln bieten dem Endbenutzer Flexibilität, wenn er nur über Anfragen mit Priorität 1 benachrichtigt werden möchte. Die Regel *Anfrage mit Priorität 1* wird ausgeführt, wenn es sich beim Tickettyp um eine Anfrage handelt und die Priorität auf "1" gesetzt wurde. Diese Benachrichtigung wird nur gesendet, wenn die an die Regel angehängte Bedingung "true" ist und die an die Regel angehängte Meldungsvorlage verwendet.

Hinweis: Sie können die Bedingung und die Meldungsvorlage einer Benachrichtigungsregel durch Öffnen der Regel und der Ändern des Felds "Bedingung" mit einem Makro ändern. Weitere Informationen zu Bedingungen finden Sie in der *Online-Hilfe*.

Das Produkt enthält im ITIL-Setup außerdem die Standardbenachrichtigungsregeln "Incident mit Priorität 1" und "Problem mit Priorität 1". Die Hauptunterschiede zwischen diesen Regeln und "Anfrage mit Priorität 1" sind Bedingungen für die Tickettypen. Zum Beispiel ist an "Anfrage mit Priorität 1" die Bedingung mit einer Sequenz von "20" angehängt, die die Benachrichtigungsregel auf Anfragen beschränkt

Standardmäßig sind der Regel keine Objektkontakte, Kontakte oder Kontakttypen angehängt. Für das Feld "Auto-Benachrichtigung" in der an die Regel angehängten Meldungsvorlage ist standardmäßig ebenfalls "Nein" festgelegt. Um eine Benachrichtigung zu senden, müssen Sie der Regel einen Objektkontakt oder Kontakt bzw. einen Kontakttyp hinzufügen. Außerdem müssen Sie in der Meldungsvorlage die Einstellung des Feldes "Automatische Benachrichtigung" zu "Ja" ändern.

Beispiel: Konfigurieren von Regeln, um nur für Anfragen mit Priorität 1 eine Benachrichtigung zu senden

Die Regel sollte sowohl mit der Aktivitätsbenachrichtigung "Erstellung" als auch "Eskalieren" verbunden sein. Dadurch stellen Sie sicher, dass der Empfänger die Benachrichtigung für eine neue Anfrage mit Priorität 1 erhält und dass die Anfragepriorität auf 1 erhöht wird.

1. Überprüfen Sie, ob entweder die an die Aktivitätsbenachrichtigung "Erstellung" und "Eskalieren" angehängte Standardregel entfernt oder für die Option "Auto-Benachrichtigung" "Nein" festgelegt wurde.

Auf diese Weise werden für diese Standardregeln keine Benachrichtigungen gesendet.

2. Öffnen Sie die Regel "Anfrage mit Priorität 1".
3. Fügen Sie der Regel einen Objektkontakt, einen Kontakt oder einen Kontakttyp hinzu.
4. Klicken Sie auf "Meldungsvorlage", und wählen Sie die Option "Auto-Benachrichtigung" aus.
5. Hängen Sie die Regel "Anfrage mit Priorität 1" an die Aktivitätsbenachrichtigungen "Erstellung" und "Eskalieren" an.
6. Tun Sie Folgendes:
 - Erstellen Sie eine neue Anfrage, und setzen Sie die Priorität auf 1. Überprüfen Sie, ob der Benutzer die Benachrichtigung erhält.
 - Erstellen Sie eine neue Anfrage, und legen Sie eine andere Priorität fest, z. B. "2". Stellen Sie sicher, dass der Benutzer die Benachrichtigung nicht erhält.

Beispiel: Verwenden der Regel "Aktuellen und vorherigen Zuständigen eines Change benachrichtigen"

Die Regel *Aktuellen und vorherigen Zuständigen eines Change benachrichtigen* benachrichtigt sowohl den aktuellen als auch den vorigen Zuständigen über den Change während der Übertragung. Sie können eine ähnliche Regel für andere Ticket-Typen erstellen.

Beispiel: Benachrichtigen des aktuellen und den vorigen Zuständigen über die Übertragung eines Changes

1. Überprüfen Sie ob, entweder die an die Aktivitätsbenachrichtigung "Erstellung" angehängte Standardregel entfernt wird oder für die Option "Auto-Benachrichtigung" in der an die Meldungsvorlage angehängten Standardregel "Nein" festgelegt wurde.

Auf diese Weise werden für diese Standardregeln keine Benachrichtigungen gesendet.

2. Beispiel: Öffnen sie die Regel "Aktuellen und vorherigen Zuständigen eines Change benachrichtigen".
3. Klicken Sie auf die Meldungsvorlage "Aktuellen und vorherigen Zuständigen eines Change benachrichtigen" und wählen Sie die Option "Automatische Benachrichtigung" aus.
4. Hängen Sie die Regel "Aktuellen und vorherigen Zuständigen eines Change benachrichtigen" an die Benachrichtigung über die Übertragung.
5. Tun Sie Folgendes:
 - a. Erstellen und speichern Sie einen Change mit einem Zuständigen.
 - b. Wechseln Sie zu einem anderen Zuständigen.

Überprüfen Sie, dass beide Benutzer die Übertragungsbenachrichtigung bekommen.

Beispiel: Verwenden der Regel "Tatsächliche Priorität - Eskalation"

Die Aktivitätsbenachrichtigung "Eskalieren" tritt nicht nur auf, wenn sich die Priorität erhöht, sondern auch wenn sich die Priorität eines Tickets ändert. Benutzer werden über Eskalationen und Deeskalationen benachrichtigt. Die Benachrichtigungsregeln bieten jetzt eine Möglichkeit, zwischen einer Änderung von Priorität 2 in Priorität 1 und einer Änderung von Priorität 1 in Priorität 2 zu unterscheiden.

Die Regel *Tatsächliche Priorität - Eskalation* bewertet den aktuellen und den vorherigen Wert des Felds "Priorität". Diese Regel benachrichtigt den angehängten Objektkontakt, den Kontakt und die Kontakttypen, die der Regel nur angehängt werden, wenn sich die Priorität eines Issue-Tickets von einer niedrigeren Priorität in eine höhere Priorität ändert.

Hinweis: Sie können eine ähnliche Regel für andere Tickettypen erstellen. Diese Benachrichtigung wird nur gesendet, wenn die der Regel angehängte Bedingung als "Wahr" bewertet wird, und verwendet die der Regel angehängte Meldungsvorlage. Standardmäßig sind der Regel kein Objektkontakt, kein Kontakt oder keine Kontakttypen angehängt. Das Feld "Auto-Benachrichtigung" in der an die Regel angehängten Meldungsvorlage ist standardmäßig ebenfalls auf "Nein" eingestellt.

Beispiel: Erhalten von Benachrichtigungen, wenn sich die Priorität für den Tickettyp "Issue" von einer niedrigeren in eine höhere Priorität ändert

1. Überprüfen Sie ob, entweder die an die Aktivitätsbenachrichtigung "Eskalieren" angehängte Standardregel entfernt wird oder für die Option "Auto-Benachrichtigung" in der an die Meldungsvorlage angehängten Standardregel "Nein" festgelegt wurde.

Damit wird das Senden von Benachrichtigungen für diese Standardregeln verhindert.

2. Öffnen Sie die Regel "Tatsächliche Priorität - Eskalation".

Fügen Sie der Regel einen Objektkontakt, einen Kontakt oder einen Kontakttyp hinzu.

Überprüfen Sie, ob der Kontakt Benachrichtigungen erhalten kann.

3. Klicken Sie im Feld "Meldungsvorlage" auf "Tatsächliche Priorität - Eskalation", und aktivieren Sie das Kontrollkästchen "Auto-Benachrichtigung".

Hängen Sie die Regel an die Aktivitätsbenachrichtigung "Eskalieren" an.

4. Erstellen Sie einen neuen Issue mit einer Priorität, z. B. "5".

5. Ändern Sie die Priorität in "4", und überprüfen Sie, ob der Benutzer die Benachrichtigung erhalten hat.

6. Ändern Sie die Priorität von "4" in "5", und stellen Sie sicher, dass der Benutzer die Benachrichtigung nicht erhalten hat.

Beispiel: Verwenden der Regel "Aktive Anfrage/Incident/Problem"

Die Regel *Aktive Anfrage/Incident/Problem* ist an eine Bedingung angehängt, nach der die erste Benachrichtigung nur dann gesendet wird, wenn die Anfrage/Incident/Problem aktiv ist.

Dadurch erhält der Kunde nur dann die Schließungsbenachrichtigung, wenn eine inaktive Anfrage erstellt wird. Diese Regel benachrichtigt den angehängten Objektkontakt/Kontakt und die angehängten Kontakttypen, die der Regel angehängt werden, nur, wenn eine/ein aktive Anfrage/Incident/Problem erstellt wird.

Hinweis: Sie können eine ähnliche Regel für Changes und Issue-Ticket-Typen erstellen.

Die Benachrichtigung wird nur gesendet, wenn die an die Regel angehängte Bedingung als "Wahr" bewertet wird, und verwendet die an die Regel angehängte Meldungsvorlage. Die Regel ist standardmäßig nicht mit Objektkontakten, Kontakten oder Kontakttypen verknüpft. Auch das Feld "Automatische Benachrichtigung" in der Meldungsvorlage, die an die Regel angehängt ist, wird standardmäßig auf "Nein" gesetzt.

Beispiel: Empfangen einer Benachrichtigung nach Schließen eines Incidents

1. Überprüfen Sie, ob entweder die an die Aktivitätsregel "Erstellung" angehängte Standardregel entfernt wird oder für die Option "Auto-Benachrichtigung" in der Meldungsvorlage, die an die (wiederum an die Aktivitätsbenachrichtigung "Eskalieren" angehängte) Standardregel angehängt ist, "Nein" eingestellt wurde

Auf diese Weise werden für diese Standardregeln keine Benachrichtigungen gesendet.
2. Öffnen Sie die Regel "Aktive Anfrage/Incident/Problem".

Fügen Sie der Regel einen Objektkontakt, Kontakt oder Kontakttyp hinzu.

Überprüfen Sie, dass der Kontakt Benachrichtigungen empfangen kann.
3. Klicken Sie auf die Meldungsvorlage "Aktive Anfrage/Incident/Problem", die an die Regel angehängt ist, und aktivieren Sie das Kontrollkästchen "Automatische Benachrichtigung".
4. Hängen Sie die Regel "Aktive Anfrage/Incident/Problem" an die Benachrichtigungsaktivität "Erstellung" an.
5. Erstellen Sie einen neuen Incident und setzen Sie das Statusfeld auf "Geschlossen".
6. Stellen Sie sicher, dass der zugewiesene Benutzer, der die Benachrichtigung erhalten soll, die Benachrichtigung "Erstellung" nicht erhält.

Beispiel: Erstellen von Meldungsvorlagen

Jede Benachrichtigungsregel muss eine Meldungsvorlage enthalten. Sie können Vorlagen erstellen, die Standardwerte für Benachrichtigungsmeldungen enthalten.

Beispiel: Erstellen von Meldungsvorlagen

Dieses Beispiel veranschaulicht die Erstellung einer Meldungsvorlage.

So erstellen Sie eine Meldungsvorlage:

1. Wählen Sie auf der Registerkarte "Administration" die Option "Benachrichtigungen" > "Meldungsvorlagen".

Das Fenster "Meldungsvorlagen - Liste" wird angezeigt.
2. Klicken Sie auf "Neu erstellen".

Das Fenster "Neue Meldungsvorlage erstellen" wird angezeigt.

3. Füllen Sie die folgenden Felder aus:

Mandant

Gibt den Mandanten an, der mit dieser Vorlage verknüpft ist.

Hinweis: Wenn Sie "Global" (gemeinsame Nutzung) auswählen, können Sie die Vorlage für gemeinsame Nachrichten verwenden.

Symbol

Definiert ein eindeutiges Kennzeichen für diesen Datensatz.

Objekttyp

Gibt den Objekttyp an, der mit dieser Vorlage verknüpft ist.

Datensatzstatus

Markieren Sie die Option "Aktiv" oder "Inaktiv" für den Status dieser Vorlage.

Auto-Benachrichtigung

Die mit dieser Vorlage verknüpfte Benachrichtigung wird automatisch gesendet, sobald die Aktivität auftritt.

Benachrichtigungsebene

Zeigt die relative Gewichtung dieser Benachrichtigung an. Wählen Sie "Notfall", "Hoch", "Niedrig" oder "Normal".

Titel der Benachrichtigungsmeldung

Gibt den Zusammenfassungstitel der Meldung an. Beim Senden einer Benachrichtigung können Sie Werte aus dem Ticket mithilfe von Variablen einfügen. Verwenden Sie beispielsweise eine Variable, mit der die Issue-Nummer in den Titel der Meldung eingefügt wird.

Benachrichtigungstext

Gibt den Inhalt der Meldung an. Beim Senden einer Benachrichtigung können Sie Werte aus dem Ticket mithilfe von Variablen einfügen. Verwenden Sie beispielsweise eine Variable, mit der der Namen des Analysten, der Name des Endbenutzers und die Beschreibung in die Meldung eingefügt werden.

HTML-Meldung

Gibt eine Meldung in HTML an, die angezeigt wird, wenn das E-Mail-Programm des Empfängers HTML-Meldungen unterstützt. Wenn der Empfänger die Meldung auf einem Mobilgerät erhält (z. B. Handy oder BlackBerry), wird sie im Nur-Text-Format angezeigt.

HTML-Meldung bearbeiten

Öffnet den HTML-Editor, in dem Sie Ihre HTML-Meldung bearbeiten können.

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 neue Meldungsvorlage wird in der Liste der Meldungsvorlagen aufgeführt.

Artefakte in Meldungen

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:

- **KEINE** – Gibt an, dass Artefakte nicht validiert werden. Dieser Wert ist der gleiche, als ob Sie kein Schlüsselwort benutzen.
- **GESCHÜTZT** – 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.

BenachrichtigungsCodes 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 Service Desk Manager 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 Service Desk Manager folgende Zeichenfolgen bereit:

Symbol	Code	Wortfolge
Benachrichtigungsverlauf - Change	notify_history_chg	Klicken Sie auf die folgende URL, um die Benachrichtigungsliste anzuzeigen: @{change_id.web_url}+HTMPL=chg_lr.html I+INSTANCE=@{id}
Benachrichtigungsverlauf - Issue	notify_history_iss	Klicken Sie auf die folgende URL, um die Benachrichtigungsliste anzuzeigen: @{issue_id.web_url}+HTMPL=iss_lr.html+I NSTANCE=@{id}
Benachrichtigungsverlauf - Anfrage/Incident/Problem	notify_history_cr	Klicken Sie auf die folgende URL, um die Benachrichtigungsliste anzuzeigen: @{call_req_id.web_url}+HTMPL=cr_lr.html

Symbol	Code	Wortfolge
		+INSTANCE=@{id}

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 Service Desk Manager 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 364) "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.

Benachrichtigungszeichenfolgen in einer Nachricht – Beispiel

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

Code	Wortfolge
	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=400723>

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.

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	Anfragen, Incidents, Probleme	Änderungsaufträge	Problemanfragen
Status	Ja	Ja	Ja
Aktiv	Ja	Ja	Ja
Verantwortlicher	Ja	Ja	Ja
Anfragebereich/Kategorie	Ja	Ja	Ja
Gruppe	Ja	Ja	Ja
Impact	Ja	Ja	Ja
Priorität	Ja	Ja	Ja
Urgency	Ja	Nein	Nein
Relevanz	Ja	Nein	Nein

Es gibt mehrere Kontakte, die Sie für jeden Objekttyp angeben können (Anfrage, 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

Nachdem die Benachrichtigungsregel gespeichert worden ist, werden die Felder "Vorheriger Zuständiger" und "Gruppe" auf der Seite mit der Liste der Objektkontaktbenachrichtigungen angezeigt.

Beispiel: Konfiguration von aktuellen und vorherigen Werten für Schlüsselfelder

Das folgende Beispiel zur Verwendung beschreibt, wie ein Administrator aktuelle und vorherige Werte für Schlüsselfelder konfiguriert, um sicherzustellen, dass der vorherige Support-Mitarbeiter benachrichtigt wird, wenn eine Anfrage von ihnen weg übermittelt 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 Anfrageformular den aktuellen und den vorherigen Zuständigen an, die benachrichtigt werden sollen.
3. **Aktion** - Wenn die Anfrage abgespeichert wird, werden die Felder "Zuständiger" und "Vorheriger Zuständiger" der Anfrage 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 Service Desk Manager-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 "Objektyp" 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 ($\geq$).
- 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 Service Desk Manager-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 Service Desk Manager-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 ($\geq$).

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.

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 ($\geq$).

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.

Umfragebenachrichtigungen

Für eine Aktivitätsbenachrichtigung können Sie getrennte Umfragebenachrichtigungsdetails für Tickets, verwaltete Umfragen, Knowledge-Dokumente und Knowledge-Kommentare definieren und sie dem Kunden schicken, der die Aktivität anstieß.

Mit Umfragebenachrichtigungen können Sie Folgendes tun:

- Neue Umfragen angeben oder eine der mit dem Produkt verfügbaren Standardumfragen verwenden
- Benachrichtigungsmethoden verwenden, die beschreiben, wie Benachrichtigungsmeldungen an Benutzer übermittelt werden
- Umfragemeldungen für den Kunden definieren

Wenn ein Benutzer die 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.

Ein Aktivitätsprotokoll wird generiert, zum einen, wenn eine Umfragebenachrichtigung gesendet wird, und zum anderen, wenn eine Umfrage von einem Kunden empfangen wird.

Weitere Informationen:

[Definieren von Umfragebenachrichtigungen](#) (siehe Seite 201)

Hinzufügen von URL-Hyperlinks an Benachrichtigungen

Das Feld "web_url" in den Tabellen "Change_Request" und "Workflow_Task" enthält einen URL-Wert, der einem Benutzer 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 Benutzer einfach auf die URL klicken und ohne weitere Abfragen direkt zur Web-Schnittstelle gehen.

Bevor Sie URL-Hyperlinks in Benachrichtigungen implementieren können, müssen Sie Ihr System folgendermaßen konfigurieren:

1. Installieren Sie und konfigurieren Sie die CA Service Desk Manager Web-Schnittstelle.

Hinweis: Weitere Informationen finden Sie im *Implementierungshandbuch*.

2. Über den Optionsmanager können Sie die Option "web_cgi_url" konfigurieren und installieren, um den Speicherort der CA Service Desk Manager-Web-Engine anzugeben, z. B. `http://hostname/scripts/pdmcgi.exe`.

Weitere Informationen:

[Verwendung des Optionsmanagers](#) (siehe Seite 363)

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 Service Desk Manager 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 Benachrichtigungsprotokolle 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 Service Desk Manager-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}
Änderungsauftrag	@{change_id.attr}
Issue	@{issue_id.attr}

Die Werte werden eingesetzt, wenn die Antwort aus dem Feld "Benutzerbeschreibung" 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.

E-Mail-Administration

Mit Hilfe von E-Mail können Sie mit Endbenutzern, wie Mitarbeitern oder Kunden, kommunizieren. Endbenutzer können auf E-Mail-Benachrichtigungen antworten, um Tickets zu aktualisieren oder zu erstellen. Dabei können sie E-Mail von einem Computer aus oder mit einem anderen Gerät, wie etwa einem Mobiltelefon, benutzen. Wenn beispielsweise von einem Endbenutzer per E-Mail zusätzliche Informationen angefordert werden, dann können Sie mit den erhaltenen angeforderten Informationen ein Ticket aktualisieren.

Die folgenden Funktionen führen die E-Mail-Kommunikation mit dem Endbenutzer durch:

■ **E-Mail-Benachrichtigungen** – Verarbeitet ausgehende E-Mails.

Informationen über ausgehende E-Mails:

- Die Programmroutine Mail Daemon (pdm_mail_nxd) sendet unter Verwendung des Protokolls SMTP ausgehende E-Mail-Benachrichtigungen.
- Sie konfigurieren die Optionen des SMTP-Servers mit Hilfe von "Optionsmanager – E-Mail".
- Sie können Standardmethoden zur E-Mail-Benachrichtigung verwenden (oder neue Methoden konfigurieren), um E-Mails direkt über SMTP an den Empfänger zu senden.

■ **Briefkästen**– Verarbeitet eingehende E-Mails.

Informationen über eingehende E-Mails:

- Die Programmroutine Mail Eater (pdm_maileater_nxd) ruft eingehende E-Mails ab, um Tickets zu erstellen und zu aktualisieren. Dabei werden die Protokolle POP3 oder IMAP bzw. IMAP4 verwendet.
- CA Service Desk Manager-Postfächer definieren E-Mail-Konten (Posteingänge).
- Die Postfachregeln definieren, wie die einzelnen Postfächer die eingehenden E-Mails verarbeiten.

Weitere Informationen:

[E-Mail-Benachrichtigungen](#) (siehe Seite 103)

Postfächer

CA Service Desk Manager stellt ein Standard-Postfach zur Verfügung, das sich mit dem Mail-Server verbindet und eine zusätzliche Konfiguration wie beispielsweise das Festlegen von Werten für Hostname, Benutzername, Kennwort usw. benötigt.

Einige Methoden zur Definition eines Postfachs zur Verarbeitung eingehender Mails sind im Folgenden aufgeführt:

- Konfigurieren des Postfachs zur Verwendung des POP3- oder IMAP-Protokolls
- Erstellen mehrerer Postfächer, damit einzelne Mandanten oder Organisationen unterschiedliche Postfächer mit jeweils unterschiedlichen Verhaltensweisen haben
- Verwenden von Postfachregeln zum Filter von Meldungen und Festlegen eines bestimmten Verhaltens, zur Definition von automatischen Antworten und Festlegen bestimmter Aktionen (zum Beispiel zur Aktualisierung von Tickets) auf der Basis des Inhalts oder der Eigenschaften der Meldung
- Verwenden von Postfachregeln zur Bereitstellung von Text-API-Standardwerten und Erstellung von E-Mail-Schnittstellen zu anderer Software. Sie können Parameter (wie beispielsweise Kategorie, Zuständiger usw.) speziell für die Schnittstelle konfigurieren.
- Verwenden von Benachrichtigungszeichenfolgen in Postfachregeln, um allgemeine Elemente für automatische Antworten über mehrere Regeln hinweg zu erstellen
- Verwenden von Postfachrichtlinien zum Schutz vor mailbasiertem Missbrauch

Weitere Informationen:

[Postfachabfrage](#) (siehe Seite 105)

Postfachregeln

Mit Postfachregeln können Sie Aktionen, Antworten oder beides konfigurieren, die für Meldungen auftreten müssen, welche aus einem Postfach abgerufen wurden. Die Tabelle (usp_mailbox_rule) pflegt die Regeln, die für die Verbindung mit jedem Mail-Server-Konto (usp_mailbox) gelten - Regeln gehören zu bestimmten Postfächern. Sie können Regeln löschen oder inaktiv machen, um sie zu deaktivieren.

Hinweis: Wenn Sie Postfachregeln erstellen, verknüpfen Sie sie mit einem bestimmten Postfach, andere Postfächer können diese Regeln nicht verwenden. Wenn Sie Regeln, die zu einem bestimmten Postfach gehören, für ein anderes Postfach verwenden wollen, dann erstellen Sie sie für dieses andere Postfach neu.

Mit Postfachregeln können Sie Folgendes tun:

- Angeben verschiedener Verhaltensweisen für Meldungen aus jedem Postfach auf Basis des Inhalts der Meldungen.
- Bereitstellen von Text-API-Standardparametern (wie Kategorie, Zuständiger usw.) für die Meldungsverarbeitung und das Meldungs-Routing.
- Setzen von Meldungsfiltren auf Basis von festen Schlüsselwörtern oder regulären Ausdrücken.
- Verwenden einer allgemeinen Benachrichtigungszeichenfolge für die automatischen Antworten für zahlreiche Postfachregeldefinitionen wie im folgenden Beispiel:

Vielen Dank für Ihre Anfrage.

@{notification_phrase[RequestReply].phrase}

Die Wortfolge ist in Antworten auf E-Mails enthalten, die an beliebige Postfächer übermittelt werden, die die Regel beinhalten.

Weitere Informationen:

[Aktionen für Postfachregeln](#) (siehe Seite 141)

[Musterabgleich in Postfachregeln](#) (siehe Seite 141)

[Objektkennungsbeschränkungen in Filterzeichenfolgen](#) (siehe Seite 143)

[Sonderzeichen in regulären Ausdrücken](#) (siehe Seite 145)

[Beispieltext für Benachrichtigungszeichenfolgen in einer Postfachregel](#) (siehe Seite 146)

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 Antworterfolgsnachrichten 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 Service Desk Manager 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 sowohl \r als auch \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.

Die obigen Zeichen müssen vermieden werden, weil sie innerhalb eines Ticket-ID-Artefaktwerts vorkommen können. 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 \n 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 "Erfolg der Antwort" der Seite "Postfachregel aktualisieren":

- Erfolgstext

Vielen Dank für Ihre Anfrage.
@{notification_phrase[IncidentURL1].phrase}
@{notification_phrase[RequestReply].phrase}

- Erfolg (HTML)

Vielen Dank für Ihre Anfrage.</p>
k@{notification_phrase[IncidentURL1H].phrase}</p>
k@{notification_phrase[RequestReplyHTML].phrase}</p>

Hinweis: Informationen zum Konfigurieren von Benachrichtigungszeichenfolgen finden Sie in der *Online-Hilfe*.

Weitere Informationen:

[Syntax von Benachrichtigungszeichenfolgen](#) (siehe Seite 124)
[Benachrichtigungscodes und -zeichenfolgen](#) (siehe Seite 122)

Postfachrichtlinien

Postfachrichtlinien schützen Ihre Organisation vor gewissen Arten des E-Mail-Missbrauchs. Sie können folgendermaßen Richtlinien implementieren:

- Sie können Einschluss- und Ausschlusslisten für E-Mail-Adressen definieren:
 - Einschlusslisten begrenzen den Empfang von E-Mails auf Mails, die von bestimmten E-Mail-Adressen (z. B. benutzer@unternehmen.com) oder E-Mail-Domänen (z. B. unternehmen.com) stammen.
 - Ausschlusslisten filtern unerwünschte E-Mail-Adressen oder E-Mail-Domänen heraus.

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.
- Sie können das Limit bezüglich der maximalen Anzahl der Meldungen pro Stunde und Adresse für die DoS-Erfassung festlegen.

Die maximale Anzahl der Meldungen beschränkt die Anzahl an E-Mails pro Stunde, 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.

Postfachrichtlinien für Einschluss- und Ausschlusslisten und die maximale Anzahl der pro Stunde erlaubten E-Mails gehören nur zum einzigen zugeordneten 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.

E-Mail-Adressen, die die Richtlinie verletzen, werden in STDLOG gemäß den Einstellungen in "log_policy_violation" protokolliert (dadurch werden entweder keine oder die erste oder aber alle Adressen protokolliert).

Implementieren von Postfächern

CA Service Desk Manager 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.

Um Postfächer zu implementieren, führen Sie zunächst folgende Schritte aus:

- Konfigurieren Sie das Mail-Server-Konto, das Sie verwenden möchten.
- Erstellen Sie Kontakte, und geben Sie deren E-Mail-Adressen an, wenn Sie anonymen Benutzern nicht erlauben wollen, Tickets zu erstellen und zu aktualisieren (Option "Anonym zulassen").

Um das Standardpostfach zu konfigurieren, führen Sie die folgenden optionalen grundlegenden Schritte aus:

1. Bearbeiten Sie das Standardpostfach.
2. Aktualisieren Sie die Postfachregeln und Richtlinien.

Das Postfach ist aktiv und beginnt mit der Abfrage. Die erste Abfrage findet nach einer Sekunde statt.

Konfigurieren des Mail-Servers

Benachrichtigungen zu einem Ereignis (sowohl automatische wie manuelle) werden unter Verwendung eines zentral festgelegten Mail-Servers versendet.

So konfigurieren Sie den Mail-Server:

1. Wählen Sie auf der Registerkarte "Administration" die Option "Optionsmanager" > "E-Mail".

Die Liste der Optionen wird angezeigt.

2. Klicken Sie auf die Option, die Sie installieren möchten.

Die Seite "Optionen - Details" wird angezeigt.

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 Optionslistenoptionen zu konfigurieren.

Hinweis: Mit den Parametern "-F" und "-T" des Befehls "pdm_mail" können Sie die Absenderadresse bzw. die Antwortadresse festlegen. Sie können diese Parameter in angepassten Benachrichtigungsmethoden verwenden, um Antworten am per E-Mail übermittelte Benachrichtigungen an die richtige Mailbox ausliefern zu lassen.

Weitere Informationen:

[Dienstprogramm "pdm_mail" - Senden von E-Mail-Informationen](#) (siehe Seite 101)

E-Mail-Optionen

Die E-Mail-Schnittstelle sendet E-Mail-Benachrichtigungen und ermöglicht Benutzern die Erstellung von Tickets per E-Mail. Über die E-Mail-Optionen können Sie Protokolle für den Postausgang konfigurieren.

mail_from_address

Gibt bei der Postbenachrichtigung das Feld "Von:" an. Die Adresse hat das Format Displayname<benutzer@unternehmen.com>.

mail_login_password

Gibt das Login-Kennwort für den SMTP-Server an.

mail_login_userid

Gibt die Benutzer-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 Benutzerkonto 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 Domännennamen, der von SMTP-Servern benötigt wird, die mit ESMTP-Protokollen arbeiten. Sie können den Domännennamen löschen, indem Sie den Wert auf NONE setzen.

mail_smtp_hosts

Gibt eine Leerstellen-getrennte Liste von SMTP-Hostnamen 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.

Bearbeiten des Standardpostfachs

CA Service Desk Manager stellt ein aktives Standardpostfach bereit, das Sie bearbeiten können, um es an die Mail-Übermittlungsanforderungen in Ihrer Organisation anzupassen.

So bearbeiten Sie das Standardpostfach:

1. Navigieren Sie auf der Registerkarte "Administration" zu "E-Mail" > "Postfächer".

Die Postfachliste wird mit den aktiven Postfächern angezeigt.

2. Klicken Sie auf "Standard" in der Spalte "Name".

Die Seite "Standardpostfach - Detailseite" wird angezeigt.

3. Klicken Sie auf "Bearbeiten".

4. Füllen Sie die anderen Felder nach Bedarf aus bzw. aktualisieren Sie sie:

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.

Filtern

Gibt an, welcher Teil der E-Mail nach dem Filtermuster durchsucht werden soll, z. B. nach Einschränkungen in der Betreffzeile.

Filterzeichenfolge

Gibt eine Zeichenfolge für reguläre Ausdrücke an, damit z. B. [\t\r\n]Anfrage[\t\r\n] gefunden wird. Mit dem Platzhalter {{object_id}} können Sie den Artefaktwert für die Text-API angeben, um somit die Meldung mit einem bestimmten Ticket zu verbinden.

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, "Anfrage".

Minimaler Artefakttyp

Gibt den gewünschten Mindestwert für das Überprüfen von Artefakten an:

- **NONE:** 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.
- **PROTECTED:** 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.
- **SECURE:** 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 PROTECTED setzen, dann sind sowohl PROTECTED und SECURE erlaubt, jedoch nicht NONE. Hinzu kommt, dass wenn PROTECTED oder SECURE ausgewählt sind, keine Befehle für Text-API-Ticket-IDs erlaubt sind.

Antwort

Gibt eine Benachrichtigungsmethode an, um eine automatische Antwort, z. B. eine E-Mail zu schicken. 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.

ReplySubject

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.

Präfix eines Protokolleintrags

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.

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.

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 Ihrer Anfrage. Ein Support-Techniker wird sich innerhalb der nächsten 24 Stunden mit Ihnen in Verbindung setzen.

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:

- **Edit Success HTML (Bearbeiten der Erfolgs-HTML-Datei):** Öffnet den HTML-Editor, mit dem Sie die HTML-Datei bearbeiten können.
- **Quick View:** Zeigt den HTML-Text in der Vorschau an.
- **HTML-Quelle:** Zeigt die HTML-Quelle an.

Fehlertext

Gibt die Nur-Text-Inhalte einer Antwortmeldung an, wenn die Verarbeitung der Meldung fehlschlägt.

Fehler (HTML)

Gibt HTML-Inhalte einer Antwortmeldung an, wenn die Verarbeitung der Meldung fehlschlägt. Mit den folgenden Optionen können Sie HTML-Text in der Vorschau anzeigen und bearbeiten:

- **Edit Failure HTML** (Bearbeiten der Fehler-HTML-Datei): Öffnet den HTML-Editor, mit dem Sie die HTML-Datei bearbeiten können.
- **Quick View**: Zeigt den HTML-Text in der Vorschau an.

HTML-Quellcode: Zeigt den HTML-Quellcode an.

5. (Optional) Erstellen oder aktualisieren Sie die Postfachregeln und Richtlinien nach Bedarf.

Hinweis: Wenn Sie Postfachregeln erstellen, verknüpfen Sie sie mit einem bestimmten Postfach, andere Postfächer können diese Regeln nicht verwenden. Wenn Sie Regeln, die zu einem bestimmten Postfach gehören, für ein anderes Postfach verwenden wollen, dann erstellen Sie sie für dieses andere Postfach neu.

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.

6. Klicken Sie auf "Speichern".

Die Änderungen am Standardpostfach werden gespeichert und angewendet. Die erste Abfrage findet nach einer Sekunde statt.

Mehrere Postfächer

CA Service Desk Manager 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.

Konfigurieren von E-Mail-Antworten

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 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.

Sie verwenden CA Service Desk Manager Administration, um E-Mail wie folgt zu konfigurieren:

1. Erstellen Sie ein Postfach für eingehende E-Mail auf einem Server.
2. Gehen Sie zu "Optionsmanager", "E-Mail", und konfigurieren Sie den Server für ausgehende Post.
3. (Optional) Geben Sie eine Benachrichtigungs-E-Mail-Adresse in der Kontaktdefinition an.

4. Gehen Sie zu "Benachrichtigungen, Benachrichtigungsmethoden, E-Mail", und erstellen oder aktualisieren Sie eine Benachrichtigungsmethode mit den folgenden Einstellungen:

- Unterstützt SMTP – aktiviert
- pdm_mail [-F *E-Mail-Adresse "Von"*] [-T *Antwort-E-Mail-Adresse*]

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.

- Schlüsselwort "\${REPLY_FROM}"

Wenn das Schlüsselwort "\${REPLY_FROM}" als Adresse angegeben wird, setzt sich diese Adresse aus dem Benutzernamen 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: Benutzername=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 Domänenenerweiterung 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 Benutzer sie liest. Wenn die Adressen identisch sind, können Sie nur die "Von"-Adresse angeben.

5. Gehen Sie zu "E-Mail, Postfachregeln", öffnen Sie jede anwendbare Postfachregel, und wählen Sie die neue Antwortmethode in der Dropdown-Liste "Antwort" aus. Speichern Sie alle aktualisierten Regeln.

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 101)

Identifizieren alternativer Absenderadressen

Sie können den Parameter "-n" im Betreff der Meldung verwenden, so dass CA Service Desk Manager 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 Service Desk Manager 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.

Artefakte

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 enthalten sein, das für diesen Tickettyp konfiguriert wurde.

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.

Verwendung: `%REQUEST=@{call_req_id.ref_num}%`

Beispiel: `%REQUEST=1234%`

Hinweise zur Verwendung von Artefakten

Wenn Sie die Filterzeichenfolge der Postfachregel erstellen, beachten Sie Folgendes:

- 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.

Schutz und Sicherheit von Artefakten

Sie benutzen Artefakte, um die Mail-Übermittlung an ein Postfach auf folgende Art und Weise zu schützen:

- Verwenden Sie das Schlüsselwort ARTIFACT in Benachrichtigungen und Benachrichtigungszeichenfolgen.

Hinweis: Die Artefaktsicherheitsstufe muss mit der Einstellung "Minimaler Artefakttyp" der Postfachregel für das Postfach übereinstimmen, an das die E-Mail gesendet wird. Typen, die sicherer als die Festlegung sind, sind erlaubt. Mit anderen Worten: Wenn Sie ARTIFACT=PROTECTED setzen, sind sowohl PROTECTED als auch SECURE erlaubt, aber NONE ist nicht erlaubt.

- Setzen Sie die Option "Minimaler Artefakttyp" im Postfachregeldetail.

Sie können ein Artefakt in eine Benachrichtigungszeichenfolge einbetten und die Sicherheitsstufe für das Artefakt angeben. Beispiel:

`%REQUEST=@{ARTIFACT=PROTECTED:call_req_id.ref_num}%`

Hinweis: Weitere Informationen zu den Tabellen für die Option "Minimaler Artefakttyp" (`filter_min_artifact_type`) und das Postfachregeledetail (`usp_mailbox_rule`-Tabelle) finden Sie im *Technischen Referenzhandbuch*.

Beispiel: Keine Validierung von Artefakten

Das folgende Beispiel zeigt kein ARTIFACT-Format. Es kann keine Validierung von Artefakten durchgeführt werden.

Nutzung: `%REQUEST=@{call_req_id.ref_num}%`

Beispiel: `%REQUEST=1234%`

Beispiel: Keine Validierung von Artefakten

Das folgende Beispiel zeigt das ARTIFACT=NONE-Format. ARTIFACT=NONE ist so, als ob Sie das Schlüsselwort nicht hinzufügen würden; es kann keine Validierung von Artefakten durchgeführt werden.

Verwendung: `%REQUEST=@{ARTIFACT=NONE:call_req_id.ref_num}%`

Beispiel: `%REQUEST=1234%`

Beispiel: Validieren einer Ticketnummer gegen den Hash-Code zur Bestätigung

Das folgende Beispiel zeigt das ARTIFACT=PROTECTED-Format. Das PROTETED-Format validiert ein Ticket gegen den Hash-Code zur Bestätigung. Der Buchstabe "A" symbolisiert den Typ der Formatierung. Das "A", der Hash-Code und die Ticketnummer werden durch Kommas getrennt.

Verwendung: `%REQUEST=@{ARTIFACT=PROTECTED:call_req_id.ref_num}%`

Beispiel: `%REQUEST=A,12345678,1234%`

Beispiel: Verschlüsseln der Ticketnummer

Das folgende Beispiel zeigt das ARTIFACT=SECURE-Format. Das SECURE-Format verschlüsselt die ref_num und verschlüsselt dann das Ergebnis in Base64-Codierung, so dass es sicher in den Meldungstext eingeschlossen werden kann. Der Buchstabe "B" symbolisiert den Typ der Formatierung. Das "B" und eine mit einem Kennwort verschlüsselte Ticketnummer werden durch Kommas getrennt.

Verwendung: %REQUEST=@{ARTIFACT=SECURE:call_req_id.ref_num}%

Beispiel:

%REQUEST=B,da1jhr+9U5GVfd2VGH4dsnx2+PaSvygDS2e3IqjpjtyNSDW2u/K
NPX61nopDu/KB%

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 Service Desk Manager 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.

Verwendung von SLAs

In CA Service Desk Manager richten Sie Service Level Agreements (SLAs) mit Hilfe von Servicetypen und Ereignissen für folgende Aufgaben ein:

- Benutzen von Ereignissen, um Tickets zu überwachen.
- Verwenden von Servicetypen zum Verfolgen von Anbieter- und Organisationsverpflichtungen sowie Schichten, die sich auf bestimmte Tickets beziehen.
- Einrichten von Datums- und Zeitsteuerungen für die Verarbeitung von Ereignissen und Diensttypen

Mit CA Service Desk Manager können Sie SLAs folgendermaßen erstellen und verwenden:

- **SLAs für mehrere Organisationen** - Sie können unterschiedliche Servicetypen für jedes Referenzfeld je nach der betroffenen Organisation des Tickets zuweisen. Zum Beispiel kann der Diensttyp für ein Ticket mit der Priorität 1 für Organisation A anders lauten als für Organisation B.
- **Mehrfache SLA-Nachverfolgung** - Ein Ticket kann mehrere Servicetypen gleichzeitig verfolgen, um sicherzustellen, dass alle Aspekte eines verhandelten SLA dargestellt werden.
- **Prognosen für verbleibende Zeit bis zur Verletzung** - Ein Subsystem, das fortwährend Tickets in CA Service Desk Manager überwacht und aufzeichnet, wann ihre SLAs auf der Basis ihres aktuellen Status Verletzungen begehen.
- **Kosten für SLA-Verletzungen** - Dieses Servicetypen-Feld hilft mit Indikatoren und der Bestimmung des Schweregrades von offenen Tickets.
- **Servicetypen für Aufgaben** - Servicetypen sind für Workflow-Aufgaben verfügbar.
- **Serviceziele** - Servicetypen können auch ein oder mehrere Serviceziele für die Abschätzung haben, ob der erforderliche Service oder die erforderliche Reparatur innerhalb der erforderlichen Zeit abgeschlossen wurde.

Klassische SLA-Behandlung

In der "klassischen" SLA-Behandlung (aktiviert, falls die Option "classic_sla_processing" im Optionsmanager installiert wurde) kann nur ein Servicetyp gleichzeitig auf ein Ticket angewandt 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.

Servicetypen und Ereignisse

Um Verpflichtungen und Schichten beim Anbieter und der Organisation zu verfolgen, insofern sie sich auf bestimmte Tickets beziehen, können Sie Ereignisse mit Servicetypen verbinden. Servicetypen bieten einen flexiblen und wirksamen Weg, Ereignisse automatisch zu Tickets zuzuordnen.

Diensttypen bieten automatische Unterstützung für die Service Level Agreements, die Sie mit Ihren Kunden abgeschlossen haben. Mit Servicetypen können Sie jeden Aspekt einer zeit- oder bedingungsabhängigen-Situation überwachen. Zum Beispiel können Sie eine Richtlinie festlegen, die eine Lösungsdauer für ein bestimmtes Issue definiert, und ihr eine Aktion zuordnen. Diensttypen bieten die Möglichkeit, Service Provider, Anbieter und den Service Desk selbst zu verwalten, wodurch eine einfache Messung der Leistung und der Erfüllung möglich wird.

Mit Servicetypen können Sie Folgendes tun:

- Die für bestimmte Tickets erforderliche Dienstebene automatisch identifizieren.
- Bedingungen für Service-Level-Verletzungen identifizieren.
- Warnmeldungen vor Ablauf der Service Level Agreements automatisch senden.
- Berichte über Verletzungen von Service Level Agreements einrichten.

Implementieren von Servicetypen

Mit Hilfe von Servicetypen können Sie Aktionen anhand benutzerdefinierbarer Bedingungen definieren. Diensttypen können auf Tickets angewandt werden. Zum Beispiel können Sie einen Diensttyp definieren, der eine Lösungsdauer für ein bestimmtes Ticket angibt. Anschließend können Sie ein Verhalten angeben, das bei Auftreten der Aktion automatisch stattfindet, wie zum Beispiel die Benachrichtigung eines Supportmitarbeiters von einer anstehenden Verletzung. Servicetypen können aus mehreren Ereignissen und Ereignisse wiederum aus mehreren Aktionen (auf "True" und auf "False") bestehen. Sie können daher ein komplexeres Verhalten definieren, indem Sie mehrere Ereignisse zu Servicetypen hinzufügen.

Verfahren Sie wie folgt, um Servicetypen zu implementieren:

1. Verknüpfen Sie einen Servicetyp mit dem jeweiligen Attribut. Sie können eine beliebige Anzahl von Diensttypen definieren und in Beziehung zueinander ordnen.
2. Weisen Sie die Servicetypen zu CIs, Kontakten, Organisationen, Issue-Kategorien, Change-Kategorien, Anfragebereichen und Prioritäten zu. Jeder Datensatz kann nur einem Servicetyp zugewiesen werden.
3. Definieren Sie bestimmte Bedingungen, die festlegen, wann ein Service Level Agreement erfüllt oder verletzt wurde.
4. Geben Sie Aktionen an, die ausgeführt werden müssen, um den Service Desk bei der Erfüllung der Service Level Agreements zu unterstützen.
5. Verwenden Sie die richtigen Aktionen, um die Service Level Agreements automatisch durchzusetzen.

Beispiel: Verknüpfen Sie einen Servicetyp mit einem Kontakt.

In diesem Beispiel führen Sie die folgenden Schritte aus, um einen Servicetyp mit einem Kontakt zu verbinden:

1. Weisen Sie im Fenster "Kontakt - Detail" einen Servicetyp zu.
Wenn der Kontakt dann einem Ticket zugewiesen wird, wird im Feld "Servicetyp" automatisch der Servicetyp eingetragen, der im Kontaktdatensatz zugewiesen wurde.
2. Geben Sie im Fenster "Issue - Detail" im Feld "Betroffener Endbenutzer" "Alpha, Beta" als Name ein, und speichern Sie den Issue.
Das Feld "Servicetyp" wird automatisch mit dem in diesem Kontaktdatensatz definierten Wert gefüllt. Sie können diesen Standardwert überschreiben, indem Sie einen anderen Diensttyp wählen.

Vordefinierte Servicetypen

CA Service Desk Manager stellt vordefinierte Servicetypen bereit. Sie können die vordefinierten Servicetypen ändern und Servicetypen erstellen, die den Bedürfnissen Ihres Unternehmens gerechter werden. CA Service Desk Manager enthält folgende vordefinierte Servicetypen:

- 4-Stunden-Lösung
- 12-Stunden-Lösung
- 48-Stunden-Lösung
- 72-Stunden-Lösung

Wenn Sie CA Service Desk Manager zum ersten Mal installieren, ist dem Diensttyp 4-Stunden-Lösung der Prioritätscode 1 zugewiesen. Das bedeutet, dass jedes mit der Priorität 1 erstellte Ticket so behandelt wird, als wenn es innerhalb von vier Stunden gelöst werden müsste. Dem Diensttyp 4-Stunden-Lösung sind mehrere Diensttypereignisse zugeordnet, um eine schnelle Lösung zu gewährleisten:

- Die Person, für die das Ticket erstellt wurde, wird benachrichtigt, dass eine Lösung innerhalb von vier Stunden erwartet werden kann.
- Der Gruppen-Manager wird benachrichtigt, wenn das Ticket nicht innerhalb von 30 Minuten zugewiesen wird.
- Eine Warnmeldung wird an den Zuständigen und den Gruppen-Manager gesendet, wenn das Ticket nicht innerhalb von 3,5 Stunden gelöst wurde.
- Schließlich wird eine Verletzungsbenachrichtigung an den Zuständigen und den Gruppen-Manager gesendet, wenn das Ticket nicht innerhalb von 4 Stunden gelöst wurde, und für das Ticket wird die SLA-Verletzungsmarkierung gesetzt.

Keinem der anderen vordefinierten Diensttypen wird ein Prioritätscode zugeordnet. Sie werden aber mit Ereignissen definiert, die den für den Diensttyp 4-Stunden-Lösung beschriebenen ähnlich sind. Als Systemadministrator können Sie diesen Diensttypen Prioritätscodes zuweisen, sofern Sie dies wünschen. Zum Beispiel könnten Sie folgende Zuweisungen vornehmen:

- Priorität 2 – 12-Stunden-Lösung
- Priorität 3 – 48-Stunden-Lösung
- Priorität 4 – 72-Stunden-Lösung

Andererseits können Sie die Zuordnung von Prioritätscode 1 und dem Servicetyp 4-Stunden-Lösung aufheben, wenn sie Ihren Bedürfnissen nicht entspricht.

Die Anpassungsoptionen "cr_sla", "chg_sla" und "iss_sla" geben an, dass alle Anfragen, Changes und Issue mit einem Servicetyp verknüpft werden müssen. Diese Optionen wählen den besten Servicetyp und wenden ihn auf die Anfrage, den Change oder das Issue an. Sie werden bei der Installation automatisch installiert. Sie können diese Optionen aber mit Hilfe des Optionsmanagers deinstallieren oder neu installieren.

Hinweis: Beschreibungen zu den Anpassungsoptionen finden Sie in der *Online-Hilfe*. Informationen zur Definition von Servicetypen und Änderung von Prioritätscodes finden Sie in der *Online-Hilfe*.

Einrichten von Ereignissen

CA Service Desk Manager verwendet als Ereignisse definierte Bedingungen und Aktionen, um Tickets und Diensttypen automatisch zu planen, zu verarbeiten und zu verfolgen. Jedes Ereignis hat drei generische Verhaltensmerkmale: Bedingungen, Aktionen bei Wahr und Aktionen bei Falsch. Zusätzlich wird der Bedingung (und somit dem Ereignis) eine Zeitverzögerung zugewiesen, die ab dem Zeitpunkt der Speicherung des Tickets gemessen wird. Die Zeitverzögerung bestimmt, wann die Bedingung bewertet ist. Sie können auch automatische Ereignisse erstellen, damit jedes Mal, wenn ein bestimmtes Ereignis eintritt, eine bestimmte Aktion ausgeführt wird. Sie können zum Beispiel für einen übertragenen Issue mit der Priorität ", die mehr als eine Stunde offen ist, automatisch eine Benachrichtigung auslösen.

- *Bedingungen* identifizieren das Ereignis, auf das CA Service Desk Manager vorbereitet sein sollte.

Eine Bedingung ist praktisch ein beliebiger messbarer Status eines Tickets. Ein Ticket mit dem Status „Nicht zugewiesen“ ist ein Beispiel für eine Bedingung. Diese Bedingung kann dann mit einer Aktion verbunden werden, die stattfindet, wenn die Bedingung wahr (True) oder falsch (False) ist. Zum Beispiel enthält der vordefinierte Servicetyp 12-Stunden-Lösung ein zugehöriges Ereignis mit der Bezeichnung "1 Stunde nicht zugewiesen" mit der Bedingung "Nicht zugewiesenes Issue". Die für dieses Ereignis definierte Aktion besteht darin, den Gruppen-Manager Problemanfragen zu benachrichtigen, wenn die Bedingung wahr, mit einer Zeitverzögerung von einer Stunde. Wenn einem Issue die 12-Stunden-Lösung zugewiesen wurde, ist das Verhalten wie folgt: eine Stunde nach Speichern der Aufzeichnung "aufwachen", prüfen, ob bereits eine Zuweisung erfolgte, und, falls keine Zuweisung erfolgte, den Gruppen-Manager für Issues benachrichtigen.

- *Aktionen* identifizieren die Prozesse, die automatisch ausgeführt werden, wenn die Bedingung nach einer bestimmten Zeitspanne wahr oder falsch ist.

Sie können für jedes überwachte Ereignis eine einzige Aktion oder eine Liste von auszuführenden Aktionen zuweisen. Wenn ein Ereignis eintritt, das einer Bedingung entspricht, verarbeitet CA Service Desk Manager die mit der Bedingung verbundenen Aktionen automatisch. In einigen Fällen verarbeiten Aktionen das Objekt automatisch, oder sie können eine Benachrichtigung verursachen.

Die folgende Tabelle enthält einige der vordefinierten Ereignisse für Issues. Es gibt ähnliche vordefinierte Ereignisse für Anforderungen und Changes sowie mehrere andere, die sich auf die vordefinierten Servicetypen beziehen:

Ereignis	Beschreibung
P1 aktiv - Zuständ. benachr.	Benachrichtigt den Zuständigen, wenn das Issue mehr als 1 Stunde aktiv und die Priorität 1 ist
P2 aktiv - Zuständ. benachr.	Benachrichtigt den Zuständigen, wenn das Issue mehr als 1 Tag aktiv und die Priorität 2 ist
N. zugew. - Prbl.anfr.-Transf.	Überträgt Issues, wenn sie mehr als 1 Tag nicht zugewiesen bleiben; benachrichtigt den alten Zuständigen, den Ersteller des Issue und den neuen Zuständigen

Nachdem die Ereignisse definiert wurden, können sie manuell oder automatisch mit Tickets und Servicetypen verbunden werden, wie im Fall von vordefinierten Servicetypen. Jedem Diensttyp können mehrere Ereignisse zugeordnet werden.

Wichtig! Benutzen Sie den Optionsmanager nicht, um automatische Ereignisse zu installieren, bis die Ereignisse erstellt werden. Wenn Sie automatische Ereignisse aktivieren, bevor Ereignisse vorhanden sind, beeinträchtigt das die Leistung erheblich. Weitere Informationen zur Definition von Ereignissen und Ereignisoptionen wie "auto_events", "chg_auto_events" und "iss_auto_events" finden Sie in der *Online-Hilfe*.

Weitere Informationen:

[Verwendung des Optionsmanagers](#) (siehe Seite 363)

Serviceziele

Um 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 einer Ticket-Erstellung weist ein Servicetyp ein oder mehrere Serviceziele zu, um jede Stufe der Ticket-Lösung zu verfolgen. 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 Hilfe von Servicezielen können Sie:

- 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.

Serviceziele werden in zwei Schritten konfiguriert. Zuerst erstellen Sie einen Satz von Servicezielvorlagen. Dann verknüpfen Sie die Vorlagen mit einem bestimmten Servicetyp. Bei der Ticket-Erstellung wird dem Ticket die entsprechende Vorlage auf der Basis des Servicetyps automatisch zugewiesen.

Berücksichtigen Sie beim Erstellen von Servicezielvorlagen die folgenden Schritte:

- 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.

So erstellen Sie eine Servicezielvorlage

1. Erstellen Sie eine Servicezielvorlage zum Verwalten von Anfragen, Incidents, Problemen, Changes oder Issues.
2. Verknüpfen Sie die Servicezielvorlage mit einem Servicetyp.
3. Weisen Sie das Detail der Servicezielvorlage einer Ticket-Kategorie zu, wie zum Beispiel Anfrage-, Incident-, Problem-, Change- oder Issue-Tickets.

Wenn ein Benutzer ein Ticket erstellt, wird der Status des Service-Ziels automatisch auf der Registerkarte "Servicetyp" 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 *betreffende Organisation* des Tickets bestimmt, die immer die Organisation des betroffenen Endbenutzers 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 Endbenutzer 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 Endbenutzer dringend eine Tastatur benötigt, kann die Servicepriorität aber erhöht werden.

Hinweis: Das SLA-Modell wird standardmäßig erzwungen. In früheren Versionen von CA Service Desk Manager 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 Service Desk Manager 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 Service Desk Manager 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.

Zeitzonen und Schichten

Um den komplexen Geschäftsanforderungen automatisierter Anwendungen gerecht zu werden, können Sie in CA Service Desk Manager so viele Zeitzonen und Schichten wie nötig definieren und sie aufzeichnen, um einfach auf sie zu verweisen.

- Zeitzonen geben die Zeitzone an, in der sich der Benutzer, das CI usw. befindet.
- Schichten definieren den Zeitraum, in dem die Ereignisüberwachung aktiv ist, oder die Arbeitszeit eines Servicetyps oder SLA.

Für die korrekte Handhabung von Ereignissen kann es äußerst wichtig sein, einen Aktionsverlauf auf der Basis des Zeitpunkts zu bestimmen, zu dem ein Ereignis auftritt. Die von Ihnen definierten Zeitzonen und Schichten stehen allen Funktionen von CA Service Desk Manager zur Verfügung.

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 Service Desk Manager-Servers eingegeben. Das bedeutet, dass Geschäftszeiten immer einheitlich verglichen werden können.

Zeitzone dienen dazu, Diensttypen, Eskalationen und die Gesamtantwort für betroffene Endbenutzer auf der Basis der Fähigkeit von CA Service Desk Manager zu verwalten, die korrekte Zeit über mehrere Zeitzone darzustellen. CA Service Desk Manager 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 Service Desk Manager-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 Service Desk Manager 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 Service Desk Manager, 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 - Zuständ. 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 275)

Sicherheit

Bevor andere Personen mit CA Service Desk Manager arbeiten, müssen Sie die Sicherheit einstellen, um festzulegen,

- welche Benutzer auf das System zugreifen dürfen,
- welche Zugriffsebenen für die Benutzer freigegeben sind,
- wie Benutzer 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-Produkte installiert haben, verwenden einige dieser unter Umständen CA EEM zum Speichern von Identitäten und Zugriffsrichtlinien. CA Service Desk Manager benutzt nur CA EEM zur Authentifizierung. CA EEM ist keine CA Service Desk Manager-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 Service Desk Manager 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 Service Desk Manager-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 Service Desk Manager-Kontaktdatensätze nicht.

Hinweis: Informationen zum Konfigurieren des Zugriffs für CA Workflow finden Sie im *Implementierungshandbuch*.

CA Service Desk Manager

CA Service Desk Manager speichert Kontaktinformationen in MDB-Tabellen. Diese Tabellen haben keine Beziehung zu CA EEM. CA Service Desk Manager verwendet EEM> nicht für die Zugangs- oder Identitätsverwaltung. CA Service Desk Manager verwaltet den eigenen Zugriff und die eigene Sicherheit mit Hilfe von Zugriffstypen und Datenaufteilungen.

CA Service Desk Manager benutzt CA EEM nur zur Authentifizierung. Wenn Sie mit CA EEM Benutzer in CA Service Desk Manager authentifizieren möchten, installieren Sie CA EEM. Wenn Sie CA Service Desk Manager in CA EEM integrieren, ersetzt es die CA Service Desk Manager-Betriebssystemauthentifizierung durch die CA EEM-Authentifizierung.

Hinweis: Informationen zum Installieren von CA EEM finden Sie im *Implementierungshandbuch*. Um CA EEM und CA Service Desk Manager zu integrieren, müssen Sie die Optionen *eiam_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 Service Desk Manager-Benutzerdatenbank ist von der Datenbank von CA EEM und daher auch von der CA Workflow-Benutzerdatenbank getrennt. Der Vorteil für CA Workflow besteht darin, dass Workflow-Elemente Personen außerhalb von CA Service Desk Manager 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 Service Desk Manager-Integration. Ein Arbeitsschritt kann dem eigentlichen CA Service Desk Manager-Kontaktdatensatz nicht direkt zugewiesen werden. Die Arbeitsschritt-Zuweisung zu CA Service Desk Manager-Kontakten kann nur durchgeführt werden, wenn beide der folgenden Bedingungen erfüllt werden:

- Der CA Service Desk Manager-Kontakt hat einen entsprechenden Datensatz in CA EEM.
- Diese Datensätze haben übereinstimmende Benutzer-IDs.

Zusammenfassung:

- CA Service Desk Manager verwendet die MDB, um Kontaktinformationen zu speichern. CA Service Desk Manager bietet auch LDAP-Integration, die es CA Service Desk Manager 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 Benutzerverwaltung. 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 Benutzerdatensätze 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 Service Desk Manager verwendet wurden.

- CA Workflow verwendet immer CA EEM für seine Benutzerinformationen und die Authentifizierung. Arbeitsschritte können nur Benutzern zugewiesen werden, die CA EEM bekannt sind. Außerdem können nur von CA EEM definierte Benutzer auf die integrierte Entwicklungsumgebung (IDE, Integrated Development Environment) von CA Workflow und die Worklist-Web-Benutzerschnittstelle zugreifen.

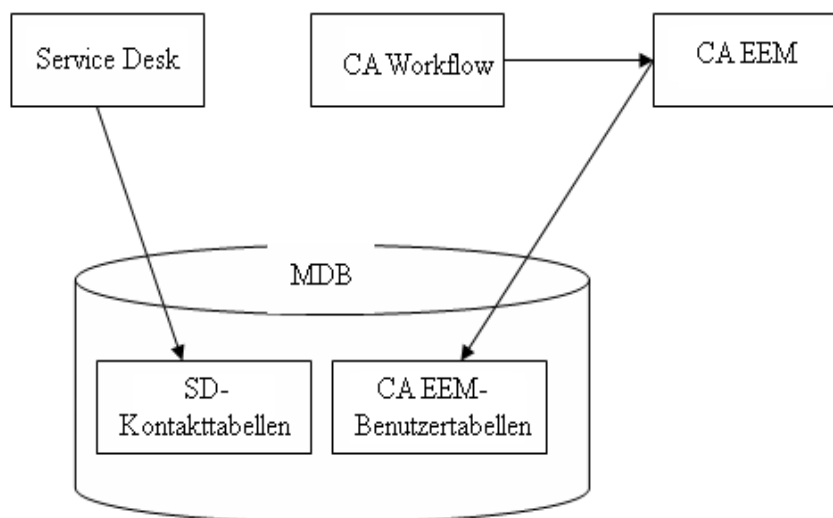
Die folgenden Informationen behandeln die unterschiedlichen Konfigurationsoptionen für die Produkte und erläutern, wie diese die Integration von CA Service Desk Manager und CA Workflow beeinflussen. Wählen Sie die Konfiguration aus, die Ihrer Verwendung von CA Workflow und (optional) einem LDAP-Verzeichnisserver am besten entspricht.

Standardkonfiguration

CA Service Desk Manager und CA Workflow speichern Benutzerdaten nach einer Standardinstallation wie folgt:

- CA Service Desk Manager speichert Benutzerdaten in den CA Service Desk Manager-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:

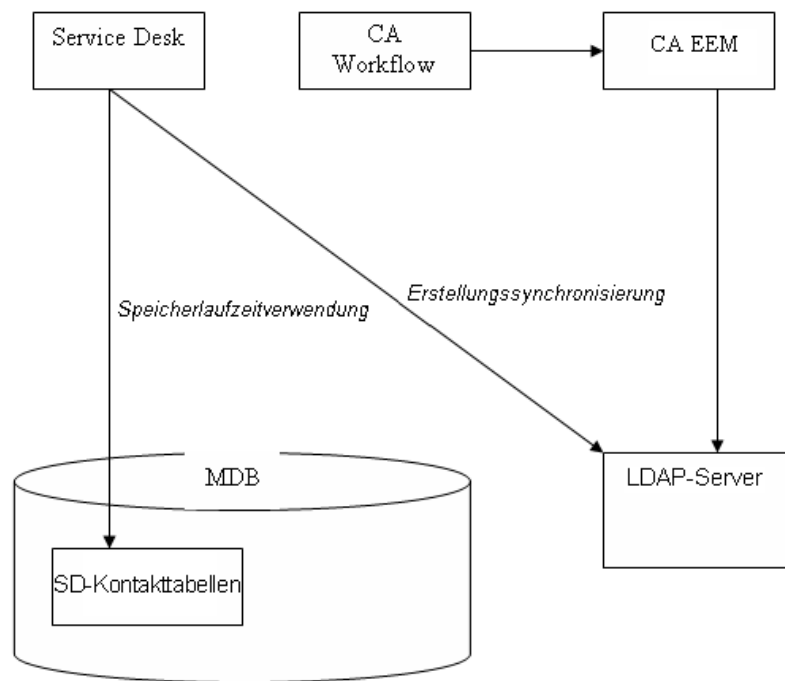


Ziehen Sie die Verwendung der Standardkonfiguration in Betracht, wenn Ihr Standort CA Workflow oder eine LDAP-Verzeichnissever nur wenig oder überhaupt nicht verwendet. Diese Konfiguration kann einige Herausforderungen bedeuten. Jeder CA Workflow-Benutzer benötigt einen CA EEM-Benutzerdatensatz.

Externe LDAP Server-Konfiguration

Die Verwaltung von Kontakten wird vereinfacht, wenn CA Service Desk Manager und CA Workflow den gleichen LDAP-Verzeichnissever benutzen. Dies ist besonders nützlich, wenn Ihr Standort bereits einen LDAP-Server als Hauptverzeichnis für Benutzer verwendet. Aufgrund der LDAP-Fähigkeit von CA Service Desk Manager entsprechen die Benutzer-IDs von Kontakteinträgen den IDs im Verzeichnis entsprechen, was eine problemlose Zuweisung von Arbeitselementen zu CA Service Desk Manager-Analysten ermöglicht. Eine noch nahtlosere Integration erzielen Sie, wenn CA Service Desk Manager 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 Service Desk Manager verwendet weiterhin die Kontakttabellen in der MDB für seine Benutzerdatensätze. Diese Datensätze können aber vom LDAP-Server importiert und regelmäßig mit diesen synchronisiert werden.

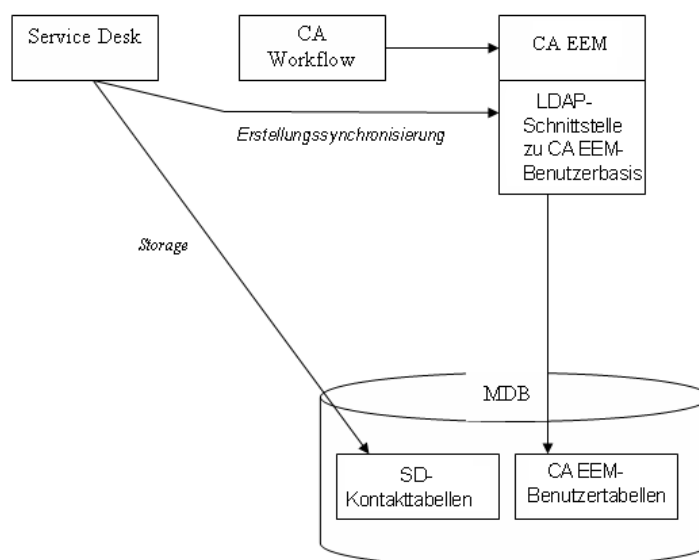


Weitere Informationen:

[LDAP-Verzeichnis-Daten](#) (siehe Seite 212)

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 Service Desk Manager 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 Service Desk Manager so, dass es auf denselben LDAP-Server und *nicht* auf CA EEM verweist.

Aktualisieren

Wenn Sie die Migration einer früheren Version von CA Service Desk Manager durchführen oder viele Kontakteinträge im Batchprozess laden, müssen Sie diese Benutzer manuell zu CA EEM hinzufügen, damit sie Zugriff auf CA Workflow erhalten.

Benutzerverwaltung in CA EEM

Im Folgenden werden die verschiedenen Benutzerverwaltungsoptionen in CA EEM behandelt.

Konfigurieren des CA EEM-Benutzerspeichers

Sie können CA EEM so konfigurieren, dass Benutzerdatensätze 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 Benutzer nicht über die CA EEM-Schnittstelle hinzufügen oder ändern.

So konfigurieren Sie die Quelle für Benutzerdatensätze für CA EEM:

1. Klicken Sie auf "Start", "Programme", "CA", "eTrust", "eTrust Embedded IAM", "Embedded IAM UI".

Die CA EEM-Benutzerschnittstelle wird angezeigt.

2. Klicken Sie auf die Registerkarte "Konfigurieren".
3. Klicken Sie auf die untergeordnete Registerkarte "Embedded IAM Server" (Eingebetteter IAM-Server).
4. Wählen Sie im linken Fenster die Verknüpfung für globale Benutzer und Gruppen.
5. Wählen Sie im rechten Fensterbereich eine der folgenden Optionen:
 - In der Management-Datenbank von CA (CA-MDB) speichern
 - Referenz von einem externen Verzeichnis

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 der Speicherung von Benutzern in CA EEM ist abgeschlossen.

Hinweis: Weitere Informationen über CA EEM finden Sie in der *CA EEM-Online-Hilfe*.

Hinzufügen von Benutzern und Gruppen

Wenn CA EEM so konfiguriert ist, dass es auf ein externes Verzeichnis verweist, können Sie über die CA EEM-Benutzerschnittstelle keine Benutzer hinzufügen. Für den LDAP-Server ist CA EEM eine schreibgeschützte Schnittstelle. Zur Aktualisierung der Benutzerdatensätze müssen Sie die Schnittstelle verwenden, die von Ihrem LDAP-Serverprodukt bereitgestellt wird.

So fügen Sie einen neuen Benutzerdatensatz hinzu:

1. Klicken Sie auf "Start", "Programme", "CA", "eTrust", "eTrust Embedded IAM", "Embedded IAM UI".
2. Melden Sie sich mit dem CA EEM-Administratorbenutzernamen und -kennwort an. Diese werden während der CA EEM-Installation angegeben. CA EEM muss getrennt installiert werden und ist keine Konfigurationsoption für CA Service Desk Manager.

3. Klicken Sie auf die Registerkarte "Identitäten verwalten".

4. Klicken Sie im linken Fensterbereich auf die Registerkarte "Benutzer", um existierende Benutzerdatensätze 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 "Benutzer".

Das Formular zum Erstellen eines Benutzerdatensatzes wird angezeigt.

6. Füllen Sie die Felder aus, und klicken Sie auf "Speichern".

Der neue CA EEM-Benutzerdatensatz wird in der MDB abgespeichert.

Hinweis: Die Schritte, um einen existierenden Benutzerdatensatz 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 Service Desk Manager angegeben wird, hat vollen Zugriff.

Standardmäßig wird dieser Benutzer von CA Service Desk Manager 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 Service Desk Manager-Anwendungsinstanz in CA EEM definiert. Wenn Sie sich in der CA EEM-Web-Benutzerschnittstelle anmelden, müssen Sie die CA Service Desk Manager-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 Service Desk Manager-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 Service Desk Manager-Anwendung aus, und geben Sie den CA EEM-Administratorknamen 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 Service Desk Manager.

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 Service Desk Manager mit der Benutzer-ID eines entsprechenden Benutzerdatensatzes in CA EEM übereinstimmt. Die Demonstration einer PC-Definition zeigt, wie Benutzer-IDs von CA Service Desk Manager 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 Service Desk Manager 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 "CMDB-Benutzer" einstellen, müssen Sie den Zugriffstyp von neuen Benutzern nicht ändern, wenn sie keine zusätzlichen Berechtigungen benötigen. Dementsprechend können Sie auch "CMDB-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 "CMDB-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 IT-PAM

CA Service Desk Manager und CA IT-PAM 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 IT-PAM-Authentifizierung die folgenden Empfehlungen:

- Eine Option für Sie ist, CA IT-PAM so zu konfigurieren, dass CA EEM als Authentifizierungsserver verwendet wird. CA IT-PAM 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 IT-PAM erforderlich.

Hinweis: Um Authentifizierungssicherheit in dieser Integration zu erreichen, ist es nicht notwendig, CA Service Desk Manager für die Verwendung von CA EEM zu konfigurieren. Allerdings ist CA EEM für das Implementieren von Mandantenfähigkeit in CA IT-PAM erforderlich. Weitere Informationen zum Implementieren von Mandantenfähigkeit mit CA IT-PAM finden Sie in der CA IT-PAM-Benutzerdokumentation. Weitere Informationen darüber, wie Sie CA IT-PAM für die Verwendung von CA EEM als Authentifizierungsserver konfigurieren können, finden Sie in der CA IT-PAM-Installations- und Konfigurationsdokumentation.

- Konfigurieren Sie CA IT-PAM 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 IT-PAM für HTTPS finden Sie in der CA IT-PAM-Installations- und Konfigurationsdokumentation.

Benutzerauthentifizierung

CA Service Desk Manager bietet eine Lösung für die Benutzerauthentifizierung, die Sie als Teil des Zugriffstyps anpassen können. Die gleiche Authentifizierung wird von allen CA Service Desk Manager-Schnittstellen und von anderen CA-Produkten verwendet.

Hinweis: Sie können die Benutzerauthentifizierung von CA Service Desk Manager 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 Service Desk Manager

CA Service Desk Manager 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 Service Desk Manager 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 Service Desk Manager 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 Service Desk Manager erlaubt Benutzern den Zugriff auf das System ohne Eingabe einer Benutzer-ID, wenn alle folgenden Voraussetzungen erfüllt sind:

- Für den Benutzer wurde eine externe Authentifizierung festgelegt.
- Die Benutzerkennung des extern authentifizierten ist einem Kontakt in der Kontakttablette zugeordnet.
- Der Kontaktdatensatz verfügt über einen Zugriffstyp, dessen Authentifizierungsdefinition eine externe Authentifizierung erlaubt.

Die externe Authentifizierung erlaubt Benutzern in den folgenden Fällen keinen Zugriff auf das System:

- Ein Benutzer versucht, über einen ungesicherten Server auf das System zuzugreifen.
- Ein Benutzer 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 Benutzer 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 Benutzern 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 Benutzeranmeldung 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 Benutzer auf der Grundlage der angegebenen Validierungsart authentifiziert.

Nachfolgend finden Sie einige Beispiele für externe Authentifizierung:

- Wenn sich ein Benutzer mit Administratorrechten an einen Windows-Computer anmeldet, kann der Benutzer administrative Aufgaben ausführen, ohne weitere Anmeldeinformationen angeben zu müssen.
- Wenn ein Benutzer über einen HTTPD-Server authentifiziert wurde, er auf die Web-Schnittstelle zugreifen, ohne weitere Anmeldeinformationen angeben zu müssen. Da der Zugriffstyp "Administrator" den Web-Benutzertyp "Analytiker" angibt, wird die entsprechende Web-Schnittstelle für den Analytiker automatisch aufgerufen.

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 Service Desk Manager 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".

Hinweis: Weitere Informationen zum Benutzervalidierungs-Host finden Sie im *Implementierungshandbuch*.

- **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 Kontaktstabelle finden Sie im *Technischen Referenzhandbuch*.

Anzahl angemeldeter und lizenzierter Benutzer

Der webLicenseCt-KPI zählt die angemeldeten Benutzer, die eine CA Service Desk Manager-Lizenz verwenden. Das Kontrollkästchen "Lizenziert?" auf der Zugriffstypen-Seite legt fest, ob dieser Kontakt ein lizenzierter Zugriffstyp ist. Kontakte, die unlicenzierten Zugriffstypen zugewiesen sind, können lediglich ihre eigenen personenbezogenen Daten anzeigen und aktualisieren. Außerdem zählt der KPI "webSessionCT" die Gesamtanzahl der Websitzungen, wobei sowohl lizenzierte Analystenbenutzer als auch Endbenutzer, die sich bei der Web-Self-Service-Schnittstelle anmelden, gezählt werden. Falls ein Benutzer mehrmals bei CA Service Desk Manager angemeldet ist – auf dem eigenen oder einem anderen Computer –, treten mehrere Websitzungen auf. Ist der Benutzer ein Analyst, werden mehrere Lizenzen verwendet. Sind für den angemeldeten Benutzer mehrere Seiten geöffnet, hat dies keinen Einfluss auf die Anzahl der Websitzungen und Weblizenzen.

Hinweis: Weitere Informationen zu Zugriffstypen finden Sie in der *Online-Hilfe*.

Beispiel: Anzahl von lizenzierten und angemeldeten Benutzern

Drei Endbenutzer sind bei 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.

Der KPI "webLicenseCt" zeigt eine Anzahl von fünf an – das heißt, es werden derzeit fünf Lizenzen verwendet.

Der KPI "webSessionCt" zeigt eine Anzahl von acht an – das heißt, es sind insgesamt acht Benutzer bei der Webschnittstelle von CA Service Desk Manager angemeldet.

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 Service Desk Manager-Integration

Der Zugriffstyp identifiziert auch den Benutzertyp, der mit diesem Zugriffstyp verbunden ist, wenn Benutzer andere CA-Produkte mit CA Service Desk Manager 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 Service Desk Manager-Sicherheitseinstellungen haben möglicherweise Vorrang vor der Datenpartition.

Datenaufteilungen

Eine Datenpartition ist eine Untermenge einer CA Service Desk Manager-Datenbank, die den Zugriff eines Benutzers auf Tickets und andere Datensätze auf der Basis ihres Inhalts steuert. Zum Beispiel können Sie die Ansicht eines Benutzers der Datenbank nur auf die Konfigurationselemente beschränken, die der Organisation des Benutzers zugewiesen wurden. Des Weiteren können Sie für einen Benutzer die Einschränkung festlegen, 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 Benutzer 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 Benutzers zuweisen, steuern die Einschränkungen und Einschränkungstypen den Zugriff des Benutzers auf die Datensätze in der CA Service Desk Manager-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.

Hinweis: Weitere Informationen zur Verwendung von Datenpartitionseinschränkungen finden Sie in der *Online-Hilfe*.

Einrichten von Datenaufteilungen

Sie können eine unbegrenzte Anzahl von Datenaufteilungen definieren. Jede Datenaufteilung 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 das zugegriffen wird, in Kombination mit beliebigen Daten im Kontaktdatensatz des Benutzers. 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 Datenaufteilungseinschränkungen für Anbieter festlegen, die direkt auf CA Service Desk Manager zugreifen dürfen.

Aus Gründen der Leistung sind in CA Service Desk Manager 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. Weitere Information zur Definition von Datenpartitionen, Einschränkungen und Einschränkungstypen finden Sie in der *Online-Hilfe*.

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 Datenaufteilungseinschränkung 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 wie folgt 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
Anzeigen	assignee.organization = @root.organization Gibt an, dass der Benutzer Changes nur dann anzeigen kann, wenn die Organisation des Zuständigen mit der Organisation des Benutzers identisch ist.
Vor-Aktualisierung	requestor = @root.id 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

Einschränkungstypen

Sie können für jede gesteuerte Tabelle in einer Datenpartition die folgenden Arten von Bedingungen zuweisen:

Erstellen

Gibt Kriterien an, die vor der Erstellung eines Datensatzes erfüllt sein müssen. Wenn ein Benutzer in der Datenaufteilung die Erstellung eines Datensatzes versucht, der nicht der Erstellungstestbedingung entspricht, gibt CA Service Desk Manager die mit der Bedingung verbundene Fehlermeldung aus und speichert den Datensatz nicht.

Standardwerte

Gibt eine oder mehrer 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 *Wert* eine Ganzzahl, eine Zeichenfolge zwischen Anführungszeichen oder ein Verweis der Form `@root.att_name` auf ein Majic-Attribut im Kontaktdatensatz für den aktuellen Benutzer 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 Kriterien an, die zum Löschen eines Datensatzes erfüllt sein müssen. Wenn ein Benutzer in der Datenaufteilung einen Datensatz zu löschen versucht, der nicht der Löschbedingung entspricht, gibt CA Service Desk Manager 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 Benutzer in der Datenaufteilung einen Datensatz anfordert, der nicht der Vor-Aktualisierungsbedingung entspricht, versetzt CA Service Desk Manager den Datensatz in den schreibgeschützten Status und gibt die mit der Bedingung definierte Fehlermeldung aus.

Update

Gibt Kriterien an, die zum Speichern eines Datensatzes erfüllt sein müssen. Wenn ein Benutzer in der Datenaufteilung einen Datensatz zu speichern versucht, der nicht der Aktualisierungsbedingung entspricht, gibt CA Service Desk Manager die mit der Bedingung verbundene Fehlermeldung aus und speichert den Datensatz nicht.

Anzeigen

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.

Erstellen einer Datenpartitionseinschränkung für CAB-Zuweisungen

Sie können eine Datenpartitionseinschränkung erstellen, die Benutzer nur Changes aktualisieren lässt, die einem CAB zugewiesen sind, dem der angemeldete Benutzer 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.

Weitere Informationen:

[CAB-Konsole und Berichterstattung](#) (siehe Seite 721)

Konfigurieren von Knowledge-Management-Datenpartitionseinschränkungen für rollenbasierte Berechtigungen

Knowledge-Management-Datenpartitionen sind in CA Service Desk Manager 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 Datenpartitionseinschränkungen aktualisieren.

Wenn Sie benutzerdefinierte Datenpartitionseinschränkungen verwendet haben, um Wissensberechtigungen in Vorversionen zu verwalten, aktualisieren Sie die Einschränkungen für die Tabellen O_INDEXES und SKELETONS manuell. Sie können die Standard-Datenpartitionseinschränkungen anzeigen und Änderungen durchführen, wenn dies für Ihre Umgebung erforderlich ist.

So aktualisieren Sie Datenpartitionseinschränkungen:

1. Wählen Sie auf der Registerkarte "Administration" die Option "Sicherheits- und Rollenmanagement" > "Datenpartitionen" > "Datenpartitionseinschränkungen".
Die Liste der Datenpartitionseinschränkungen wird angezeigt.
2. Klicken Sie auf "Filter anzeigen".
Der Suchfilter wird angezeigt.
3. Geben Sie **Service Desk-Analyst** in der Datenpartitionssuche ein.
4. Geben Sie **O_INDEXES** in der Tabellensuche ein.
5. Klicken Sie auf "Suche".
Das Fenster "Suchergebnisse" wird angezeigt.
6. Klicken Sie auf den Einschränkungstyp *Anzeige*.
Die Seite "Datenpartitionseinschränkungen - Detail" wird geöffnet.
7. Klicken Sie auf "Bearbeiten".
Die Seite "Datenpartitionseinschränkung aktualisieren" wird geöffnet.
8. Ändern Sie die Registerkarte "Einschränkung", indem Sie "READ_PGROUP in @root.pgroups" folgendermaßen ersetzen:

```
READ_PGROUP in @root.pgroups OR  
READ_PGROUP.[pgroup]contained_roles.role IN @root.id
```


Speichern Sie die Einschränkung.
9. Öffnen Sie die Einschränkungstypen der *Löschen* und *Voraktualisierung* aus der Liste der Datenpartitionseinschränkungen.
10. Ändern Sie die Registerkarte "Einschränkung", indem Sie "WRITE_PGROUP in @root.pgroups" in *Löschen* und *Voraktualisierung* folgendermaßen ersetzen:

```
WRITE_PGROUP in @root.pggroups OR WRITE_PGROUP.[pgroup]contained_roles.role IN  
@root.role
```

11. Speichern Sie die Einschränkungen.
12. 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 Service Desk Manager-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 Service Desk Manager 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 Service Desk Manager 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 Service Desk Manager 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 Service Desk Manager-Datenbank verwaltet werden, auch Ihre eigenen Berichte entwerfen.

Verwaltete Umfrage

Mit der Funktion „Verwaltete Umfrage“ kann der CA Service Desk Manager-Administrator eine gewünschte ausgefüllte Beispielumfrage auswählen und sie einer bestimmten Umfrage zuordnen. Der Administrator kann dann gezielte Anfragen 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 Anfragen, 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).

Hinweis: Weitere Informationen hierzu finden Sie in der *Onlinehilfe*.

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 5: Konfiguration von Benutzerkonten

Dieses Kapitel enthält folgende Themen:

[Kontakte](#) (siehe Seite 205)
[Kontaktdefinitionen](#) (siehe Seite 206)
[Gruppen](#) (siehe Seite 207)
[Kontakttypen](#) (siehe Seite 208)
[Spezielle Verarbeitungstypen](#) (siehe Seite 209)
[LDAP-Verzeichnis-Daten](#) (siehe Seite 212)

Kontakte

Ein wichtiger Teil der Einrichtung eines funktionierenden Service Desk ist die Definition der Benutzer, die auf den Service Desk zugreifen. In CA Service Desk Manager 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 Service Desk Manager-Kontakte auf der Basis ihrer Art der Nutzung des Systems in logische Gruppen zu unterteilen
- Importieren Sie LDAP-Benutzerinfo in einen CA Service Desk Manager-Kontaktdatensatz.
- 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 Service Desk Manager nutzt, muss als Kontakt definiert werden. Der Kontaktdatensatz eines Benutzers definiert die Benutzerinformationen, die das System benötigt, folgendermaßen:

Grundlegende Informationen

Definiert grundlegende Identifikationsdaten wie den Name des Benutzers 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.

Anmeldung

Definiert Anmeldeinformationen, wie die Benutzer-ID und in einigen Fällen ein PIN-Feld, das als Kennwort verwendet werden muss und den Benutzer bei der Anmeldung authentifiziert. Die Benutzer-ID wird verwendet, um den Benutzer für Authentifizierungszwecke in der Kontakttable 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 Benutzer 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 Benutzers auf der Basis der Mitgliedschaft des Benutzers in einer LDAP-Verzeichnisgruppe zugewiesen werden.

Der Zugriffstyp eines Benutzers 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 Benutzer erhält. Der Diensttyp eines Kontakts definiert die Dienstebene, die ein Benutzer erhalten soll. Mit CA Service Desk Manager-Kunden werden Service Level Agreements (SLAs) ausgehandelt, und Diensttypen dienen als Mechanismus für CA Service Desk Manager zur Implementierung von SLAs. Indem Sie dem Kontaktdatensatz eines Benutzers einen Servicetyp zuweisen, können Sie garantieren, dass bei der Erstellung eines Tickets für einen als betroffener Endbenutzer identifizierten Benutzer 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 Anforderungen und wird als Teil der Definition von Anforderungsbereichen festgelegt. Des Weiteren wird sie mit den Gruppen verbunden, denen der Analyst angehört.

Senden von Benachrichtigungsmeldungen an Benutzer

Definiert die Benachrichtigungsinformationen für einen Kontakt und umfasst die verschiedenen E-Mail-Adressen und Telefonnummern, die für Benachrichtigungszwecke verwendet werden können, die Methode für Benachrichtigungen mit verschiedenen Dringlichkeitsstufen und die Schichten, innerhalb derer Benachrichtigungen empfangen werden sollen.

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 Benutzer 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 Service Desk Manager 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 Service Desk Manager-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 Service Desk Manager-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 95)

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 Verarbeitungstypen

Sie können besondere Verarbeitungstypen definieren, die Kontakte identifizieren, die besondere Aufmerksamkeit benötigen. Sie können die besonderen Verarbeitungstypen benutzen, für CA Service Desk Manager zur Verfügung stellt, oder Ihre eigenen Typen erstellen. Sie können Ticket anzeigen und lokalisieren, die einen betroffenen Endbenutzer angeben, welcher besondere Aufmerksamkeit benötigt. Zum Beispiel können Analysten den V.I.P. durchsuchen. Ordner im Scoreboard zur Identifizierung von Tickets, die einen VIP als betroffenen Endbenutzer 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 Endbenutzer" ein Warnungsbanner, ein Warnsymbol oder beides an. Mithilfe von Ticket-Feldern und speziellen Verarbeitungstypen können Sie Tickets verfolgen und zwischen zwei verwandten, aber möglicherweise unterschiedlichen Kontakttypen unterscheiden. Zum Beispiel hat ein VIP (Betroffener Endbenutzer) einen Assistenten (Requestor), der im eigenen Namen handelt. Wenn es sich bei dem betroffenen Endbenutzer um einen Kontakt handelt, der einem speziellen VIP-Verarbeitungstyp zugewiesen ist, können Tickets von einem Analysten genauer priorisiert werden.

Weitere Informationen:

[Konfigurieren von Kontakten zur speziellen Verarbeitung](#) (siehe Seite 210)
[Zuordnen von Kontakten zu bestimmten Verarbeitungstypen](#) (siehe Seite 211)

Weitere Informationen

[Zuordnen von Kontakten zu bestimmten Verarbeitungstypen](#) (siehe Seite 211)

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 211). 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 Endbenutzer 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. Die V.I.P.-Unterordner enthalten Tickets für betroffene Endbenutzer, die VIP-Kontakte zur speziellen Verarbeitung sind.

Hinweis: Der V.I.P.-Scoreboard-Ordner wird für Analystenrollen angezeigt.

Zuordnen von Kontakten zu bestimmten Verarbeitungstypen

Sie können Kontakten einen besonderen Verarbeitungstyp zuweisen, so dass Analysten bei Tickets, die Endbenutzer 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 Service Desk Manager zeigt je nach Verarbeitungstyp Folgendes an, wenn ein Ticket den Kontakt im Feld "Betroffene Endbenutzer" angibt:

- Für den betroffenen Endbenutzer 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 Endbenutzer) 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 Benutzern, Gruppen, Computern, Druckern und anderen Entitäten in einem Netzwerk enthält.

CA Service Desk Manager 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-Benutzerdatensätzen. Die Synchronisierung kann folgendermaßen geschehen:
 - **Bei Anmeldung** - Wenn ein Benutzer sich am Produkt anmeldet und ein LDAP-Datensatz für diesen Benutzer 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 Service Desk Manager-Zugriffstypen zu.
- Implementieren Sie eine Alternativmethode zur Durchführung der CA Service Desk Manager-Authentifizierung.

Hinweis: Die ldap_virtb-Komponente sorgt für LDAP-Integrations-Funktionalität, wird mit CA Service Desk Manager standardmäßig installiert, und kann entweder auf einem Primär- oder Sekundärserver unabhängig vom Typ des Betriebssystems ausgeführt werden. Weitere Informationen finden Sie im *Implementierungshandbuch*. Die Datei "\$NX_ROOT/bopcfg/majic/ldap.maj" gibt die Zuordnung zwischen LDAP-Attributen und Kontaktdatensatzattributen an.

Wichtig! Bei CA Service Desk Manager müssen LDAP-Datensätze einen Eintrag im Feld "Nachname" haben, um die LDAP-Daten zu suchen, anzuzeigen und zu importieren.

Wichtig! CA Service Desk Manager 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 SunOne 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 finden Sie in der [Datei "NX.env"](#) (siehe Seite 229).

Konfigurieren von LDAP-Optionen

Sie können CA Service Desk Manager so konfigurieren, dass der Zugriff auf LDAP-Verzeichnisdaten möglich ist.

So konfigurieren Sie CA Service Desk Manager 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 Service Desk Manager-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 Service Desk Manager.
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
ldap_filter_prefix	(&(objectClass=user)	Gibt das Präfix an, das beim Suchen nach LDAP-Benutzern auf einen automatisch erstellten Filter angewendet wird.

Option	Standardwert	Beschreibung
		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-Benutzern 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-Benutzern sucht.
ldap_enable_group	Ja	Optional. Aktiviert die Zuweisung eines CA Service Desk Manager-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-Benutzern 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.
ldap_sync_on_null	Ja	Optional. Überschreibt bestehende CA Service Desk Manager-Kontaktattribute mit ungültigen Daten, wenn das entsprechende LDAP-Benutzerattribut

Option	Standardwert	Beschreibung
		einen ungültigen Wert enthält.
ldap_service_type	Active Directory	Optional. Wählen Sie diese Option, wenn Windows als CA Service Desk Manager-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 Service Desk Manager-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 228).

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 Service Desk Manager-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 Service Desk Manager-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 "Idap_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 Service Desk Manager so konfigurieren, dass immer automatisch ein Kontakt aus einem entsprechenden LDAP-Benutzerdatensatz erstellt wird, wenn sich ein neuer Benutzer in CA Service Desk Manager 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 Service Desk Manager 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 Service Desk Manager 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 Service Desk Manager-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 Service Desk Manager-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 Benutzer-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.

-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 Benutzerkennung, 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 Benutzer-ID `jsmith11`:

```
pdm_ldap_import -l "Benutzer-ID = 'jsmith11'"
```

Dieses Beispiel importiert alle LDAP-Datensätze mit einer Benutzer-ID, die mit dem Buchstaben C anfängt:

```
pdm_ldap_import -l "userid = 'c%'"
```

Dieses Beispiel importiert alle LDAP-Benutzerdatensätze im Verzeichnis:

```
pdm_ldap_import -l "userid = '%'"
```

Weitere Informationen:

[Batch-Aktualisierung von Kontakten anhand von LDAP-Daten](#) (siehe Seite 223)

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 Gesamtanzahl der gefundenen LDAP-Einträge
Aktualisiert	1	Die Anzahl an Kontaktdatensätzen, die aktualisiert wurden,

Status	Anzahl	Beschreibung
		weil der entsprechende LDAP-Eintrag abweichende Information enthielt
Keine Übereinstimmungen	7	Die Anzahl an LDAP-Einträgen ohne entsprechenden Kontaktdatensatz
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 Service Desk Manager 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 Service Desk Manager 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 Benutzer-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 220)

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 Gesamtanzahl der gefundenen LDAP-Einträge
Aktualisiert	1	Die Anzahl der LDAP-Einträge, deren Informationen sich von ihren entsprechenden CA Service Desk Manager-Kontakteinträgen unterscheiden
Keine Übereinstimmungen	7	Die Anzahl der LDAP-Einträge mit keinem entsprechenden CA Service Desk Manager-Kontaktdatensatz
Keine Änderungen	11	Die Anzahl der LDAP-Einträge, deren Informationen mit ihren entsprechenden CA Service Desk Manager-Kontakteinträgen übereinstimmen
Mehrere Übereinstimmungen	0	Die Anzahl der LDAP-Einträge mit mehreren übereinstimmenden Kontaktdatensätzen in CA Service Desk Manager, 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 Benutzer authentifizieren, die sich in CA Service Desk Manager anmelden. Die DAP-Authentifizierung ist verfügbar, wenn die CA EEM-Authentifizierungskomponente in CA Service Desk Manager 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 Benutzers 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 Benutzer-ID stimmt mit einem CA Service Desk Manager-Kontaktdatensatz überein.
- Die Benutzer-ID stimmt mit einem Benutzerprofil in CA EEM überein.
- Die Kombination aus Benutzer-ID und Kennwort wird von >EEM> bestätigt.

Hinweis: Weitere Informationen zur Verwendung von CA EEM zur Authentifizierung finden Sie im *Implementierungshandbuch*. Weitere Informationen zum Setup des Zugriffstyps finden Sie in der *Online-Hilfe*.

Transport Layer Security

Sie können CA Service Desk Manager 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 Service Desk Manager 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 Service Desk Manager-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 die Zuordnung. Bei den Attributnamen in der linken Spalte ("id") handelt es sich um die CA Service Desk Manager-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 Service Desk Manager 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 Service Desk Manager-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 Service Desk Manager userid attribute to ADAM Userid
//
MODIFY ldap userid cn ;
MODIFY ldap middle_name middleName ;
OBJECT ldap LDAP {
  ATTRIBUTES LDAP_Entry{
    contact_num employeeNumber STRING ;
  };
} ;
```

Problembehandlung

Bei der Behandlung von Problemen der Kommunikation mit LDAP-Servern ist zu berücksichtigen, dass es selten zwei vollständig identische LDAP-Implementierungen gibt. CA Service Desk Manager-Dienstprogramme können überprüfen, ob die LDAP-Integration ordnungsgemäß funktioniert.

Hinweis: CA Service Desk Manager 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 Service Desk Manager und der virtuellen LDAP-Datenbank.

So zeigen Sie den Status aller Daemons (UNIX) oder Prozesse von CA Service Desk Manager 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 Service Desk Manager 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 (boplgln)	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=qouser
@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 SunOne Directory-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.

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 Service Desk Manager-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=Paul b. Gordon,CN=Users,DC=USVDTEST
    c(2)(0): US
    displayName(14)(0): Paul b. Gordon
    mail(14)(0): gorpa02@ca.com
    givenName(4)(0): Paul
    initials(1)(0): b
    distinguishedName(38)(0): CN=Paul b.
Gordon,CN=Users,DC=USVDTEST
    objectGUID(3)(0): 314738
    pager(12)(0): 516-647-1111
    postalCode(5)(0): 11111
    SAMAccountName(7)(0): gorpa02
    sn(6)(0): Gordon
    telephoneNumber(12)(0): 631-342-6265
    userPrincipalName(16)(0): gorpa02@USVDTEST

DN: CN=mike Habek,CN=Users,DC=USVDTEST
    displayName(10)(0): mike Habek
    givenName(4)(0): mike
    distinguishedName(34)(0): CN=mike
Habek,CN=Users,DC=USVDTEST
    objectGUID(12)(0): 312328
    SAMAccountName(7)(0): habmi02
    sn(5)(0): Habek
    userPrincipalName(16)(0): habmi02@USVDTEST
```


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 Service Desk Manager 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 Service Desk Manager 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 cpasdl    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_virtldb.c 1023 LDAP
Server port id missing
06/03 17:00:18.78 cpasdl    bopLDAP    1964 SEVERE_ERROR ldap_virtldb.c 1023 LDAP
Server distinguished name missing
06/03 17:00:18.78 cpasdl    bopLDAP    1964 SEVERE_ERROR ldap_virtldb.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_virtldb.c 958
LDAP_SRVR connecting to host(Francisco.us.danconia.net) port(389)
06/05 12:35:11.01 frisco    bopLDAP    1912 SIGNIFICANT  ldap_virtldb.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 Service Desk Manager 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 Suchenanforderung 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 Service Desk Manager 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 Service Desk Manager 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_virtldb.c    1396 Value  
not available for 'modifyTimestamp'
```

```
06/24 14:18:28.41 mclda04- bopLDAP      3844 TRACE    ldap_virtldb.c    1396 Value  
not available for 'telephoneNumber,pzWorkPhoneNumber'
```


Kapitel 6: Verwalten von Rollen

Hinweis: Weitere Informationen über andere Aspekte der Web-Schnittstelle finden Sie unter [Konfigurieren der Web-Schnittstelle](#) (siehe Seite 371).

Dieses Kapitel enthält folgende Themen:

[Rollen](#) (siehe Seite 241)
[Vordefinierte Rollen](#) (siehe Seite 241)
[Rollenbasierte Sicherheit](#) (siehe Seite 244)
[Rollenbasierte Navigation](#) (siehe Seite 253)
[Implementieren einer benutzerdefinierten Menüstruktur](#) (siehe Seite 262)
[Implementieren einer benutzerdefinierten Menüstruktur](#) (siehe Seite 264)
[Erstellen von Rollendatensätzen](#) (siehe Seite 265)
[Erstellen von Registerkartendatensätzen](#) (siehe Seite 266)
[Erstellen von Menüleistendatensätzen](#) (siehe Seite 267)
[Erstellen von Webformular-Datensätzen](#) (siehe Seite 268)
[Kopieren von Menüstrukturen](#) (siehe Seite 270)
[Erstellen und Anpassen von Menüstrukturen](#) (siehe Seite 271)
[Erstellen und Veröffentlichen von Helpsets](#) (siehe Seite 272)
[Wechseln von Rollen](#) (siehe Seite 274)

Rollen

Rollen sind die primären Datensätze, die die CA Service Desk Manager-Sicherheit und Benutzeroberflächennavigation steuern. Jede Rolle definiert eine Detailansicht des Systems und zeigt nur die Funktionen an, die Benutzer zum Ausführen der Aufgaben benötigen, die ihren Rollen 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 Service Desk Manager 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 Service Desk Manager unterstützt nur ITIL; außerdem orientiert sich die CA Service Desk Manager-Dokumentation an ITIL. Weitere Informationen finden Sie unter [ITIL-Konfiguration](#) (siehe Seite 30).

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.
	Anbieteranalyst	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

Rollentyp	Rollenname	Beschreibung
		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.
	CA Service Desk-Manager	Ist für Eskalationen zuständig und beaufsichtigt Level-1-Analysten. Kann auch globale Service-Desk-Operationen verwalten.
Administratoren	Administrator	Führt administrative Aufgaben während der CA Service Desk Manager- 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 Service Desk Manager-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

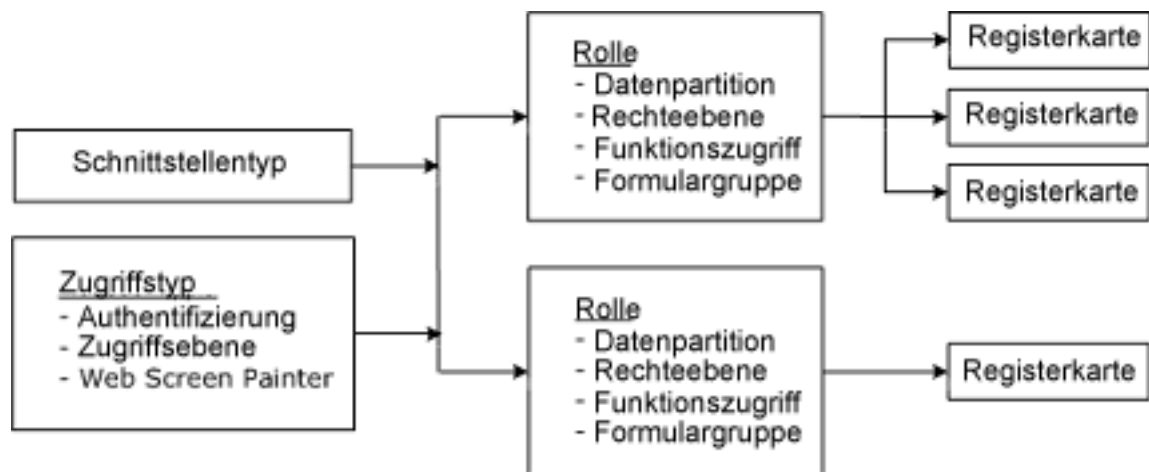
Rollentyp	Rollenname	Beschreibung
		Mandantenfähigkeit zusammenhängen; diese gelten nur für einen bestimmten Mandanten oder eine Support-Organisation.

Rollenbasierte Sicherheit

Zugriffstypen und Rollen sind die ersten Komponenten, die Sie benutzen, um die CA Service Desk Manager-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 175).



Funktionsweise von Zugriffstypen

Jeder Zugriffstyp für einen Benutzer steuert die folgenden Aspekte des Systemverhaltens:

- CA Service Desk Manager-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.
Knowledge-Management	■ Konfigurationsadministrator ■ Konfigurationsanalyst ■ Konfigurations-Viewer ■ Mitarbeiter	Verschafft administrativen Zugriff für Benutzer, die Knowledge-Management-Merkmale verwalten.

Zugriffstyp	Verknüpfte Rollen	Beschreibung
	■ Knowledge-Analyst ■ Knowledge Management-Administrator (Standard) ■ Knowledge-Manager ■ Level 2-Analyst	
Prozess-Management	■ Change Manager ■ Konfigurationsanalyst ■ Mitarbeiter ■ Incident Manager (Standard) ■ Level 2-Analyst ■ Problem Manager ■ 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.
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

Zugriffstyp	Verknüpfte Rollen	Beschreibung
		(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 Benutzerzugriff.

Die folgende Tabelle zeigt die standardmäßigen funktionellen Zugriffsebenen:

Name	Codename	Neu
Administration	admin	Nein
Incident/Problem/Anfrage	call_mgr	Nein
Änderungsauftrag	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-/Anfragereferenz	call_mgr_reference	Ja
Incident-/Problem-/Anfragevorlage	call_mgr_template	Ja
Change-Vorlage	change_mgr_template	Ja
Change-Referenz	change_reference	Ja
Konfigurationselement	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
Zeitplan	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 251) oder [mehreren](#) (siehe Seite 250) 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.

Anzeigen

Gewährt Lesezugriff auf das Funktionsobjekt.

Ändern

Gewährt Lese-/Schreibzugriff auf das Funktionsobjekt.

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.

Anzeigen

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

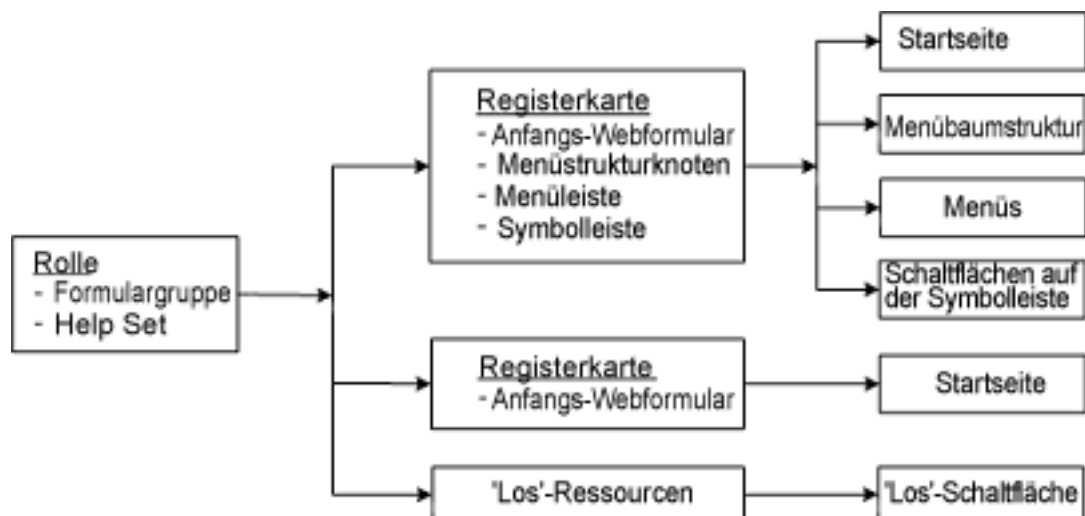
Datenpartitionen sind Untermengen der CA Service Desk Manager-Datenbank, mit denen Sie den Zugriff auf Datensatzebene steuern können. Sie können eine Datenpartition mit einer Rolle verknüpfen und so den Zugriff auf Tickets und andere Datensätze steuern, die über die Web-Schnittstelle zugänglich sind.

Weitere Informationen zum Arbeiten mit Datenpartitionen finden Sie unter [Datenpartitionszuordnungen](#) (siehe Seite 193).

Rollenbasierte Navigation

Die Ansicht jedes Benutzers der Web-Schnittstelle wird von einer Rolle definiert. Benutzer 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 737).
- 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 Service Desk Manager bietet mehrere vordefinierte Registerkarten. Sie können die vordefinierten Registerkarten einer Rolle zuweisen oder ändern sowie benutzerdefinierte 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 1101).

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 Service Desk Manager-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

Rolle	Registerkarten
Konfigurations-Viewer	■ CA CMDB-Scoreboard - Konfigurations-Viewer
Kunde	■ Registerkarte "Kunde"
Kundenservicemanager	■ Registerkarte "Service Desk" - Kundenservicemanager ■ Registerkarte "Knowledge" ■ Registerkarte "Berichte" - Kundenservicemanager
Kundenservicemitarbeiter	■ Registerkarte "Service Desk" - Kundenservicemitarbeiter ■ Registerkarte "Schnellprofil" ■ Registerkarte "Knowledge"
Mitarbeiter	■ Registerkarte "Mitarbeiter"
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

Rolle	Registerkarten
	■ 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"
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
Anbieteranalyst	■ Registerkarte "Service Desk" - Anbieteranalyst

Webformulare

Webformulare definieren die Seiten, die in der CA Service Desk Manager-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 268).

Formulargruppen

Formulargruppen definieren die Seitensätze in der CA Service Desk Manager-Web-Schnittstelle, die für eine Rolle verfügbar sind. Jede Rolle besitzt eine Formulargruppe. Benutzer 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 Service Desk Manager 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 1101) 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 Service Desk Manager 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 benutzerdefinierte 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

Menüleiste	Zugeordnete Registerkarten
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 Service Desk Manager-Hauptfenster und in allen Popupfenstern. 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:

- Änderungsauftrag
- Dokument nach ID
- Incident (Störung)
- Issue
- Wissen
- Problem
- Anforderung
- Benutzer nach ID
- Benutzer nach Name
- Benutzer nach Telefonnummer

Hilfesätze

Hilfesätze sind Sammlungen von Themen in der Online-Hilfe, die für die Benutzer 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 272).
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 264).

Implementieren einer benutzerdefinierten Menüstruktur

Für viele Standorte sind die vordefinierten Menüstrukturen hinreichend. Es kann allerdings vorkommen, dass Sie eine Rolle anpassen möchten, indem Sie eine benutzerdefinierte 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 benutzerdefinierte 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 benutzerdefiniertes 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 benutzerdefinierte Menüstruktur haben soll.
5. Melden Sie sich bei CA Service Desk Manager ab und erneut an.

Auf der Registerkarte "Administration" wird Ihre benutzerdefinierte Menüstruktur angezeigt.

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 Rollenverwaltung", "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 Benutzern.

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 1101) 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.

HTMPL-Name

Gibt den Namen des HTMPL-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 Service Desk Manager-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 HTMPL-Formular

"menu_tab_dflt.html":

`$cgi?SID=$SESSION.SID+FID=123+OP=DISPLAY_FORM+HTMPL=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 Service Desk Manager-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 auswählen, wird auch das Containerthema "Navigieren in CA Service Desk Manager" eingebunden, wenn Sie das Helpset 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 205).

So wechseln Sie Ihre Rolle:

1. Wählen Sie die gewünschte Rolle aus der Dropdown-Liste "Rolle" oben rechts in der Hauptseite der CA Service Desk Manager-Web-Schnittstelle.
2. Klicken Sie auf "Rolle festlegen".

Die Web-Schnittstelle und die verfügbare Funktionalität werden entsprechend der neu angenommenen Rolle angepasst.

Kapitel 7: Einrichten einer Support-Struktur

Dieses Kapitel enthält folgende Themen:

[Support-Struktur](#) (siehe Seite 275)
[Modelle](#) (siehe Seite 276)
[CA Workflow](#) (siehe Seite 279)
[CA IT-PAM-Workflow-Integration](#) (siehe Seite 282)
[Freigegebene Codes](#) (siehe Seite 289)
[Statuscodes](#) (siehe Seite 291)
[Aufgabentypen](#) (siehe Seite 296)
[Incident-Nachverfolgung](#) (siehe Seite 298)
[Anfrage-/Incident-/Problembereiche](#) (siehe Seite 299)
[Change- und Issue-Kategorien](#) (siehe Seite 303)
[Automatisches Schließen von Tickets](#) (siehe Seite 310)
[Aktivitäten zugehöriger Tickets](#) (siehe Seite 313)
[Prioritätsberechnung](#) (siehe Seite 315)
[Statusübergänge und abhängige Attributsteuerungen](#) (siehe Seite 332)
[Statusübergänge für Self-Service](#) (siehe Seite 343)
[Timer](#) (siehe Seite 348)
[Zeitzone](#) (siehe Seite 348)
[Dateianhänge](#) (siehe Seite 351)
[Ankündigungen](#) (siehe Seite 356)
[Einrichten von gespeicherten Abfragen](#) (siehe Seite 358)
[Sequenznummern](#) (siehe Seite 359)
[Verwenden des Audit-Protokolls](#) (siehe Seite 360)
[Integration in das CA-Netzwerk und Systemverwaltung](#) (siehe Seite 361)

Support-Struktur

Die *Support-Struktur* Ihres Service Desk besteht aus den Komponenten, die der Benutzer zur Problemlösung benötigt. Sie können die CA Service Desk Manager-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*.

Modelle

CA Service Desk Manager 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 Service Desk Manager 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 Service Desk Manager 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 Service Desk Manager 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, Anfragen 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 Kontaktyp 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.

CA Workflow

Eine CA Workflow-Prozessdefinition kann mit jedem CA Service Desk Manager-Ticket-Typ verknüpft werden. Die Prozessdefinition, die auf einzelne Tickets angewendet wird, wird von der Change-Kategorie, der Issue-Kategorie oder vom Anfrage-/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 Service Desk Manager-Installation optional CA Workflow installieren oder CA Service Desk Manager anweisen, eine andere Instanz von CA Workflow durch Aktualisieren mehrerer Optionen Optionsmanager zu verwenden, einschließlich:

CAWF_USERNAME

Gibt den CA EEM-Benutzer 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>:8080/pm/` an.

CAWF_PM_URL

Gibt als URL `http://<server>:8080/pm/services/pmService` an.

CAWF_WL_LOCATION

Gibt als Lokation `http://<server>:8080/wl/` an.

CAWF_WL_URL

Gibt als URL `http://<server>:8080/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 WF 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 Anfrage-/Incident-/Problembereich verknüpft ist. Dieses Attribut muss als Eingabeparameter gekennzeichnet werden. Wenn CA Service Desk Manager 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 Service Desk Manager zu ermöglichen.

Wichtig! Change- und Issue-Kategorien können entweder das interne (klassische) Workflow-System oder die CA Workflow-Anwendung von CA Service Desk Manager verwenden, nicht aber beide gleichzeitig. Anfrage-/Incident-/Problembereiche können nur die CA Workflow-Anwendung verwenden. Das klassische interne Workflowsystem wird nicht für Anfrage-, 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. Aktivieren Sie auf der Registerkarte "Workflow" das Kontrollkästchen "CA Workflow Workflow verwenden".

Hinweis: Wenn Sie diesen Vorgang fortsetzen und die Kategorie speichern, wird ein mit der Kategorie verbundener Workflow im Stil von CA Service Desk Manager 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 Service Desk Manager 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 IT-PAM-Workflow-Integration

CA IT-PAM ist ein eigenständiges CA-Produkt mit Funktionen zur Automatisierung und Verfolgung von Hardware- und Softwareverwaltungsaufgaben in IT-Umgebungen von Unternehmen. CA IT-PAM dient zur Automatisierung von Aufgaben und Verwaltung von Benutzerinteraktionen, wie Genehmigungen und Benachrichtigungen, um Compliance und Genauigkeit in Produktionsumgebungen zu gewährleisten.

Wenn Sie CA Service Desk Manager und CA IT-PAM integrieren, dann können Sie die Vorteile der CA IT-PAM-Workflowfunktionen von wichtigen Punkten in CA Service Desk Manager nutzen. Eine wirksame Integration von CA Service Desk Manager und CA IT-PAM erfordert, dass Sie beide Produkte kennen.

Weitere Informationen:

[CA IT-PAM-Komponenten](#) (siehe Seite 283)

[CA IT-PAM Integration mit CA Service Desk Manager zur Laufzeit](#) (siehe Seite 284)

[Erstellen einer Prozessdefinition](#) (siehe Seite 285)

[Erstellen von Startauftragsformularen](#) (siehe Seite 286)

[Anhängen von CA IT-PAM-Prozessdefinitionen](#) (siehe Seite 288)

CA IT-PAM-Komponenten

CA IT-PAM bietet viele Möglichkeiten und Strukturen, die eine breite Palette von Aktivitäten als Teile des CA IT-PAM-Prozessmanagement erleichtern. Für die Integration in CA Service Desk Manager sind allerdings nur die folgenden CA IT-PAM-Komponenten für die CA IT-PAM-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 IT-PAM-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 IT-PAM, 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 Service Desk Manager-Integration in CA IT-PAM nützlich.

Hinweis: Der Anwendungsbereich der Definitionen von CA IT-PAM-Komponenten ist auf die Verwendung innerhalb von CA Service Desk Manager beschränkt. Informationen zu CA IT-PAM-Komponenten und -Funktionen finden Sie in der CA IT-PAM-Dokumentation.

CA IT-PAM Integration mit CA Service Desk Manager zur Laufzeit

Wenn Sie die Integration durchführen, sind für CA Service Desk Manager-Benutzer folgende Funktionen verfügbar:

- Bei einer neuen Anfrage, Change oder Issue wird eine auf der Ticketkategorie oder dem Ticketbereich basierende CA IT-PAM-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 IT-PAM-Prozessinstanz beendet und eine neue Prozessinstanz ausgelöst.
- Wenn Sie als CA Service Desk Manager-Benutzer versuchen, eine Anfrage, einen Change oder ein Issue mit einer unvollständigen CA IT-PAM-Prozessinstanz zu schließen, dann können Sie das Ticket nicht schließen. Statt dessen müssen Sie zuerst das Ticket annullieren. Der Status "Annullieren" beendet die CA IT-PAM-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 IT-PAM-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 IT-PAM-Aufgabenliste aufgeführt sind.

Hinweis: Wenn Sie die CA Service Desk Manager-Schaltfläche "Vorgang anzeigen" oder CA IT-PAM-Prozessinstanz-Nachrichten auswählen, dann fordert Sie das System zur Eingabe eines CA IT-PAM-Benutzernamens und eines Kennworts für eine einzelne Browsersitzung auf. Nach der ersten Eingabeaufforderung werden Sie kein weiteres Mal aufgefordert, bis der CA Service Desk Manager-Browser beendet wird.

Erstellen einer Prozessdefinition

Wenn Sie die Prozessdefinition erstellen, füllen Sie CA IT-PAM mit Inhalt aus, der in CA Service Desk Manager angezeigt werden soll. Sie verwenden den grafischen Prozessentwickler CA IT-PAM zum Erstellen, Testen und Einchecken einer Prozessdefinition. Über CA Service Desk Manager können Sie auch Makros zum Initiieren des CA IT-PAM-Vorgangs erstellen.

Hinweis: Weitere Informationen zum Erstellen von CA IT-PAM-Makros finden Sie in der *Online-Hilfe*.

So erstellen Sie eine Prozessdefinition in CA IT-PAM:

1. Melden Sie sich beim CA IT-PAM-Client als Administrator an.
2. Verwenden Sie den grafischen Prozessentwickler CA IT-PAM zum Erstellen, Testen und Einchecken einer Prozessdefinition. Wenn Sie mit der Prozessdefinition arbeiten, benutzen Sie die Anweisungen in der CA IT-PAM-Benutzerdokumentation.

Hinweis: Wenn Sie versäumen, die Prozessdefinition einzuchecken, bevor Sie versuchen, sie zu benutzen, kann der Workflow nicht richtig in CA Service Desk Manager funktionieren.

Die folgenden Elemente der Prozessdefinition sind in CA Service Desk Manager 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 Service Desk Manager 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 Service Desk Manager-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 Service Desk Manager-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 Service Desk Manager nicht angezeigt.

So erstellen Sie ein Startauftragsformular:

1. Melden Sie sich beim CA IT-PAM-Client als Administrator an.
2. Öffnen Sie die CA IT-PAM-Bibliothek, und navigieren Sie zum Pfad des Startauftragsformulars.

Das Startauftragsformular wird im rechten Fenster der CA IT-PAM-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 Service Desk Manager-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 Service Desk Manager-Anfragebereich verfügbar zu machen, geben Sie das Schlüsselwort "pcat" ein.

Ticket	Zu verwendendes Schlüsselwort
Anforderungsbereich	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 Anfragebereichen 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 IT-PAM 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 Service Desk Manager angezeigt.

Die CA IT-PAM-Startauftragsformularinformationen werden in der CA Service Desk Manager-Startauftragsformular-Liste angezeigt. Der CA Service Desk Manager-Administrator kann das CA Service Desk Manager-Startauftragsformular mit der Prozessdefinition auf der Seite "Anfragebereich", "Change-Kategorie" oder "Issue-Kategorie - Detail" verknüpfen.

Die folgenden Startauftragsformularelemente werden in CA Service Desk Manager angezeigt:

Startauftragsformular-Name

Wird auf den Seiten "Anfragebereiche", "Change-Kategorien" und "Issue-Kategorien" angezeigt.

Startauftragsformular-Referenzpfad

Wird auf den Seiten "Anfragebereiche", "Change-Kategorien" und "Issue-Kategorien" angezeigt.

Startauftragsformular-Beschreibung

Wird auf den Seiten "Anfragebereiche", "Change-Kategorien" und "Issue-Kategorien" angezeigt. Der Text in diesem Feld beschreibt, inwieweit das Startauftragsformular für die Auswahl für einen bestimmten Anfragebereich, eine Change-Kategorie oder eine Issue-Kategorie geeignet ist.

Anhängen von CA IT-PAM-Prozessdefinitionen

Wenn Sie eine CA IT-PAM-Prozessdefinition an einen CA Service Desk Manager-Ticketbereich oder eine Kategorie anhängen, erstellen Sie eine statische Verbindung zwischen einem CA Service Desk Manager-Ticketbereich oder einer Kategorie und einer CA IT-PAM-Prozessdefinition.

Wenn ein CA Service Desk Manager-Benutzer ein Ticket erstellt oder bearbeitet und eine Ticket-Kategorie auswählt, wird die verknüpfte CA IT-PAM-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. Kategorieliste wird angezeigt.
3. Erstellen oder bearbeiten Sie einen Ticketbereich oder eine Kategorie.
Die Seite zum Aktualisieren des Objekts wird angezeigt.
4. Klicken Sie auf die Registerkarte "Workflow".
Sind die CA IT-PAM-Optionen im CA Service Desk Manager-Optionsmanager installiert, ist die Schaltfläche "CA IT-PAM verwenden" auf der Registerkarte "Workflow" verfügbar.
5. Klicken Sie auf "CA IT-PAM verwenden".

Es wird die Anfrageliste für das CA IT PAM-Startformular angezeigt. Jede Zeile in der Liste stellt ein CA IT-PAM-Startauftragsformular dar.

Hinweis: Sie können CA IT-PAM, CA Workflow oder den internen Workflow von CA Service Desk Manager 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 Anfrageliste für das CA IT PAM-Startformular 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 Benutzer 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 Benutzer kann durch Klicken auf "Prozess anzeigen" auf der Registerkarte "Workflow-Aufgaben" auf weitere Informationen zur Prozessinstanz zugreifen.

Freigegebene Codes

In CA Service Desk Manager benutzen verschiedene Arten von Tickets bestimmte zugrunde liegende Codes gemeinsam, wie zum Beispiel Codes für Priorität, Schweregrad, Auswirkung und Dringlichkeit. Anfragen und Changes sind einige Codes gemeinsam, und allen Arten von Tickets sind 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*.

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 161)

[Implementieren von Servicetypen](#) (siehe Seite 163)

Schweregrad-Codes

Schweregradcodes geben den Umfang des Schadens an Ausrüstungen an, die von einer Anfrage betroffen sind. Auf Schweregradcodes wird nur in Anfragen 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.

Wenn das System für die Verwendung der ITIL-Methode konfiguriert ist, ist für jeden Auswirkungscode ein zusätzliches Feld für den Wert verfügbar. Dieses Feld hilft, die Incident-Priorität zu berechnen.

Auswirkungskodes

Auswirkungskodes 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 Auswirkungskodes 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 291) 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 Auswirkungskodes 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
Anforderung	Muss für alle internen und kombinierten Service Desk-Modelle eingerichtet sein.
Änderungsauftrag	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.

Anfragestatuscode	Beschreibung
Problem behoben	Eine Problemanfrage wurde behoben, aber noch nicht geschlossen.
Offene Probleme	Eine Anfrage wurde als Problem identifiziert.
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

De 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.

Statuscode von Changes	Beschreibung
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.
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.
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.
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 Vervollständigung 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*.

Incident-Nachverfolgung

Durch Auswahl einer oder mehrerer Incident-Markierungen können Analysten den betreffenden Incident nachverfolgen. 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 Schließung auf niedrigerer Ebene innerhalb der Support-Organisation.
- Identifizieren Sie Tickets, die falsch zugewiesen sind.
- Angeben, dass das Ticket mithilfe eines Remote Control-Tools gelöst wurde.

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 Service Desk Manager neu.

Die Registerkarte "Effizienznachverfolgung" wird auf den Detailseiten für Incidents angezeigt.

Anfrage-/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 Service Desk Manager-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 Service Desk Manager 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 300)

[Definieren von Anfrage/Zwischenfall-/Problembereichen für Self-Service](#) (siehe Seite 303)

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 301) 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 eine 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/Problemebereiche" 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 Service Desk Manager-Modelle einrichten.
- Sie müssen Issue-Kategorien für externe und kombinierte CA Service Desk Manager-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 305)

[Vordefinierte Issue-Kategorien](#) (siehe Seite 305)

[Regeln zum Ändern von Kategorien in einem Ticket](#) (siehe Seite 305)

[Kategorieeigenschaften](#) (siehe Seite 306)

[Definieren von Change-Kategorien und Issue-Kategorien für Self-Service](#) (siehe Seite 309)

Vordefinierte Change-Kategorien

Die folgenden Gruppen von vordefinierten Change-Kategorien werden mit CA Service Desk Manager installiert:

- Hinzufügen
- Ändern
- Verschieben
- Retire

Hinweis: All diese Categoriesätze 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 Service Desk Manager 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 IT-PAM benutzt, wird eine Verknüpfung der CA IT-PAM-Prozessdefinition mit einem Workflow auf einem CA IT-PAM-Server hergestellt.
- Wenn sowohl die alte als auch die neue Kategorie den CA Service Desk Manager-Workflow verwendet, gelten die Regeln von früheren Versionen.

- Wenn die neue Kategorie CA Workflow oder CA IT-PAM und die alte den CA Service Desk Manager-Workflow benutzt, tritt Folgendes ein:
 - Alle unvollständigen und ausstehenden (Aufgaben, die aktualisiert werden können) Workflow-Aufgaben im Stil von CA Service Desk Manager 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 IT-PAM-Definition wird instanziiert.
- Wenn die neue Kategorie den CA Service Desk Manager-Workflow und die alte Kategorie den CA Workflow-Workflow verwendet, tritt Folgendes ein:
 - Die CA Workflow- oder CA IT-PAM-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 Service Desk Manager-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 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 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 Endbenutzer 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 Endbenutzer 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 311)

[Definieren einer Aktivitätsbenachrichtigung für die automatische Schließung](#) (siehe Seite 312)

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 Service Desk Manager-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 Service Desk Manager-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 Aktivitätsbenachrichtigungen 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 Systemadministratoren 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:

[Definieren von Aktivitätsbenachrichtigungen für zugehörige Tickets](#) (siehe Seite 314)

[Definieren von Benachrichtigungen über die Aktivität zugehöriger Tickets](#) (siehe Seite 315)

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.

Wenn Sie diese Version von CA Service Desk Manager installieren, verwaltet eine Standard-Prioritätsberechnung automatisch Ticketwerte. Sie können die Einstellungen der Standard-Prioritätsberechnung ändern oder zusätzliche Prioritätsberechnungen erstellen, um Incidents oder Probleme zu verwalten. Für mehrere Mandanten können Sie oder die Mandanten zusätzliche Prioritätsberechnungen mit bestimmten Einstellungen für jeden Mandanten erstellen.

In der Prioritätsberechnung definieren Sie das Ergebnis auf Basis von Business-Szenarien, um die Bedeutungsstufe und Ticketverarbeitung konsequenter zu machen. Benutzer können einige Einstellungen überschreiben, aber sie können die Priorität auf dem Ticket nicht mehr festlegen, da dieser Wert datengetrieben ist.

Hinweis: Bei einer Migration von einer Vorgängerversion ist die Prioritätsberechnung standardmäßig deaktiviert. Informationen zum Aktivieren der Prioritätsberechnung oder Beibehaltung der Anpassungen finden Sie im *Implementierungshandbuch*.

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 Endbenutzer
- 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 Benutzer Dringlichkeits- oder Auswirkungswerte überschreiben und auf "Speichern" klicken, wird die Detailseite für "Eskalieren" angezeigt, auf der die Benutzer 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.

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 Benutzeraktionen für Probleme, Incidents, Webservice, E-Mail und der Text-API ändert:

Aktion	Automatische Feldänderungen	Beschreibung
Benutzer 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" werden als CIs definiert, deren Klasse in der Unternehmensservicefamilie definiert wird. Falls das Datum "Geöffnet am" des Tickets innerhalb des Zeitrahmens des Ausfallfensters liegt,

Aktion	Automatische Feldänderungen	Beschreibung
		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.
Benutzer ändert Incident-Bereich	Urgency	Der Dringlichkeitswert ändert sich nur, wenn der neue Wert größer als der Standardwert ist.
Benutzer ändert Incident-Bereich <i>und</i> betroffenen Endbenutzer	Urgency Priorität	Wenn der Benutzer das Feld "Incident-Bereich" zuerst festlegt, ändert sich der Dringlichkeitswert, nachdem der Benutzer den Wert für "Betroffener Endbenutzer" festlegt. Die Prioritätsberechnung legt die Priorität fest.
Benutzer ändert Dringlichkeit <i>und</i> 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 Ausfallfenster 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 Benutzer einen Grund für die Änderung angeben. Wenn der Benutzer die Dringlichkeits- oder Auswirkungswerte ändert, bleiben diese Werte während der gesamten Ticket-Erstellung oder während der Ticket-Aktualisierung gleich, es sei denn, der Benutzer ändert sie erneut. Allerdings kann das System die überschriebenen Werte für Dringlichkeit oder Auswirkung aktualisieren, wenn der Benutzer das nächste Mal das Ticket aktualisiert. Nachdem das System die Dringlichkeit und Auswirkung eingestellt hat, legt die Prioritätsberechnung den Prioritätswert fest.
Benutzer wählt neuen Incident aus Basis des Knowledge-Dokument, und System hat Überschreibungen für	Impact Urgency	Das System benutzt immer das Knowledge-Dokument oder Knowledge-Lösungs-Werte unabhängig davon, ob die Werte größer oder kleiner als die standardmäßigen Prioritätsberechnungswerte sind.

Aktion	Automatische Feldänderungen	Beschreibung
Knowledge-Dokumente (siehe Seite 325)		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.
Benutzer 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.
Benutzer leitet Incident aus Knowledge-Dokument durch Auswählen einen neuen Incidents ab	Impact Urgency Priorität	Das System benutzt die Prioritätsberechnungswerte.
Benutzer leitet Incident aus Knowledge-Dokument ohne System- Überschreibungen für Knowledge-Dokumente (siehe Seite 325) ab	Impact Urgency Priorität	Das System verwendet die Prioritätsberechnungswerte unabhängig davon, wie der Benutzer 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, falls die Werte nicht leer sind. Wenn der Auswirkungs/Dringlichkeitswert im Knowledge-Dokument leer ist, verwendet das System Werte von Problem 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.

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 322).
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 Prioritätsberechnungs 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 Unternehmen 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 Mandaten 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 Service Desk Manager 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" > "Anfragen/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 Auswirkungswert 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 Dringlichkeitseskalation 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 Dringlichkeitseskalation 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/Anfragen beschränken und bestimmen, welche Felder für die einzelnen Ticket-Status angezeigt werden oder erforderlich sind:

Übergänge

Steuert, wie Benutzer verfügbare Status auf dem Incident-/Problem-/Anfrage-, 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 Endbenutzer 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 333)

[Konfigurieren der Statusübergänge](#) (siehe Seite 333)

[Konfigurieren abhängiger Attributsteuerelemente](#) (siehe Seite 335)

[Web-Service-Methoden](#) (siehe Seite 336)

[Vordefinierte Übergangsabläufe](#) (siehe Seite 337)

[Best Practices: Vordefinierte Statusübergänge](#) (siehe Seite 341)

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 333)
- [Konfigurieren abhängiger Attributsteuerelemente](#) (siehe Seite 335)

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 Service Desk Manager 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 Service Desk Manager-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 Untermandanten.

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 Attributsteuerungs-Webservices-Methoden konfigurieren:

getValidTransitions

Ermöglicht es Benutzern, die Übergänge für ein Ticket aufzulisten. Diese Methode ähnelt der vorhandenen Methode "getValidTaskTransitions", mit dem Unterschied, dass das Argument ein Ticket oder ein Status sein kann.

getDependentAttrControls

Ermöglicht es Benutzern, die gesperrten und erforderlichen Attribute für ein Attribut eines Objekts aufzulisten, das von einem permanenten ID angegeben wird. Das Status-Attribut wird ab diesem Zeitpunkt unterstützt.

Hinweis: Weitere Informationen zu Web-Service-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,

Aktueller Status:	Standardübergang	Verfügbare Folgestatus
		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		Bestätigt, Geschlossen, Offen

Aktueller Status:	Standardübergang	Verfügbare Folgestatus
geschlossen		
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		Bestätigt, Geschlossen, Offen

Aktueller Status:	Standardübergang	Verfügbare Folgestatus
geschlossen		
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
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,

Aktueller Status:	Standardübergang	Verfügbare Folgestatus
		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 "Übergänge - Listenseite" aufgelisteten Status ist ein Standard-Statusübergang (oder nächster Status) vorhanden. Der von Standard-Statusübergang gewählte Pfad stellt die Best Practice dar. Die zusätzlichen auf "Übergänge - Listenseite" aufgelisteten Statusübergänge dienen dazu, eine Reihe von Ticket-Verwaltungs-Workflows durchzuführen. Allerdings können nur "aktive" Statusübergänge, die diese Best Practice verwenden, sicherstellen, dass der richtige Workflow für die Verwaltung von Anfragen, 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	Nein	Statusübergang: von "Bestätigt" auf "Geschlossen"	Inaktiv
Bestätigt	Ungelöst geschlossen	Nein	Statusübergang: von "Bestätigt" auf "Ungelöst geschlossen"	Inaktiv
Bestätigt	Öffnen	Ja	Statusübergang: von "Bestätigt" auf "Offen"	Inaktiv

Status	Neuer Status	Standard	Status Description	Datensatzstatus
Wartet auf Antwort des Endbenutzers	Bestätigt	Nein	Statusübergang: von "Wartet auf Antwort des Endbenutzers" auf "Bestätigt"	Inaktiv
Wartet auf Antwort des Endbenutzers	Öffnen	Nein	Statusübergang: von "Wartet auf Antwort des Endbenutzers" auf "Öffnen"	Inaktiv
Wartet auf Anbieter	Bestätigt	Nein	Statusübergang: von "Wartet auf Anbieter" auf "Bestätigt"	Inaktiv
Wartet auf Anbieter	Geschlossen	Nein	Statusübergang: von "Wartet auf Anbieter" auf "Geschlossen"	Inaktiv
Wartet auf Anbieter	Öffnen	Nein	Statusübergang: von "Wartet auf Anbieter" auf "Offen"	Inaktiv
Geschlossen	Bestätigt	Nein	Statusübergang: von "Geschlossen" auf "Bestätigt"	Inaktiv
Ungelöst geschlossen	Bestätigt	Nein	Statusübergang: von "Ungelöst geschlossen" auf "Bestätigt"	Inaktiv
Ungelöst geschlossen	Geschlossen	Nein	Statusübergang: von "Ungelöst geschlossen" auf "Bestätigt"	Inaktiv
Halten	Bestätigt	Nein	Statusübergang: von "Halten" auf "Bestätigt"	Inaktiv
Halten	Geschlossen	Nein	Statusübergang: von "Halten" auf "Geschlossen"	Inaktiv
Halten	Öffnen	Nein	Statusübergang: von "Halten" auf "Offen"	Inaktiv
In Bearbeitung	Bestätigt	Nein	Statusübergang: von "In Bearbeitung" auf "Bestätigt"	Inaktiv
In Bearbeitung	Geschlossen	Nein	Statusübergang: von "In Bearbeitung" auf "Geschlossen"	Inaktiv
In Bearbeitung	Öffnen	Nein	Statusübergang: von "In Bearbeitung" auf "Offen"	Inaktiv

Status	Neuer Status	Standard	Status Description	Datensatzstatus
Öffnen	Geschlossen	Nein	Statusübergang: von "Offen" auf "Geschlossen"	Inaktiv
Pending Change (Anstehende Änderung)	Bestätigt	Nein	Statusübergang: von "Ausstehender Change" auf "Bestätigt"	Inaktiv
Pending Change (Anstehende Änderung)	Geschlossen	Nein	Statusübergang: von "Ausstehender Change" auf "Geschlossen"	Inaktiv
Pending Change (Anstehende Änderung)	Öffnen	Nein	Statusübergang: von "Ausstehender Change" auf "Offen"	Inaktiv
Nachforschen	Öffnen	Nein	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 Anfrage-Detailformularen hinzufügen, um [Statusübergänge](#) (siehe Seite 332) anzuzeigen.

Die Schaltfläche "Statusübergang" für Incident- und Anfrageprozessworkflows wird in der Mitarbeiterschnittstelle angezeigt, wenn Incident- oder Anfrageübergänge 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. "Anfrage schließen") und "Incident neu öffnen" (bzw. "Anfrage neu öffnen") nicht auf den Ticket-Detailformularen angezeigt. Stattdessen kann der Mitarbeiter den Status des Incidents oder der Anfrage 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 Anfragestatusübergang verbinden.

Hinweis: Weitere Informationen zum Verwenden von Übergangstypen finden Sie in der *Online-Hilfe*.

Weitere Informationen:

[Funktionsweise der Übergänge für Self-Service](#) (siehe Seite 344)

[Erstellen oder Aktualisieren von Übergangstypen für Übergänge](#) (siehe Seite 345)

[Verknüpfen von Übergangstypen mit Übergängen](#) (siehe Seite 345)

[Vordefinierte Übergangstypen](#) (siehe Seite 346)

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.

Vordefinierte Übergangstypen

Da alle mit dem Produkt gelieferten Beispielübergangstypen 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 346)

[Beispielübergangstypen für Anfragestatusübergänge](#) (siehe Seite 347)

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	Schließung anfordern	Schließung anfordern	■ Von "Offen" zu

Symbol	Schaltflächentext	Kopfzeilentext des Formulars	Incident-Statusübergang
Ablehnen der Incident-Schließung			"Ungelöst geschlossen" ■ Wartet auf Antwort des Endbenutzers ■ Wartet auf Anbieter ■ In Bearbeitung ■ Bestätigt

Beispielübergangstypen für Anfragestatusübergänge

Die folgende Tabelle beschreibt die Beispielübergangstypen für Anfragestatusübergänge:

Hinweis: Der Status "Schließung angefordert" für Anfragen ist die Entsprechung des Status "Gelöst" für Incidents.

Symbol	Schaltflächentext	Kopfzeilentext des Formulars	Anfragestatusübergang anfordern
Schaltfläche "Anfragelösung akzeptieren"	Annehmen	Lösung akzeptieren	"Schließung angefordert" zu "Geschlossen"
Schaltfläche "Anfragelösung ablehnen"	Ablehnen	Lösung ablehnen	"Schließung angefordert" zu "Offen"
Schaltfläche "Anfrage schließen"	Schließung anfordern	Schließung anfordern	■ Von "Offen" zu "Abgebrochen" ■ Wartet auf Antwort des Endbenutzers ■ Wartet auf Anbieter ■ Genehmigung in Bearbeitung ■ Bestätigt
Schaltfläche "Anfrage 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 Service Desk Manager-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 349)

[Verwenden einer Zeitzone](#) (siehe Seite 350)

[Festlegung der zu verwendenden Zeitzone](#) (siehe Seite 350)

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.

Verwenden einer Zeitzone

Eine Zeitzone, die mit dem Servicetyp verknüpft wird, kann die Uhrzeiten zum Auslösen von Ereignissen beschränken.

Beispiel: Ereignis-Auslöser nach Zeitzone

In diesem Beispiel beschränkt eine Zeitzone, die mit dem Servicetyp verknüpft ist, den tatsächlichen Zeitpunkt, zu dem ein Ereignis ausgelöst wird, wie folgt:

- Schicht von 8:00 bis 17:00 Uhr.
- Die Ereignisverzögerung beträgt 3 Stunden.
- Aktuelle Serverzeit 15:00 Uhr.
- Aktuelle Uhrzeit in Zeitzone ist 12:00 Uhr.

Das Ereignis 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 Ereignisverzögerung beträgt drei Stunden (00:00 Uhr bis 3:00 Uhr Uhrzeit der Zeitzone; 15:00 Uhr bis 18:00 Uhr Serverzeit).

Folglich fängt das Ereignis um 18:00 Uhr Serverzeit oder 15:00 Uhr Zeitzonezeit an.

Festlegung der zu verwendenden Zeitzone

Sie können eine Zeitzone für einen Server, für eine Lokation und für einen Servicetyp angeben. Sie können auch CA Service Desk Manager anweisen, die Zeitzone des betroffenen Endbenutzers eines Tickets zu benutzen. CA Service Desk Manager verwendet die folgenden Regeln, um zu bestimmen, welche Zeitzone ein Ereignis auslöst:

- **Zeitzone des betroffenen Endbenutzers** - CA Service Desk Manager verwendet diese Regel, wenn die folgenden Bedingungen gelten:
 - Die Option "Zeitzone des Endbenutzers verwenden" ist ausgewählt.
 - Für den betroffenen Endbenutzer des Tickets ist eine Zeitzone angegeben.

- **Zeitzone der betroffenen Endbenutzerlokation** - CA Service Desk Manager verwendet diese Regel, wenn die folgenden Bedingungen gelten:
 - Die Option "Zeitzone des Endbenutzers verwenden" ist ausgewählt.
 - Für den betroffenen Endbenutzer des Tickets ist keine Zeitzone angegeben.
 - Für die betroffene Endbenutzerlokation ist eine Zeitzone angegeben.
- **Servicetyp-Zeitzone** - CA Service Desk Manager verwendet diese Regel, wenn die folgenden Bedingungen gelten:
 - Für den Servicetyp ist eine Zeitzone angegeben.
 - Die Option "Zeitzone des Endbenutzers verwenden" ist nicht ausgewählt.
- **Serverzeitzone** - CA Service Desk Manager verwendet diese Regel, wenn die folgenden Bedingungen gelten:
 - Für den Server ist eine Zeitzone angegeben.
 - Die Option "Zeitzone des Endbenutzers verwenden" ist nicht ausgewählt.
 - Für den Server ist keine Zeitzone angegeben.
- **Kein Zeitzonensupport** - CA Service Desk Manager verwendet diese Regel, wenn die folgenden Bedingungen gelten:
 - Für den Server ist keine Zeitzone angegeben.
 - Die Option "Zeitzone des Endbenutzers verwenden" ist nicht ausgewählt.
 - Es gibt keine Server-Datensätze.

Dateianhänge

Manchmal soll eine Datei mit einem Ticket verknüpft werden, z. B. die folgenden Dateien:

- ein Screenshot eines bestimmten Fehlers
- Protokolldateien, die zu einem Problem geführt haben
- eine E-Mail, die ein Problem erläutert
- ein Weblink, der auf eine Webseite verweist, die repariert werden muss

Sie richten Ihren Service Desk ein, damit Benutzer mit Anhängen arbeiten können. Alle Arten von Tickets können Anhänge haben. Daher müssen Sie Anhänge für alle Service Desk-Modelle einrichten.

CA Service Desk Manager klassifiziert Anhänge folgendermaßen:

- **Gespeichert** - Gespeicherte Anhänge werden geladen und in einem Repository gespeichert. Wenn ein Analyst einen gespeicherten Anhang einsieht, wird die Datei über einen Webbrowser abgerufen und lokal angezeigt. Die gespeicherte Datei verbleibt im Repository.

Gespeicherte Anhänge können über einen Webserver mit dem HTTP-Protokoll in ein Repository geladen werden. Durch Verwendung eines Webserver zum Speichern von Dateien können Dateien über die Benutzerschnittstelle gespeichert und abgerufen werden. Auf Netzwerk-Repositorys kann von einem Webclient nicht effizient zugegriffen werden. Sie werden daher nicht unterstützt.
- **Verknüpft** - Speichert nur eine Verknüpfung zur Datei in der Datenbank.

Weitere Informationen:

[Hoch- und Herunterladen von Dateianhängen](#) (siehe Seite 352)
[Repositorys](#) (siehe Seite 353)

Hoch- und Herunterladen von Dateianhängen

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 Service Desk Manager Repository Daemon auf dem Computer ausgeführt werden.

Hinweis: Repositorys auf freigegebenen Laufwerken werden unter WIN2003 nicht unterstützt.

- 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.

Hinweis: Bisherige Clients funktionieren weiterhin auf dieselbe Weise und haben direkten Zugriff auf neue Uploads in vorhandene Repositorys.

Hinweis: Weitere Informationen zum Arbeiten mit Anhängen finden Sie in der *Online-Hilfe*.

Repositorys

Ein Repository stellt ein Festplattenverzeichnis auf einem lokalen oder einem Remote-Computer dar. Sie können ein großes Repository oder mehrere kleine haben. Wie Sie Repositorys unterteilen, hängt ausschließlich von Ihrer Geschäftspraxis und Ihren Bedürfnissen ab.

Die Verschiebung oder Kombination von Repositorys ist einfach, da alle Attribute zu einem Repository im Repository-Datensatz definiert sind. Nur das Repository und der Dateiname sind mit den einzelnen Tickets verbunden.

Dateien werden in ein Repository hochgeladen und verbleiben dort. Wird eine Datei angefragt, erfolgt eine der folgenden Aktionen:

- Ein Webbrowser (HTTP) ruft eine Version der Datei ab und zeigt sie dem Benutzer an.
- Die Anwendung, die mit der Dateierweiterung verknüpft ist, öffnet die Datei automatisch.

Beispiel: Ändern der Verzeichnisstruktur auf einem Webserver

In diesem Beispiel wird gezeigt, wie Sie die Verzeichnisstruktur auf einem Webserver ändern.

Ändern Sie den Upload-Pfad im Repository-Datensatz.

Alle vorhandenen Anhänge zeigen automatisch auf den neuen Speicherort.

Einrichten von Repositorys

Sie müssen die Repositorys einrichten, bevor CA Service Desk Manager-Benutzer mit Anhängen arbeiten können.

Die verteilte Architektur ermöglicht die benutzerdefinierte 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 Service Desk Manager-Server** — Wenn Sie einen Repository-Server auf einem geschützten CA Service Desk Manager-Server einrichten (typischerweise ein sekundärer Server hinter einer Firewall), müssen Sie das Servlet nicht auf diesem Computer bereitstellen. Sie können stattdessen die Ausführung des Servlets auf dem primären Server oder einem anderen uneingeschränkten CA Service Desk Manager-Server festlegen, wobei weiterhin ein erfolgreicher Upload oder Download zum Repository-Server möglich ist. Je nach Netzwerkverbindung sind zwischen den beiden CA Service Desk Manager-Servern gewisse Leistungseinbußen beim Upload oder Download möglich.

Hinweis: Eine gute Art der Einrichtung für ein Remote-Repository ist die Installation eines sekundären Servers mit dem Repository auf dem Remote-Server und die Einstellung des Upload-Pfades als lokaler Pfad.

- **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.

Systemanforderungen

Standardmäßig befinden sich die Repositorys auf dem primären Server, und zum Hochladen von Dateianhängen ist keine zusätzliche Konfiguration erforderlich. Wenn sich das Repository jedoch auf einem Remote-Computer befindet, muss ein sekundärer Server installiert und auf dem primären Server "rep_daemon" ausgeführt werden. Für den Server gelten folgende Systemanforderungen:

- sekundärer Server (für Remotesystem) mit aktivem Repository Daemon
- Tomcat und Upload-Servlet

So richten Sie ein Repository auf einem Remote-Computer ein:

1. Öffnen Sie eine Eingabeaufforderung, und geben Sie Folgendes ein:
`cd $NX_ROOT/samples/pdmconf`
2. Führen Sie "pdm_edit.pl" aus.
Ihnen werden zwei Fragen gestellt. Beantworten Sie die Fragen, um zum Hauptmenü zurückzukehren.
3. Wählen Sie "8" aus, und drücken Sie die EINGABETASTE, um "Repository Daemon" auszuwählen.

4. Geben Sie den Namen des sekundären Servers ein, und drücken Sie die EINGABETASTE.

Hinweis: Der Name des sekundären Servers muss mit NX_LOCAL_HOST auf dem sekundären Server übereinstimmen.

Das Hauptmenü wird angezeigt.

5. Wählen Sie "X" aus, und drücken Sie zum Speichern und Beenden die EINGABETASTE.

Die gespeicherte Datei ist die Datei "pdm_startup.rmt". Diese Datei ersetzt "\$NX_ROOT/pdmconf/pdm_startup.tpl".

6. Benennen Sie die aktuelle Datei "pdmconf/pdm_startup.tpl" um.

7. Kopieren Sie die neue Datei "pdm_startup.rmt" auf "pdmconf/pdm_startup.tpl".

8. Installieren Sie einen sekundären Server, und starten Sie den Proctor auf diesem.

Hinweis: Unter Windows NT ist der Proctor ein Dienst, und unter Linux lautet er "pdm_proctor_nxd".

9. Starten Sie den primären Server, und verwenden Sie "pdm_status", um zu sehen, ob der neue Daemon angezeigt wird.

10. Ändern Sie den Servernamen und den Upload-Pfad, damit diese auf das Remote-System verweisen, auf dem der Repository Daemon ausgeführt wird.

Der Remote-Computer ist nun so konfiguriert, dass er Dateianhänge laden kann.

Definieren von Repositories

Um Dateianhänge zu verwenden, definieren Sie mit der administrativen Funktion der Web-Schnittstelle von CA Service Desk Manager ein Repository:

So definieren Sie das Repository:

1. Wählen Sie im Menü "Administration" die Option "Anhänge" > "Repository", um die Seite "Repository-Liste" anzuzeigen.

2. Wählen Sie "Datei" > "Neu".

Die Seite "Repository - Detail" wird angezeigt.

3. Geben Sie Daten in den folgenden Feldern ein:

Symbol

Bezeichnet das Repository mit einem Namen, wie zum Beispiel "Nur große Dateien", "Permanente Dateien" oder Ähnliches.

Standard-Repository

Automatisch ausgewähltes Standard-Repository für alle Anhänge.
Benutzer können zu einem anderen Repository wechseln, sofern nötig.

Servername

Der Servername des Repositorys.

Klicken Sie auf "Speichern".

4. Klicken Sie auf "OK".

Die Detail- und die Listenseite werden geschlossen und die Hauptseite angezeigt.

Ankündigungen

Sie können CA Service Desk Manager verwenden, um Benutzern 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 Benutzer. Benutzer 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 Service Desk Manager. 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 357)

[Angaben der Ankündigungsdringlichkeit](#) (siehe Seite 357)

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.

Angaben 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 Service Desk Manager 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 Service Desk Manager 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 Abfragendefinitionen:

- 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 Service Desk Manager 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 die letzte geöffnete Anforderung 5 lautet, wird der nächsten Anforderung die Nummer 6 zugewiesen.

Wichtig! Nachdem Sie eine neue Version von CA Service Desk Manager 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 Anforderungen, Änderungsaufträge und Problemanfragen nummeriert werden, indem Sie ein eindeutiges Präfix oder Suffix in das Nummerierungsschema für diese Elemente einschließen. Wenn Sie zum Beispiel Anforderungen nach Monat verfolgen möchten, können Sie ein Monatskennzeichen als Präfix oder Suffix zum Nummerierungsschema für Anforderungen 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 Anfragen, 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 Anfragen, Changes und Incidents angeben. Bei diesem Setup können Benutzer problemlos zwischen den verschiedenen Tickettypen unterscheiden, so dass keine Verwirrung entsteht.

Für ITIL-konfigurierte Systeme haben Incidents und Problemen Nummerierungsschemas mit Anfragen gemeinsam, weil es sich bei Incidents und Problemen intern um verschiedene Arten von Anfragen handelt.

Verwenden des Audit-Protokolls

CA Service Desk Manager erstellt ein Audit-Protokoll, das die folgenden Informationen aufzeichnet:

- alle Changes an einem Issue
- alle Changes an einer Anfrage (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
- (ITIL-Konfiguration) 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 Service Desk Manager bereitzustellen.

Hinweis: Weitere Informationen zur CA NSM-Integration finden Sie im *Implementierungshandbuch*.

Kapitel 8: Steuerung des Systemverhaltens

Dieses Kapitel enthält folgende Themen:

[Verwendung des Optionsmanagers](#) (siehe Seite 363)

[Ändern der System-Umgebung](#) (siehe Seite 364)

[Ereignisse](#) (siehe Seite 365)

[Makros](#) (siehe Seite 365)

Verwendung des Optionsmanagers

Mit dem CA Service Desk Manager-Web-Client können Sie den Optionsmanager von der Administrations-Registerkarte aus verwenden, um folgende Aktionen durchzuführen:

- Einstellen von Optionen
- 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 Installieren oder Deinstallieren einiger Optionen den CA Service Desk Manager-Server aktualisieren, damit die Option wirksam wird. Wenn dies der Fall ist, gibt die Beschreibung in der *Online-Hilfe* diese Information für die betreffende Option an.

- Den Status aller Optionen auf Zusammenfassungsebene prüfen.
- Jede der verfügbaren Optionen deinstallieren.

Viele der Optionen sind vorkonfiguriert und werden bei der Installation von CA Service Desk Manager installiert. Bei Verwendung des Optionsmanagers zur Installation oder Deinstallation von Optionen können einige oder alle Standardeinstellungen verändert werden.

- Jede definierte Option installieren.

Hinweis: Während eines Release-Zyklus werden Optionen gelegentlich auf Benutzeranfrage vom CA Service Desk Manager-Support zur Verfügung gestellt. Um weitere Informationen zu diesen Optionen zu erhalten, wenden Sie sich an den CA Service Desk Manager-Support. Hinweis: Weitere Informationen zur Verwendung des Optionsmanagers finden Sie in der *Online-Hilfe*.

Ändern der System-Umgebung

CA Service Desk Manager 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 keinesfalls die Umgebungsdatei (NX.env) direkt, auch nicht auf Ihrem Client oder auf Sekundärserver-Installationen.

Um die Umgebungsdateivorlage zu ändern

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 die Vorlagendatei für Umgebungsvariablen auf dem primären Server. Sie können die Datei mit einem beliebigen Texteditor anzeigen und bearbeiten (Windows-Benutzer 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-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. Fahren Sie den primären Server von CA Service Desk Manager herunter und wieder hoch, damit die an der Umgebungsdatei vorgenommenen Änderungen wirksam werden. Um das komplette Herunterfahren Ihres Systems zu vermeiden, kann der Supporttechniker Sie anweisen, nur bestimmte Prozesse zu beenden und neu zu starten, anstatt den gesamten CA Service Desk Manager-Server zu aktualisieren.

Ereignisse

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 Service Desk Manager 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:

- Ereignisse
- Verhaltensvorlagen für Issues oder Changes
- Aktivitätsbenachrichtigungen

Das Produkt enthält mehrere Makros. Benutzer 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 Service Desk Manager 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.

Ereignis 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 Service Desk Manager-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 9: Konfiguration der Web-Schnittstelle

Dieses Kapitel enthält folgende Themen:

[Konfiguration der Web-Schnittstelle](#) (siehe Seite 371)
[Funktionsweise der Web-Schnittstelle](#) (siehe Seite 372)
[WebDirector und Verteilen der Webauslastung](#) (siehe Seite 372)
[Konfiguration von WebDirectors und Web-Engines](#) (siehe Seite 377)
[Verbessern der Leistung mit Browser-Caching](#) (siehe Seite 412)
[Verhalten für die Anzeige von Datensätzen in der Web-Schnittstelle](#) (siehe Seite 415)
[Drucken von CA Service Desk Manager-Webseiten](#) (siehe Seite 416)
[Änderung der Konfigurationsdatei](#) (siehe Seite 416)

Konfiguration der Web-Schnittstelle

Die *Web-Schnittstelle* bietet CA Service Desk Manager-Funktionen über das World Wide Web. Die Web-Schnittstelle ermöglicht das unabhängige Durchsuchen der Knowledge Base, verringert die Anzahl der Anrufe beim Service Desk und verkürzt die Lösungszeiten. Die Schnittstelle ermöglicht ferner Folgendes:

- Öffnen, Verarbeiten und Schließen von Tickets
- Anzeigen und Bereitstellen von Ankündigungen
- Zugreifen auf ergänzende Daten

Wenn Sie CA Service Desk Manager entsprechend den Anweisungen im *Implementierungshandbuch* installiert und konfiguriert haben, können Sie die CA Service Desk Manager-Nutzung verwalten und sichern und gemäß Ihren Anforderungen konfigurieren. Sie konfigurieren die Web-Schnittstellen-Sicherheit durch die Verwendung von Rollen und Zugriffstypen. Sie können die Schnittstelle für die Verwendung mit Webbrowsern konzipieren.

Funktionsweise der Web-Schnittstelle

Die Web-Schnittstelle von CA Service Desk Manager verwendet einen HTTP-Standardserver, wie zum Beispiel Tomcat, Apache oder Microsoft Internet Information Server (IIS).

- Mit dem Tomcat-Server werden Web-Anfragen von einem Java-Servlet, "pdmweb.jar", bearbeitet.
- Mit einem Apache- oder IIS-Server werden Web-Anfragen von einer CGI-Schnittstelle, "pdmweb.exe", bearbeitet.

Die CA Service Desk Manager-Web-Schnittstelle arbeitet folgendermaßen:

1. Wenn ein Benutzer eine CA Service Desk Manager-Webseite anfordert, ruft der HTTP-Server "pdmweb.jar" oder "pdmweb.exe" auf. Diese Dateien stellen eine Verbindung zu einem CA Service Desk Manager-Daemon (oder Windows-Dienst) her, der als Web-Engine bezeichnet wird.
2. Die Web-Engine interpretiert die Anfrage des Benutzers. Bei den meisten Anforderungen muss die Web-Engine in einer HTML-Vorlagendatei (HTMPL) nachsehen und die Anforderung in Standard-HTML übersetzen.
3. Für die Übertragung ist es normalerweise erforderlich, dass das Webmodul mit einem CA Service Desk Manager-Server kommuniziert, um die Datenbank zu lesen oder zu aktualisieren und die Datenbankinformationen in den generierten HTML-Code einzuschließen.
4. Nachdem der HTML-Code vollständig ist, sendet die Web-Engine diesen an "pdmweb.jar" oder "pdmweb.exe", die ihn wiederum an den Browser des Benutzers zurücksenden.
5. Nachdem die Daten an den Browser zurückgesendet wurden, wird "pdmweb.exe" beendet, während "pdmweb.jar" aktiv bleibt.

WebDirector und Verteilen der Webauslastung

Bei zunehmender Nutzung des Internets an Ihrem Standort ist es möglicherweise ratsam, die Last auf mehrere Web-Engines und/oder mehrere HTTP-Server zu verteilen. Auf diese Weise können Sie die Kapazität des Webserver entsprechend dem von Ihrer Organisation geforderten Nutzungsgrad erhöhen. Sie können das von CA Service Desk Manager bereitgestellte Tool WebDirector verwenden, um die Weblast zu verteilen. WebDirector empfängt Verbindungsanfragen von Benutzern, wählt eine Web-Engine zur Bearbeitung der Anfrage und leitet die Anfrage an diese Web-Engine um. Außer der Änderung der URL ist dieses Verfahren für den Endbenutzer transparent: Er greift immer mit derselben URL auf CA Service Desk Manager zu, unabhängig von der Anzahl der konfigurierten Web-Engines.

Sie können WebDirector wie folgt verwenden:

- Konfigurieren von CA Service Desk Manager 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 Benutzers kann WebDirector die Sitzung an eine andere Web-Engine auf dem gleichen oder auf einem anderen HTTP-Server verschieben. Somit können Sie SSL für eine Anmelde-Web-Engine konfigurieren. Dies bietet maximalen Schutz für Ihre Kennwörter, während das HTTP-Standardprotokoll für andere Transaktionen verwendet wird, um deren Leistung zu maximieren.

- 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 Endbenutzern liegen sollen.

Web.cfg und CA Service Desk Manager

Bei der Konfiguration von Web-Engines für CA Service Desk Manager können Sie das mitgelieferte Skript `pdm_edit.pl` zur Unterstützung verwenden. Ohne Skript muss ein Benutzer, der eine Web-Engine hinzufügt, manuell den Namen angeben und eine eindeutige Instanz der Datei `"web.cfg"` erstellen. Das Skript führt diese Aufgaben automatisch aus.

Wenn Sie das Skript `"pdm_edit.pl"` zur Konfiguration einer Web-Engine verwenden, erstellt das Skript automatisch ein Skript und benennt es. Der Name wird folgendermaßen gebildet:

```
"<Host_Name>-web[#].cfg"
```

Hostname

Legt den Server als Primärserver fest, wenn sich die Web-Engine auf einem Primärserver befindet, oder gibt den eigentlichen Serverhostnamen an, wenn sich die Web-Engine auf einem Sekundärserver befindet.

[#]

Legt eine Ganzzahl fest, die automatisch von `"pdm_edit.pl"` zugewiesen und für jede Web-Engine auf einem Server erhöht wird.

Als Konfigurationsdatei der Standard-Web-Engine liefert die CA Service Desk Manager-Installation eine Standardkonfigurationsdatei für die Web-Engine:

```
$NX_ROOT/bopcfg/www/web.cfg
```

Nachdem die Standard-Web-Engine durch "pdm_edit.pl" geändert wurde, folgt die generierte Web-Engine-Konfigurationsdatei diesem neuen Benennungsschema:

```
<Host_Name>-web[#].cfg
```

Danach wird die ursprüngliche Datei "web.cfg" sowie etwaige Anpassungen dieser ignoriert. Wenn Benutzer Anpassungen der ursprünglichen "web.cfg" bewahren möchten, müssen sie sicherstellen, dass "\$NX_ROOT/bopcfg/www/web.cfg" als zu verwendende Vorlagendatei gewählt wird, wenn "pdm_edit.pl" die Dateien "<Host_Name>-Web[#].cfg" generiert.

Zuweisen einer Web-Engine zu einem WebDirector

Eine Web-Engine wird einem WebDirector durch die WebDirector-Parameter in der folgenden Web-Engine-Datei zugewiesen:

```
'<Host_Name>-web[#].cfg'
```

Während jede Web-Engine ihre eigene Datei "<Host_Name>-Web[#].cfg" erfordert, verwenden WebDirectors keine Webkonfigurationsdatei. Diese Web-Engine/WebDirector-Zuordnung erfolgt ursprünglich durch das folgende Hilfsprogrammskript:

```
'pdm_edit.pl'
```

Um das Verhalten der Web-Engine bei der Umleitung zu ändern, müssen Sie gegebenenfalls zusätzliche Änderungen für die WebDirector-Parameter in der Datei "<Host_Name>-web[#].cfg" der Web-Engine durchführen. Wenn eine Web-Engine keinem WebDirector zugewiesen ist (Standardwert), ist der Parameter "UseDirector" in der Konfigurationsdatei der Web-Engine auf "No" eingestellt. CA Service Desk Manager ignoriert dann die restlichen WebDirector-Parameter für die Web-Engine.

Nachdem eine Web-Engine einem WebDirector zugewiesen wurde, definieren die folgenden Parameter, wie die Web-Engine mit dem zugewiesenen WebDirector interagiert:

- UseDirector Yes | No | AfterLogin | BeforeLogin
- WebdirectorSlumpName (der Slump-Name wird automatisch zugewiesen)
- WillingnessValue Bereich von 0 bis 10
- RedirectingURL [http/https]://<machineName>/<cgi directory>/<cgi name>

Definieren der Web-Engine-Rolle durch WebDirector-Parameter

Nachdem eine Web-Engine für die Verwendung eines WebDirectors konfiguriert wurde, nimmt die Web-Engine eine bestimmte Rolle an. Diese Rolle definiert, welche Webclient-Anforderungen die Web-Engine behandelt. Folgende Rollen sind möglich:

- nur Anmeldungen bedienen (Nicht-Anmeldeanforderungen woandershin umleiten)
- nur Nicht-Anmeldeanforderungen bedienen (Anmeldungen woandershin umleiten)
- Anmeldeanforderungen sowie Nicht-Anmeldeanforderungen bedienen (universelle Web-Engine)

Die betreffende Rolle wird von den WebDirector-Parameterwerten in der Datei "<Host_Name>-Web[#].cfg</cs>" der Web-Engine bestimmt. Die folgende Tabelle illustriert die Beziehung von Web-Engine-Rolle und WebDirector-Parametereinstellung:

Web-Engine-Rolle	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]

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. Das HTTP-Protokoll ist für die Kommunikation zwischen dem Web-Client und dem Webserver zuständig.

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. Jede Web-Anmeldungsanfrage wird an die SSL-Web-Engines umgeleitet und von diesen bedient. Alle anderen Anfragen 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.

Konfiguration von WebDirectors und Web-Engines

Machen Sie sich mit den folgenden Informationen zum Hinzufügen und Konfigurieren von WebDirectors und Web-Engines auf der Basis von Server- und Komponententypen vertraut:

SSL

Gibt das SSL-Protokoll an.

pdm_edit.pl

Gibt das CA Service Desk Manager-Perl-Skript an, das zum Hinzufügen und Ändern von Web-Engines, WebDirectors, Objektmanagern und anderen Komponenten verwendet wird.

CGI I/F

Gibt den von "pdm_edit.pl" zugewiesenen Skriptnamen für Web-Engines und WebDirectors 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", (WebDirectors) "pdmweb_d1" und "pdmweb_d2"

Systeme, die Servlet-Server wie Tomcat verwenden, benötigen keine ausführbaren CGI/IF-Dateien. Die CGI/IF-Datei wird von einem Servlet simuliert, das auf dem Servlet-Server ausgeführt wird. Diese Systeme erfordern stattdessen die Datei "web.xml" im Verzeichnis "\$NX_ROOT/bopcfg/CATALINA_BASE/webapps/CAisd/WEB-INF".

"pdm_edit.pl" erstellt "web.xml"-Beispieldateien, die "<hostname>-web.xml.tpl" genannt werden. Sie kopieren diese Dateien auf den geeigneten Server im Verzeichnis "WEB-INF", damit sie die Datei "web.xml.tpl" auf jedem Server ersetzen, und rekonfigurieren dann den sekundären Server.

SSL-Anmeldung

Gibt die CA Service Desk Manager-Konfiguration an, in der sich eine oder mehrere Web-Engines in einem virtuellen Verzeichnis mit SSL-Erzwingung befinden. Alle Anmeldeanfragen von Web-Clients erfolgen ausschließlich über verschlüsselte HTTP-Kommunikation. Nach der Benutzerauthentifizierung leitet ein WebDirector den Webclient für den Rest der Clientsitzung an eine zulässige Web-Engine in einem virtuellen Verzeichnis ohne SSL-Erzwingung um, und es wird eine unverschlüsselte HTTP-Kommunikation verwendet.

Web-Engine für sichere Anmeldung

Gibt die Web-Engine in der SSL-Anmeldeumgebung an, die ausschließlich die Anfragen zur Benutzerauthentifizierung von CA Service Desk Manager-Web-Clients abwickelt.

Nicht sichere Web-Engine

Gibt die Web-Engine in der SSL-Anmeldeumgebung an, die alle Anfragen von Webclients abwickelt, bei denen es nicht um die Benutzerauthentifizierung geht, nachdem die Benutzerauthentifizierung über die Web-Engine für sichere Anmeldung erfolgt ist.

Web-Engine-Rolle

Gibt die Pflichten einer Web-Engine an, die diese übernimmt, nachdem sie einem WebDirector zugewiesen wurde. Diese Rollen umfassen:

- Nur Anmeldeanforderungen von Web-Clients verarbeiten.
- Alle Anforderungen mit Ausnahme von Anmeldeanforderungen von Web-Clients verarbeiten.
- Alle Web-Client-Anforderungen verarbeiten.

Implementieren einer SSL-Anmeldeumgebung mit nur einem primären Server

Sie können eine SSL-Anmeldeumgebung implementieren, die nur einen primären Server verwendet.

Hinweis: Der primäre Server muss installiert und konfiguriert werden, damit das System erstellt werden kann.

Um eine SSL-Anmeldeumgebung zu implementieren, gehen Sie wie folgt vor:

1. Überprüfen Sie, dass der SSL-aktivierte Webserver erfolgreich ein SSL-Zertifikat importiert hat.
2. 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

3. Fügen Sie ein neues virtuelles Verzeichnis für den Webserver mit der Bezeichnung *CAisdsec* hinzu. Dieses virtuelle Verzeichnis soll auf das folgende physische Verzeichnis zeigen:

\$NX_ROOT/bopcfg/www/wwwrootsec

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 benutzerdefiniert und kann umbenannt werden.

4. Erstellen eines Systems mit nur einem primären Server

Erstellen eines Systems, das nur einen primären Server umfasst

Sie können ein System erstellen, das nur einen primären Server verwendet.

Hinweis: Der primäre Server muss installiert und konfiguriert werden, damit das System erstellt werden kann.

Gehen Sie wie folgt vor, um ein System mit nur einem primären Server zu erstellen:

1. Fügen Sie mit "pdm_edit.pl" WebDirector-Einträge hinzu, und/oder bearbeiten Sie diese nach Belieben. Ein WebDirector kann die Last unter mehreren Web-Engines aufteilen. Weisen Sie allen neuen Web-Engines und WebDirectors dem Host "primär" zu. Dies ist der primäre Server.

Hinweis: Die automatische Zuweisung des WebDirectors CGI I/F weist Namen aus der Datei "pdm_edit.pl" zu:

- Dem ersten WebDirector auf dem Primärserver wird automatisch der Name "pdmweb_d1.exe" zugewiesen.
- Der zweite WebDirector auf dem primären Server erhält den Namen "pdmweb_d2.exe",
- der dritte "pdmweb_d3.exe" und so weiter.

Ein sekundärer Server könnte auch WebDirectors mit CGI I/F-Werten aus "pdmweb_d1.exe", "pdmweb_d2.exe" und "pdmweb_d3.exe" haben. Namenskonflikte treten nicht auf, da der WebDirector eindeutige Namen für den lokalen Computer vergibt, auf dem die WebDirectors ausgeführt werden.

2. Lesen Sie die folgenden Informationen, die je nach CA Service Desk Manager-Web-Engine-Umgebung gelten können:
 - Anzahl der hinzuzufügenden Web-Engines - Beim Implementieren eines beliebigen Lastenausgleichschemas, einer beliebigen SSL-Anmeldung oder beiden für die Web-Engine, müssen demselben WebDirector mindestens zwei Web-Engines zugewiesen werden.
 - SSL-Login-Umgebung - Beim Definieren der Web-Engine für sicheren Anmeldung in "pdm_edit.pl" muss diese Web-Engine von einem WebDirector gesteuert werden. Stellen Sie den Protokollparameterwert der Web-Engine für sichere Anmeldung auf "https" ein, um sicherzustellen, dass der WebDirector den korrekten Wert für "RedirectingURL" für den Webclient generiert.
3. Speichern Sie die Änderungen, und beenden Sie das Skript "pdm_edit.pl". Geben Sie die Datei an, die als web.cfg-Vorlage verwendet werden soll, wenn Sie dazu aufgefordert werden.

Hinweis: WebDirectors verwenden nicht die Datei "<Host_Name>-web[#].cfg". Web-Engines erfordern jedoch die eindeutige Datei "<Host_Name>-Web[#].cfg". Beim Speichern und Beenden des Skripts werden mit Hilfe des Skripts "pdm_edit.pl" automatisch "web.cfg"-Beispieldateien generiert. Der Benutzer wird aufgefordert, eine Datei vom Typ "web.cfg" anzugeben, die bei der Erstellung neuer Webkonfigurationsdateien als Vorlage dient. Die Anpassungen in der ursprünglichen Datei web.cfg können auf die neuen Webkonfigurationsdateien übertragen werden, indem Sie die ursprüngliche Datei web.dfg als die gewünschte Vorlagendatei angeben.

4. Kopieren und Speichern Sie die folgenden Dateien. Eine Sicherung von diesen Dateien ist nützlich, wenn Sie sich für die Wiederherstellung der ursprünglichen Umgebung entscheiden:
 - `$NX_ROOT/pdmconf/pdm_startup.tpl`
 - `$NX_ROOT/pdmconf/pdm_startup`
 - `$NX_ROOT/bopcfg/www/web.cfg` file
 - jede vorhandene Datei `"primary-web[#].cfg"`
 - `$NX_ROOT/bopcfg/www/CATALINA_BASE/webapps/CAisd/WEB-INF/web.xml` und `web.xml.tpl`
5. Verschieben Sie `"$NX_ROOT/samples/pdmconf/pdm_startup.rmt"` nach `"$NX_ROOT/pdmconf"`, und benennen Sie sie in `"pdm_startup.tpl"` um.
6. Stellen Sie für jede Web-Engine, die einem Webdirector zugewiesen wurde, sicher, dass die Webdirector-Parameter für die Datei `<Host_Name>-web[#].cfg` der Web-Engine richtig festgelegt wurden. Überprüfen Sie hierfür die Datei in einem Text-Editor. Ändern Sie bei Bedarf die Parameterwerte des WebDirectors, um die Web-Engine-Rolle zu reflektieren. Kopieren Sie sie dann in das Verzeichnis `"$NX_ROOT/bopcfg/www"`.
7. Verschieben Sie alle Dateien `"$NX_ROOT/samples/pdmconf/primary-web[#].cfg"` in das Verzeichnis `"$NX_ROOT/bopcfg/www"`.
8. Wenn Sie einen Servlet-Server wie Tomcat verwenden, werden vom Dienstprogramm `"pdm_edit.pl"` die Dateien vom Typ `"web.xml.tpl"` erstellt. Diese können verwendet werden, um die Datei `"web.xml.tpl"` auf jedem Server, der eine Web-Engine hostet, zu ersetzen. Diese Dateien haben den Namen `"primary-web.xml.tpl"`. Benennen Sie die Dateien um und kopieren Sie sie in das Verzeichnis `"$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 `"$NX_ROOT/bopcfg/www/wwwroot"`, eine Datei vom Typ `"pdmweb[#].exe"` für jede Web-Engine sowie eine Datei vom Typ `"pdmweb_d[#].exe"` für jeden in `"pdm_edit.pl"` definierten WebDirector. Stellen Sie sicher, dass `"pdmweb[#].exe"` und `"pdmweb_d[#].exe"` gemäß den korrekten CGI I/F-Werten aus den Definitionen des Skripts `"pdm_edit.pl"` benannt wurden (zum Beispiel `"pdmweb1.exe"`, `"pdmweb2.exe"`, `"pdmweb_d1.exe"` usw.)
9. Wenn Sie IIS verwenden und für jede CGI-Schnittstelle Servererweiterungen hinzufügen möchten, können Sie die Datei `"primary-site.dat"` als `"site.dat"` in das Verzeichnis `"$NX_ROOT/bopcfg/www"` kopieren. Bei der erneuten Konfiguration des Systems werden diese Sites IIS hinzugefügt.

10. Konfigurieren Sie den Primärserver ohne die Datenbank erneut zu initialisieren, und starten Sie die Dienste.
11. Überprüfen Sie die aktuellen Einstellungen nach dem Neukonfigurieren auf Gültigkeit. Starten Sie die CA Service Desk Manager-Daemons. Prüfen Sie, ob keine Fehler in den STDLog-Dateien vorhanden sind. Zeigen Sie mit "pdm_status</cs>" die Daemons und ihren Status an. Sie können von einem Browser auf das System zugreifen: "http://localhost:8080/CAisd/pdmweb.exe".
12. Für die Integration von Knowledge-Management in CA Service Desk Manager muss der URL-Protokollwert von CA Service Desk Manager geändert werden, wenn SSL für CA Service Desk Manager erzwungen wurde.
 - a. Ändern Sie im Knowledge Tools-Einstellungsmanager unter "Allgemein" > "Integration" den CA Service Desk Manager-URL-Protokollwert von "http" in "https".
 - b. Klicken Sie auf „Speichern“ und anschließend auf „Beenden“.
13. Öffnen Sie die CA Service Desk Manager-Anmeldeseite in einem Web-Browser, und überprüfen Sie, ob sich ein Benutzer anmelden kann und ob das erwartete Umleitungs-/Anmeldeverhalten eingehalten wird.

Prüfen der WebDirector-Parameterwerte

Sie können WebDirector-Parameterwerte überprüfen.

So prüfen Sie die WebDirector-Parameterwerte:

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" in "AfterLogin".
 - 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 abwickeln, jeweils die Datei "<Host_Name>-web[#].cfg" für die nicht sicheren Web-Engines, die Nicht-Anmeldeaktivitäten abwickeln sollen. Überprüfen Sie, ob der "CAisd"-Parameterwert "/CAisd" ist.
 - a. Ändern Sie den "UseDirector"-Parameterwert von "Yes" in "BeforeLogin".
 - b. 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.
 - c. Stellen Sie sicher, dass als Protokoll für den Parameter "RedirectingURL" der Wert "http" eingestellt ist.
 - d. Stellen Sie sicher, dass der "RedirectingURL <cgi directory>"-Wert "CAisd" lautet.
 - e. Speichern Sie die Änderungen.

Die WebDirector-Parameterwerte werden überprüft.

Prüfen der SSL-Anmeldeumgebung

Sie können die SSL-Anmeldeumgebung für Web-Engines folgendermaßen überprüfen:

- 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 in "pdm_edit.pl" definierte Web-Engine für sichere Anmeldung entsprechen.

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

- Die nicht sicheren Web-Engines und die WebDirectors 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". Für jede nicht sichere Web-Engine und für jeden nicht sicheren WebDirector, die in "pdm_edit.pl" definiert sind, muss eine Kopie von "pdmweb.exe" vorliegen. 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 WebDirectors in "pdm_edit.pl" definiert wurden.

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

Sekundäre Server und Webfunktionen

Alle Systeme verfügen über einen primären Server. Dieser Server hostet die grundlegenden Systemdienste, wie den Kommunikations-Hub und die Datenbank. Viele Benutzer im Unternehmen verbreiten das System auf andere Server, die als sekundäre Server bezeichnet werden. In diesem Fall können Sie den sekundären Servern Webfunktionen hinzufügen.

So bereiten Sie Webfunktionen vor:

Um sekundären Servern Webfunktionen hinzuzufügen (wenn Sie eine SSL-Anmeldeumgebung implementieren), müssen folgende vorbereitende Aufgaben durchgeführt werden:

1. Überprüfen Sie, dass der primäre und die sekundären Server installiert und konfiguriert sind.
2. Überprüfen Sie, dass der SSL-aktivierte Webserver, der die Web-Engine für sichere Anmeldung hosten soll, ein SSL-Zertifikat importiert hat.
3. Erstellen Sie auf dem Webserver, der die Web-Engine für sichere Anmeldung hostet, eine physische Kopie (einschließlich Unterverzeichnissen) des Verzeichnisses "\$NX_ROOT/bopcfg/www/wwwroot", und nennen Sie es "\$NX_ROOT/bopcfg/www/wwwrootsec".
4. Definieren Sie ein neues virtuelles Verzeichnis für den Webserver mit der Bezeichnung "CAisdsec".
5. Dieses virtuelle Verzeichnis soll auf das physische Verzeichnis "\$NX_ROOT/bopcfg/www/wwwrootsec" zeigen.
6. Stellen Sie sicher, dass die virtuellen Verzeichnisberechtigungen für "CAisdsec" den virtuellen Verzeichnisberechtigungen von "CAisd" zur Skriptausführung entsprechen.
7. Erzwingen Sie SSL für das virtuelle Verzeichnis "CAisdsec".

Hinweis: Der Name "CAisdsec" ist benutzerdefiniert, und Sie können ihn ändern.

Erstellen eines Systems mit sekundären Servern

Gehen Sie wie folgt vor, um ein System mit sekundären Servern zu erstellen:

1. Verwenden Sie "pdm_edit.pl", um WebDirector-Einträge wie gewünscht hinzuzufügen oder zu bearbeiten. Ein Webdirector kann die Last unter mehreren Web-Engines aufteilen. Fügen Sie anderen Servern Web-Engines und WebDirectors hinzu. Verwenden Sie beim Angeben eines sekundären Servers denselben Namen, mit dem dieser Server konfiguriert wurde. Dies ist der Wert von "NX_LOCAL_HOST" in der Datei "NX.env" auf dem sekundären Server.

Hinweis: Die automatische Zuweisung des CGI I/F des WebDirectors weist Namen aus der Datei "pdm_edit.pl" zu: Dem ersten WebDirector auf dem Primärserver wird automatisch der Name "pdmweb_d1.exe" zugewiesen. Der zweite WebDirector auf dem primären Server wird "pdmweb_d2.exe" genannt, der dritte "pdmweb_d3.exe" und so weiter. Ein sekundärer Server kann auch WebDirectors haben, deren CGI I/F-Werte "pdmweb_d1.exe", "pdmweb_d2.exe" und "pdmweb_d3.exe" lauten. Namenskonflikte treten nicht auf, da der WebDirector eindeutige Namen für den lokalen Computer vergibt, auf dem die WebDirectors ausgeführt werden.

2. Jede Web-Engine muss auf einen Objektmanager verweisen. Es gibt immer einen Objektmanager namens "domsrvr". Sie können weitere Objektmanager auf dem sekundären Server hinzufügen und diesen dann wie folgt Web-Engines zuweisen:
 - Anzahl der hinzuzufügenden Web-Engines - Beim Implementieren eines beliebigen Lastenausgleichschemas, einer beliebigen SSL-Anmeldung oder beiden für die Web-Engine, müssen demselben WebDirector mindestens zwei Web-Engines zugewiesen werden.
 - SSL-Login-Umgebung - Beim Definieren der Web-Engine für sicheren Anmeldung in "pdm_edit.pl" muss diese Web-Engine von einem WebDirector gesteuert werden. Stellen Sie den Protokollparameter der Web-Engine für sichere Anmeldung auf den Wert "https" ein. Diese Einstellung sorgt dafür, dass der WebDirector den richtigen URL-Umleitungswert für den Web-Client erstellt.

3. Speichern Sie die Änderungen, und beenden Sie das Skript "pdm_edit.pl". Geben Sie die Datei an, die als "web.cfg"-Vorlage verwendet werden soll, wenn Sie dazu aufgefordert werden.

Hinweis: WebDirectors verwenden die Datei "<Host_Name>-web[#].cfg" nicht. Web-Engines erfordern jedoch eine eindeutige Datei vom Typ "<Host_Name>-web[#].cfg". Beim Speichern und Beenden des Skripts werden mit Hilfe des Skripts "pdm_edit.pl" automatisch "web.cfg"-Beispieldateien generiert. Sie werden aufgefordert, die Datei "web.cfg" anzugeben, die bei der Erstellung neuer Webkonfigurationsdateien als Vorlage dient. 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.

4. Speichern Sie auf dem primären Server die folgenden Sicherungskopien. Sie sind nützlich, wenn die ursprüngliche Umgebung wiederhergestellt werden soll:

```
$NX_ROOT/pdmconf/pdm_startup.tpl  
$NX_ROOT/pdmconf/pdm_startup  
$NX_ROOT/bopcfg/www/*web*.cfg  
$NX_ROOT/bopcfg/www/CATALINA_BASE/webapps/CAisd/WEB-INF/web.xml*
```

5. Speichern Sie auf dem sekundären Server Sicherungskopien von allen vorhandenen Dateien vom Typ "\$NX_ROOT/bopcfg/www/web.cfg" oder "<secondary_name>-web[#].cfg".

```
$NX_ROOT/bopcfg/www/CATALINA_BASE/webapps/CAisd/WEB-INF/web.xml*
```

6. Verschieben Sie auf dem primären Server die Datei "\$NX_ROOT/samples/pdmconf/pdm_startup.rmt" nach "\$NX_ROOT/pdmconf", und benennen Sie sie in "pdm_startup.tpl" um.
7. Überprüfen Sie für jede Web-Engine, die einem WebDirector zugewiesen ist, ob die WebDirector-Parameter "< Host_Namen >-web[#].cfg" der Web-Engine richtig festgelegt wurden. Untersuchen Sie die Datei dazu in einem Texteditor. Ändern Sie falls notwendig die WebDirector-Parameterwerte, um die gewünschte Web-Engine-Rolle anzugeben.
8. Verschieben Sie auf dem primären Server alle Dateien "\$NX_ROOT/samples/pdmconf/primary-web[#].cfg" in das Verzeichnis "\$NX_ROOT/bopcfg/www".
9. Verschieben Sie alle Dateien vom Typ "\$NX_ROOT/samples/pdmconf/secondary_server_name-web[#].cfg" vom primären Server in das Verzeichnis "\$NX_ROOT/bopcfg/www" auf dem sekundären Server.

10. (Servlet-Server wie Tomcat) Geben Sie in jedem Verzeichnis "\$NX_ROOT/bopcfg/www/CATALINA_BASE/webapps/CAisd/WEB-INF" eine Datei vom Typ "web.xml.tpl" an. Wenn Sie diesen Server konfigurieren, erstellt der Konfigurationsprozess eine Datei vom Typ "web.xml". Das Dienstprogramm "pdm_edit.pl" hat "web.xml.tpl"-Beispieldateien erstellt. Diese haben jeweils den Namen "<hostname>-web.xml.tpl". Sie können diese Dateien als Beispieldateien verwenden: Kopieren Sie sie für jeden Ihrer Server, und benennen Sie sie in "web.xml.tpl" um.
11. (HTTP-Server wie IIS oder Apache) Erstellen Sie auf jedem CA Service Desk Manager-Server (primär, sekundär oder beiden), der eine Web-Engine oder einen WebDirector hosten soll, Kopien der Datei "pdmweb.exe" im Verzeichnis "\$NX_ROOT/bopcfg/www/wwwroot". Für jede Web-Engine ist eine "pdmweb [#].exe" und für jeden WebDirector eine "pdmweb_d[#].exe" in "pdm_edit.pl" definiert, die auf diesem Server ausgeführt werden soll. Überprüfen Sie, dass "pdmweb[#].exe" und "pdmweb_d[#].exe" mit den CGI I/F-Werten der Skriptdefinitionen in "pdm_edit.pl" 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, kopieren Sie die Datei "primary-site.dat" als "site.dat" in das Verzeichnis "\$NX_ROOT/bopcfg/www". 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 Services.
14. Konfigurieren Sie jeden sekundären Server erneut.
15. Für die Integration von Knowledge-Management in CA Service Desk Manager muss der URL-Protokollwert von CA Service Desk Manager geändert werden, wenn SSL für CA Service Desk Manager erzwungen wurde.
 - a. Ändern Sie im Knowledge-Management-Einstellungsmanager unter "Allgemein Integration" den CA Service Desk Manager-URL-Protokollwert von "http" in "https".
 - b. Klicken Sie auf „Speichern“ und anschließend auf „Beenden“.
16. Öffnen Sie die CA Service Desk Manager-Anmeldeseite in einem Web-Browser, und überprüfen Sie, ob sich ein Benutzer anmelden kann und ob das erwartete Umleitungs- oder Anmeldeverhalten eingehalten wird.

Serverkonfiguration

Mit "pdm_edit.pl" können Sie Funktionen hinzufügen und die Leistung des Unternehmenssystems steigern. Sie können die CA Service Desk Manager-Services konfigurieren. CA Service Desk Manager verfügt auf dem primären Server über grundlegende Daemons. Sie können auf diesem Primärserver weitere Daemons hinzufügen und Ihr System serverübergreifend erweitern, indem Sie weitere Sekundärserver hinzufügen, die Kapazität, Leistung und Sicherheit verbessern.

Wenn Sie die Daemon-Konfiguration mit "pdm_edit.pl" ändern, werden die mit "pdm_configure" verfügbaren Anpassungen deaktiviert. Wenn Sie zum Beispiel die Datei "pdm_startup.tpl" mit "pdm_edit.pl" geändert haben, können Sie einen WebDirector oder einen Event Converter nicht über die grafische Benutzeroberfläche von "pdm_configure" aktivieren. Sie können diese Funktionen mit dem Dienstprogramm "pdm_edit.pl" anpassen.

Das Hauptmenü von "pdm_edit.pl" wird angezeigt, nachdem Sie "pdm_edit.pl" ausführen und betriebssystemspezifische Fragen eingeben. Dieses Menü listet die Funktionen des Dienstprogramms auf. Durch Eingeben eines Wertes aus diesem Menü gelangen Sie zu den Untermenüs für die ausgewählte Funktion. Von den Untermenüs können Sie wieder zum Hauptmenü zurückkehren. Am Ende der Sitzung können Sie das Programm entweder beenden, ohne zu speichern (Quit NO SAVE), oder Sie können speichern und das Programm anschließend beenden (Save and quit). Dadurch wird die Datei "pdm_startup.dat" erstellt, in der alle Auswahldaten zusammengefasst werden. Behalten Sie diese Datei bei, um später darauf zurückzukommen. Das Dienstprogramm erstellt die Datei "pdm_startup.rmt", die als Ersatz für die Datei "\$NX_Root/pdmconf/pdm_startup.tpl" auf dem primären Server dient. Nach der Installation der Datei "pdm_startup.rmt" als "pdm_startup.tpl" auf dem primären Server konfigurieren Sie diesen erneut, ohne die Datenbank erneut zu initialisieren, um die Änderungen zu aktivieren.

Hinweis: Bei den Hostnamen aller Sekundärserver muss die Groß-/Kleinschreibung beachtet werden. Sie entsprechen dem Wert von "NX_LOCAL_HOST" in der Datei "NX.env" auf dem Sekundärserver.

Ausführen von "pdm_edit.pl" auf einem UNIX-Server

Sie können "pdm_edit.pl" auf einem UNIX-Server ausführen. Hierzu ist eine primäre Serverinstallation erforderlich sowie optional die Installation eines sekundären Servers, der für alle relevanten CA Service Desk Manager-Dokumente konfiguriert ist.

Hinweis: Führen Sie "pdm_edit.pl" nur auf dem primären Server aus. Weitere Informationen zu sekundären Servern, auf denen die Web-Schnittstelle ausgeführt wird, finden Sie im *Implementierungshandbuch*.

So führen Sie "pdm_edit.pl" auf einem UNIX-Server aus:

1. Wechseln Sie über die Befehlszeile auf dem primären Server zum folgenden Speicherort:

```
$NX_ROOT/samples/pdmconf
```

2. Setzen Sie den folgenden Befehl ab:

```
$NX_ROOT/bin/pdm_perl pdm_edit.pl
```

Die ausführbare CA Service Desk Manager-Datei "pdm_perl" führt das Skript "pdm_edit.pl" aus. Eine Reihe textbasierter Menüoptionen und Eingabeaufforderungen werden angezeigt, mit denen Sie Objektmanager, WebDirectors und Web-Engines hinzufügen, ändern oder löschen können. Speichern Sie anschließend die Änderungen oder Zusätze in den Dateien "pdm_startup.dat" und "pdm_startup.rmt" auf dem primären Server.

Ausführen von "pdm_edit.pl" auf einem Windows-Server

Sie können "pdm_edit.pl" auf einem Windows-Server ausführen. Hierzu ist eine primäre Serverinstallation erforderlich sowie optional die Installation eines sekundären Servers, der für alle relevanten CA Service Desk Manager-Dokumente konfiguriert ist.

Hinweis: Führen Sie "pdm_edit.pl" nur auf dem primären Server aus. Weitere Informationen zu sekundären Servern, auf denen die Web-Schnittstelle ausgeführt wird, finden Sie im *Implementierungshandbuch*.

So führen Sie "pdm_edit.pl" auf einem Windows-Server aus:

1. Öffnen Sie ein Eingabeaufforderungsfenster, und wechseln Sie in das folgende Verzeichnis:

```
%installation-directory\samples\pdmconf
```

2. Setzen Sie den folgenden Befehl ab:

```
%installation-directory\bin\pdm_perl pdm_edit.pl
```

Die ausführbare CA Service Desk Manager-Datei "pdm_perl" führt das Skript "pdm_edit.pl" aus. Eine Reihe textbasierter Menüoptionen und Eingabeaufforderungen werden angezeigt, mit denen Sie Objektmanager, WebDirectors und Web-Engines hinzufügen, ändern oder löschen können. Speichern Sie anschließend die Änderungen oder Zusätze in den Dateien "pdm_startup.dat" und "pdm_startup.rmt" auf dem primären Server.

Objektmanager

Objektmanager verwalten alle CA Service Desk Manager-Objekte. Auf dem primären Server befindet sich immer ein Objektmanager. Jeder Objektmanager hat einen Namen, der gleichbedeutend mit dem Namen ist, den der Objektmanager zur Kommunikation mit anderen Objekten benutzt. Der Standardobjektmanager auf dem primären Server ist immer "domsrvr". Unternehmenssysteme mit Multiprozessor-Servern oder sekundären Servern können dem primären Server und den sekundären Servern weitere Objektmanager hinzufügen. Sie können in Objektmanagern navigieren und diese hinzufügen, bearbeiten und löschen.

Jeder Objektmanager ist einem Host zugewiesen. Objektmanager, die dem primären Server zugewiesen sind, geben immer "primary" als Hostname ein.

Sie können Objektmanager gruppieren, damit die Gruppen zugewiesen werden können, die bestimmte Gruppen von Web-Engines und Java-Clients bedienen. In der Regel ist es nicht nötig, eine *Gruppe* zu definieren, denn die Lastenausgleichsfunktion des Systems verteilt die Last auf alle Objektmanager. Benutzer, die die Gruppenfunktion benötigen, haben häufig Web-Engines, die geografisch vom primären Server getrennt sind. In diesem Fall soll ein Objektmanager in der Nähe der Web-Engine liegen. Die Benutzer gruppieren die Objektmanager, die den lokalen Web-Engines zugewiesen sind, und weisen dann dieser Gruppe von Objektmanagern die Web-Engines zu.

Die Annahmemaske (Accept Mask) ist eine erweiterte Funktion. Sie teilt dem Objektmanager mit, von welchen Clients er Verbindungen annehmen soll. Normalerweise versucht eine Web-Engine, eine Verbindung zu einem Objektmanager mit einem Namen wie "web:seattle:1", "web:seattle:2" oder "web:texas:1" herzustellen. Der Administrator kann eine Annahmemaske wie web:seattle.* angeben, um alle Seattle-Verbindungen anzunehmen und andere abzulehnen. Er kann zum Beispiel auch die Maske "web:.*" angeben, um Verbindungen von Web-Engines anzunehmen und Verbindungen von Clients abzulehnen.

Der Anzeigewert (Display Value) ist manchmal nützlich. Die meisten Benutzer überlassen es dem System, für diesen Wert den Hostnamen als Standardwert vorzugeben. Dieser Wert wird auf den Clients angezeigt, um anzugeben, mit welchem Objektmanager der Client verbunden ist.

Starten und Beenden des Objektmanagers

Hinweis: Die Installation von CA Service Desk Manager bietet standardmäßig einen Objektmanager auf dem primären Server. Der Standardobjektmanager, `comm. name = domsrvr`, wird in der Liste der Objektmanager nicht angezeigt. Beachten Sie jedoch, dass dieser Objektmanager vorhanden ist und gestartet wird, wenn der CA Service Desk Manager-Daemon Manager startet.

So starten und beenden Sie einen Objektmanager:

1. Wählen Sie im Hauptmenü von "pdm_edit.pl" die Option "1" aus, und drücken Sie die EINGABETASTE.

Das Objektmanager-Untermenü wird angezeigt.

2. Drücken Sie die Eingabetaste.

Daraufhin wird das Objektmanager-Untermenü geschlossen und das Hauptmenü von "pdm_edit.pl" angezeigt.

Hinzufügen von Objektmanagern

Sie können dem Objektmanager-Untermenü weitere Objektmanager hinzufügen.

So fügen Sie Objektmanager hinzu:

1. Wählen Sie im Objektmanager-Untermenü "a" aus, und drücken Sie die EINGABETASTE.

Es wird eine Eingabeaufforderung angezeigt, in der Sie den Hostnamen angeben müssen.

2. Drücken Sie die EINGABETASTE, um den Standardwert des Primärservers oder einen Wert für den Hostnamen des Sekundärservers auszuwählen.

Hinweis: Bei den Hostnamen aller Sekundärserver muss die Groß-/Kleinschreibung beachtet werden. Sie entsprechen dem Wert von "NX_LOCAL_HOST" in der Datei "NX.env" auf dem Sekundärserver.

3. Drücken Sie die Eingabetaste.

Es wird eine Eingabeaufforderung angezeigt, in der Sie die Gruppe angeben müssen.

4. Drücken Sie die EINGABETASTE, um den Standardwert (keine Annahmemaske) zu übernehmen, oder geben Sie einen Gruppennamen ein, und drücken Sie anschließend die EINGABETASTE.

Es wird eine Eingabeaufforderung angezeigt, in der Sie die Annahmemaske angeben müssen.

Hinweis: Eine Annahmemaske ist ein Filter, der die Kommunikation des Objektmanagers auf die Prozesse beschränkt, deren Name der Annahmemaske entspricht.

5. Drücken Sie die EINGABETASTE, um den Standardwert (keine Annahmemaske) zu übernehmen, oder geben Sie die Zeichenfolge für die Annahmemaske ein.

Es wird eine Eingabeaufforderung angezeigt, in der Sie den Anzeigenamenwert des Scoreboards angeben müssen.

6. Drücken Sie die EINGABETASTE, um den Standardwert zu übernehmen, oder geben Sie einen Wert für den Anzeigenamen ein, und drücken Sie die EINGABETASTE.

Das Objektmanager-Untermenü wird angezeigt und der neu hinzugefügte Objektmanager aufgeführt.

Bearbeiten eines Objektmanagers

Sie können Objektmanager bearbeiten.

So bearbeiten Sie einen Objektmanager:

1. Wählen Sie im Objektmanager-Untermenü "e" aus, und drücken Sie die EINGABETASTE.

In einer Eingabeaufforderung wird die Meldung "Please enter Key" (Schlüssel eingeben) angezeigt.

Hinweis: Dieser Schlüssel wird in der Objektmanagerliste angezeigt und automatisch generiert, wenn Sie einen Objektmanager hinzufügen. Der Schlüssel hat das Format "hostname: #", wobei # eine Ganzzahl in sequenzieller Reihenfolge ist, und die höchste Nummer der Gesamtzahl von Objektmanagern auf dem angegebenen Host entspricht. Wenn zum Beispiel zwei Objektmanager auf dem primären Server und zwei Objektmanager auf einem sekundären Server (host name=godzilla) vorhanden sind, lauten die Schlüssel wie folgt: "primary:1", "primary:2", "godzilla:1" und "godzilla:2".

2. Geben Sie den gewünschten Schlüssel (godzilla:1) ein, und drücken Sie die EINGABETASTE.

Es wird eine Eingabeaufforderung angezeigt, in der Sie die Gruppe angeben müssen.

3. Drücken Sie die EINGABETASTE, um den angezeigten Wert zu übernehmen, oder ändern Sie den Wert, indem Sie einen Wert für die Gruppe eingeben und anschließend die EINGABETASTE drücken.

Es wird eine Eingabeaufforderung angezeigt, in der Sie die Annahmemaske angeben müssen.

4. Drücken Sie die EINGABETASTE, um den angezeigten Wert zu übernehmen, oder ändern Sie den Wert, indem Sie einen Wert für die Annahmemaske eingeben und anschließend die EINGABETASTE drücken.
Es wird eine Eingabeaufforderung angezeigt, in der Sie den Anzeigewert angeben müssen.
5. Drücken Sie die EINGABETASTE, um den angezeigten Wert zu übernehmen, oder ändern Sie den Wert, indem Sie einen Anzeigewert eingeben und anschließend die EINGABETASTE drücken.
Das Objektmanager-Untermenü wird angezeigt und der Objektmanager bearbeitet.

Löschen eines Objektmanagers

Sie können einen Objektmanager löschen.

So löschen Sie einen Objektmanager:

1. Wählen Sie im WebDirector-Untermenü "d" aus, und drücken Sie die EINGABETASTE.

In einer Eingabeaufforderung wird die Meldung "Please enter Key" (Schlüssel eingeben) angezeigt.

2. Geben Sie den gewünschten Schlüssel ein, und drücken Sie die EINGABETASTE.

Hinweis: Wenn Sie einen falschen Schlüssel eingegeben haben (der den falschen domsrvr-Eintrag löscht), beenden Sie das Skript "pdm_edit.pl", *ohne* die Änderungen zu speichern.

Der Objektmanager wird gelöscht und das Objektmanager-Untermenü angezeigt.

Angeben von WebDirectors

WebDirectors sind optional und werden verwendet, wenn Systeme zwei oder mehr Web-Engines benötigen. Ihre Funktion ist der Lastausgleich zwischen den Web-Engines. Es können keine oder mehrere WebDirectors vorhanden sein. Jeder WebDirector gleicht die Last zwischen zwei oder mehr Web-Engines aus.

Führen Sie die folgenden Schritte aus, um einen WebDirector anzugeben:

1. Geben Sie den Hostnamen an.

Wenn sich der WebDirector auf dem primären Server befindet, geben Sie "primär" ein. Geben Sie andernfalls den Namen des sekundären Servers ein. Der sekundäre Servername ist der Eintrag "NX_LOKAL_HOST" in der Datei "NX.env" auf dem sekundären Server.

Hinweis: Es wird zwischen Groß- und Kleinschreibung unterschieden.

2. (Optional) Geben Sie die-Schnittstelle an.

In den meisten Fällen können Sie den Standardwert übernehmen. Wenn Sie einen HTTP-Server wie IIS oder Apache verwenden, handelt es sich bei diesem Wert um die ausführbare CGI-Datei, die auf eine CGI-Anfrage hin ausgeführt wird, (der Name der ausführbaren CGI-Datei). Sie müssen Kopien von "pdmweb.exe" im Verzeichnis "\$NX_ROOT/bopcfg/www/wwwroot" mit diesem Namen erstellen. Wenn Sie einen Servlet-Server wie Tomcat verwenden, wird eine "web.xml.tpl"-Beispieldatei erstellt. Sie verwenden diese Datei, um die Datei "web.xml.tpl" im Verzeichnis ""\$NX_ROOT/bopcfg/www/CATALINA_BASE/webapps/CAisd/WEB-INF" des betreffenden Servers zu ersetzen. Jede "web.xml.tpl"-Beispieldatei wird im aktuellen Verzeichnis erstellt und erhält den Namen "<hostname>-web.xml.tpl".

Starten und Beenden von WebDirectors

Beim Definieren eines WebDirectors werden nur die WebDirector-Informationen hinzugefügt. Dieser WebDirector wird von CA Service Desk Manager nur verwendet, wenn dem WebDirector eine oder mehrere Web-Engines zugewiesen sind. Sie können den WebDirector starten und beenden.

So starten und beenden Sie WebDirectors:

1. Wählen Sie im Hauptmenü von "pdm_edit.pl" die Option "d" aus, und drücken Sie die EINGABETASTE.

Das WebDirector-Untermenü wird angezeigt.

2. Drücken Sie die Eingabetaste.

Daraufhin wird das WebDirector-Untermenü geschlossen und das Hauptmenü von "pdm_edit.pl" angezeigt.

Hinzufügen von WebDirectors

Sie können WebDirectors hinzufügen. Jeder in "pdm_edit.pl" definierter WebDirector muss einen eindeutigen CGI I/F-Wert haben. Der CGI I/F-Name wird automatisch generiert. Sie können den vorgeschlagenen CGI I/F-Namen aber manuell überschreiben, um das gewünschte CGI-Benennungsschema zu reflektieren.

Ziehen Sie Folgendes in Erwägung, bevor Sie WebDirectors hinzufügen:

- Wenn Sie einen HTTP-Server wie IIS oder Apache verwenden, muss im Verzeichnis "\$NX_ROOT/bopcfg/www/wwwroot" eine korrekt benannte ausführbare Datei "pdmweb[#].exe" vorhanden sein.
- Wenn Sie einen Servlet-Server wie Tomcat verwenden, erhalten Sie eine "web.xml.tpl"-Beispieldatei. Diese Datei hat den Namen "<hostname>-web.xml.tpl" und befindet sich im Arbeitsverzeichnis. Verwenden Sie diese Datei, um die Datei "web.xml.tpl" im Verzeichnis "\$NX_ROOT/bopcfg/www/CATALINA_BASE/webapps/CAisd/WEB-INF" auf dem betreffenden Server zu ersetzen.

So fügen Sie WebDirectors hinzu:

1. Wählen Sie im WebDirector-Untermenü "a" aus, und drücken Sie die EINGABETASTE.

Es wird eine Eingabeaufforderung angezeigt, in der Sie den Hostnamen angeben müssen.

2. Drücken Sie die Eingabetaste, um den Standardwert des Primärservers oder einen Wert für den Hostnamen des Sekundärservers auszuwählen.
3. Drücken Sie die Eingabetaste.

Es wird eine Eingabeaufforderung angezeigt, in der Sie einen Namen für die CGI-Schnittstelle eingeben müssen.

4. Drücken Sie die EINGABETASTE, um den angezeigten Wert anzunehmen, oder geben Sie den gewünschten Wert manuell ein, und drücken Sie anschließend die EINGABETASTE.

Das WebDirector-Untermenü wird angezeigt und der neu hinzugefügt WebDirector aufgeführt.

Bearbeiten eines WebDirectors

Sie können einen WebDirector bearbeiten.

So bearbeiten Sie einen WebDirector:

1. Wählen Sie im WebDirector-Untermenü "e" aus, und drücken Sie die EINGABETASTE.

In einer Eingabeaufforderung wird die Meldung "Please enter Key" (Schlüssel eingeben) angezeigt.

2. Geben Sie den gewünschten Schlüssel ein, und drücken Sie die EINGABETASTE.

Es wird eine Eingabeaufforderung angezeigt, in der Sie einen CGI-Wert angeben müssen.

3. Drücken Sie die EINGABETASTE, um den angezeigten Wert anzunehmen, oder ändern Sie den Wert durch Eingeben des gewünschten CGI I/F-Wertes und Drücken der EINGABETASTE.

Das WebDirector-Untermenü wird angezeigt und der WebDirector geändert.

Löschen eines WebDirectors

Sie können einen WebDirector-Eintrag löschen.

So löschen Sie einen WebDirector-Eintrag:

1. Wählen Sie im WebDirector-Untermenü "d" aus, und drücken Sie die EINGABETASTE.

In einer Eingabeaufforderung wird die Meldung "Please enter Key" (Schlüssel eingeben) angezeigt.

2. Geben Sie den gewünschten Schlüssel ein, und drücken Sie die EINGABETASTE.

Hinweis: Wenn Sie einen falschen Schlüssel eingegeben haben (der den falschen WebDirector-Eintrag löscht), beenden Sie das Skript "pdm_edit.pl", *ohne* die Änderungen zu speichern.

Das WebDirector-Untermenü wird angezeigt und der WebDirector-Eintrag gelöscht.

Ändern des CGI I/F-Wertes für einen WebDirector

Sie können den CGI I/F-Wert für einen WebDirector ändern.

So ändern Sie den CGI/IF-Wert:

1. Wählen Sie im WebDirector-Untermenü "c" aus, und drücken Sie die EINGABETASTE.

In einer Eingabeaufforderung wird die Meldung "Please enter Key" (Schlüssel eingeben) angezeigt.

2. Geben Sie den gewünschten Schlüssel ein, und drücken Sie die EINGABETASTE.

Es wird eine Eingabeaufforderung angezeigt, in der Sie einen CGI-Wert angeben müssen.

3. Drücken Sie die EINGABETASTE, um den angezeigten Wert zu übernehmen, oder ändern Sie den Wert, indem Sie den gewünschten CGI I/F-Wert eingeben und anschließend die EINGABETASTE drücken.

Das WebDirector-Untermenü wird angezeigt und der CGI I/F-Wert für den WebDirector geändert.

Web-Engines

Web-Engines unterstützen Sie bei der Vorbereitung von Webseiten für den Web-Client. Alle Systeme verfügen über eine oder mehrere Web-Engines. Auf jedem Server können keine oder mehrere Web-Engines vorhanden sein. Sie können in Web-Engines navigieren und diese hinzufügen, bearbeiten und löschen. Jede Web-Engine stellt eine Verbindung zu einem Objektmanager her, um alle Anfragen für CA Service Desk Manager-Objekte zu verarbeiten. Standardmäßig erfolgt eine Verbindung zum Standardobjektmanager. Wenn es aber mehrere Objektmanager gibt, können Sie diesen Wert auf "ANY" einstellen.

Wenn Sie eine Web-Engine definieren, geben Sie den Hostnamen an. Geben Sie **primär** für alle Web-Engines ein, die auf dem primären Server gestartet werden. Geben Sie andernfalls den Hostnamen des sekundären Servers ein. Bei diesem Namen wird zwischen Groß- und Kleinschreibung unterschieden, und er muss dem NX_LOCAL_HOST-Eintrag in der Datei "NX.env" des sekundären Servers entsprechen.

Jede Web-Engine kann direkt ausgeführt werden, und auf jede Web-Engine kann direkt zugegriffen werden. Beim Direktzugriff startet jeder Webbrowser die spezifische CGI-Schnittstelle für diese Web-Engine, und die Benutzer legen die Systemlast fest (der Lastenausgleich erfolgt nicht automatisch). Alle Clients können eine Verbindung zu derselben Web-Engine herstellen, die somit überlastet ist, während andere Web-Engines ungenutzt bleiben. Daher empfiehlt es sich, einem einzelnen WebDirector zwei oder mehr Web-Engines zuzuweisen. Alle Anfragen, die an eine dieser Web-Engines gehen, werden zum Lastausgleich an den WebDirector geleitet und dann an die Web-Engine in der Gruppe mit der höchsten Verfügbarkeit umgeleitet.

Andere Konfigurationen können WebDirectors umfassen. Bei einer dieser Konfigurationen werden alle Anmeldungen an eine einzelne durch SSL abgesicherte Web-Engine geleitet, die alle Anmeldungen abwickelt. Nach der Anmeldung wird der Client für die weitere Verarbeitung an eine andere verfügbare Web-Engine geleitet.

CGI-Schnittstelle

Jedes Webmodul verfügt über eine CGI-Schnittstelle und verwendet sie folgendermaßen:

- Wenn Sie einen HTTP-Server wie IIS oder Apache verwenden, ist dies eine ausführbare Datei, die im Verzeichnis "NX_ROOT/bopcfg/www/wwwroot" gespeichert ist. Der Name der CGI-Schnittstelle ist der Name der ausführbaren Datei. Browser geben die CGI-Schnittstelle in der Adresszeile ein, und die Anfrage wird an die entsprechende Web-Engine geleitet.
- Wenn Sie einen Servlet-Server wie Tomcat verwenden, wird die CGI-Schnittstelle durch ein Servlet simuliert. Jeder Servlet-Server hat eine Datei "web.xml.tpl", die alle CGI-Schnittstellen beschreibt. Das Dienstprogramm "pdm_edit.pl" erstellt Beispieldateien des Typs "web.xml.tpl" mit dem Namen "<hostname>-web.xml.tpl". Verwenden Sie die Dateien, um die Datei "web.xml.tpl" auf dem entsprechenden Server zu ersetzen, und konfigurieren Sie den Server erneut.
- Bei der Verwendung eines WebDirectors ist es oft nützlich, eine einzelne CGI-Schnittstelle für eine einzelne Web-Engine auf einen bekannten CGI-Namen einzustellen. Alle Anfragen gehen an diese Web-Engine und werden dann an eine Web-Engine mit höherer Verfügbarkeit umgeleitet. Auf diese Weise müssen die Benutzer sich nur einen einzelnen CGI-Schnittstellennamen merken, und alle Anfragen werden auf alle verfügbaren Web-Engines verteilt.

Starten und Beenden der Web-Engine

Die CA Service Desk Manager-Installation installiert und konfiguriert standardmäßig eine Web-Engine auf dem primären Server (key= primary:1; object manager = domsrvr; CGI I/F= pdmcgi, protocol= nicht angegeben).

So starten und beenden Sie die Web-Engine:

1. Wählen Sie im Hauptmenü von "pdm_edit.pl" die Option "w" aus, und drücken Sie die EINGABETASTE.

Das Web-Engine-Untermenü wird angezeigt.

2. Drücken Sie die Eingabetaste.

Daraufhin wird das Web-Engine-Untermenü geschlossen und das Hauptmenü von "pdm_edit.pl" angezeigt.

Überlegungen für das Hinzufügen von Web-Engines

Ziehen Sie folgende Informationen in Erwägung, wenn Sie Webmodule hinzufügen:

- **Umleiten von Clients auf Web-Engines** — Sie können angeben, wie Web-Clients zu Web-Engines umgeleitet werden. In dem folgenden Beispiel werden zwei WebDirectors verwendet: "miko:1" und "godzilla:1". "miko:1" sind vier Web-Engines zugewiesen, "godzilla:1", "godzilla:2", "godzilla:3" und "primary:3". Ein Webclient kann "https:godzilla:8080/Caisd/ComputerAssociates.exe" aufrufen und wird an eine der vier Web-Engines in dieser Gruppe umgeleitet. Wenn ein Web-Client "http://localhost:8080/CAisd/pdmweb6.exe" eingibt, wird der Client immer zu dieser Web-Engine umgeleitet. Beachten Sie auch, dass einige Web-Engines dem Objektmanager "domsrvr" zugewiesen sind, und andere so eingerichtet sind, dass sie mit einem beliebigen Objektmanager (ANY) verbunden sind.
- **Verwendung der Werte CGI I/F** — Jede Web-Engine, das in "pdm_edit.pl" definiert wird, muss über einen eindeutigen CGI I/F-Wert verfügen:
 - Wenn Sie einen HTTP-Server wie IIS oder Apache verwenden, muss im Verzeichnis "\$NX_ROOT/bopcfg/www/wwwroot" ebenfalls eine korrekt benannte ausführbare Datei "pdmweb[#].exe" vorhanden sein.
 - Wenn Sie einen Servlet-Server wie Tomcat verwenden, ersetzt ein Servlet die CGI-Schnittstelle. Für diese Server muss jeweils eine Datei "web.xml.tpl" im Verzeichnis "\$NX_ROOT/bopcfg/www/CATALINA_BASE/webapps/CAisd/WEB-INF" vorhanden sein, die die jeweilige CGI-Schnittstelle beschreibt. Das Dienstprogramm "pdm_edit.pl" erstellt Beispieldateien des Typs "web.xml.tpl" mit dem Namen "<hostname>-web.xml.tpl". Verwenden Sie diese Dateien, um die Datei "web.xml.tpl" zu ersetzen und den Server neu zu konfigurieren.

Hinzufügen von Web-Engines

Sie können Web-Engines hinzufügen.

So fügen Sie Web-Engines hinzu:

1. Wählen Sie im Web-Engine-Untermenü "a" aus, und drücken Sie die EINGABETASTE.

Es wird eine Eingabeaufforderung angezeigt, in der Sie den Hostnamen angeben müssen.

2. Drücken Sie die Eingabetaste, um den Standardwert des Primärservers oder einen Wert für den Hostnamen des Sekundärservers auszuwählen.
3. Drücken Sie die Eingabetaste.

Es wird eine Eingabeaufforderung angezeigt, in der Sie den Objektmanager angeben müssen.

4. Drücken Sie die EINGABETASTE, um den Standardwert "<primary domsrvr>" zu übernehmen, oder geben Sie eine Kombination aus Aliasnamen und domsrvr-Kommunikationsnamen ein, und drücken Sie die EINGABETASTE.

Es wird eine Eingabeaufforderung angezeigt, in der Sie den WebDirector-Schlüssel angeben müssen.

5. Drücken Sie die EINGABETASTE, um den Standardwert (kein WebDirector) zu übernehmen, oder geben Sie einen der aufgeführten WebDirectors über den Schlüsselwert ein, und drücken Sie die EINGABETASTE.

Es wird eine Eingabeaufforderung angezeigt, in der Sie einen Namen für die CGI-Schnittstelle eingeben müssen.

6. Drücken Sie die EINGABETASTE, um den angezeigten Wert anzunehmen, oder geben Sie manuell einen Wert ein, und drücken Sie die EINGABETASTE.

Wenn für diese Web-Engine kein WebDirector angegeben wurde, wird das Web-Engine-Untermenü angezeigt. Wenn ein WebDirector-Wert angegeben wurde oder zuvor in der Web-Engine-Definition vorhanden war, wird eine Eingabeaufforderung angezeigt, in der Sie das Protokoll angeben müssen, das als Präfix für den "RedirectingURL"-Wert der Web-Engine verwendet wird.

7. Drücken Sie die EINGABETASTE, wenn Sie dem „RedirectionURL“-Wert kein Protokollpräfix voranstellen möchten.

8. Geben Sie **http** ein, um das Protokollpräfix "http" für den Umleitungswert anzuhängen, für diese Web-Engine wird SSL erzwungen. Geben sie beispielsweise **https** ein, um das Protokollpräfix "https" an den Umleitungswert anzuhängen.

Hinweis: Wenn ein WebDirector für diese Web-Engine definiert wurde, steuert er die Umleitung zu dieser Web-Engine anhand des "RedirectionURL"-Wertes. Wenn das SSL-Protokoll für diese Web-Engine nicht verwendet wird, geben Sie **http** oder keinen Wert an. Wenn das SSL Protokoll für diese Web-Engine durchgesetzt werden soll, geben Sie **https** an. Wenn Sie "https" für eine Web-Engine, die dem SSL-Protokoll unterliegt, nicht angeben, kann dies einen erfolglosen Umleitungsversuch des WebDirectors zur Folge haben.

9. Drücken Sie die Eingabetaste.

Das Web-Engine-Untermenü wird angezeigt und die neu hinzugefügte Web-Engine aufgeführt.

Bearbeiten einer Web-Engine

Sie können eine Web-Engine bearbeiten.

So bearbeiten Sie eine Web-Engine:

1. Wählen Sie im Web-Engine-Untermenü "e" aus, und drücken Sie die EINGABETASTE.

In einer Eingabeaufforderung wird die Meldung "Please enter Key" (Schlüssel eingeben) angezeigt.

2. Geben Sie den gewünschten Schlüssel ein, und drücken Sie die EINGABETASTE.

Es wird eine Eingabeaufforderung angezeigt, in der Sie den Objektmanager angeben müssen.

3. Drücken Sie die EINGABETASTE, um den angezeigten Wert zu übernehmen, oder ändern Sie den Wert, indem Sie den gewünschten Objektmanager-Wert eingeben und anschließend die EINGABETASTE drücken.

Es wird eine Eingabeaufforderung angezeigt, in der Sie den WebDirector angeben müssen.

4. Drücken Sie die EINGABETASTE, um den angezeigten Wert zu übernehmen, oder ändern Sie den Wert, indem Sie den gewünschten WebDirector-Wert eingeben und anschließend die EINGABETASTE drücken.

Es wird eine Eingabeaufforderung angezeigt, in der Sie einen CGI-Wert angeben müssen.

5. Drücken Sie die EINGABETASTE, um den angezeigten Wert zu übernehmen, oder ändern Sie den Wert, indem Sie den gewünschten CGI I/F-Wert eingeben und anschließend die EINGABETASTE drücken.

Es wird eine Eingabeaufforderung angezeigt, in der Sie das HTTP-Protokoll angeben müssen.

6. Drücken Sie die EINGABETASTE, um den angezeigten Wert zu übernehmen, oder ändern Sie den Wert, indem Sie den gewünschten HTTP-Protokollwert eingeben und anschließend die EINGABETASTE drücken.

Das Web-Engine-Untermenü wird angezeigt.

Löschen einer Web-Engine

Sie können eine Web-Engine löschen.

So löschen Sie eine Web-Engine:

1. Wählen Sie im WebDirector-Untermenü "d" aus, und drücken Sie die EINGABETASTE.

In einer Eingabeaufforderung wird die Meldung "Please enter Key" (Schlüssel eingeben) angezeigt.

2. Geben Sie den gewünschten Schlüssel ein, und drücken Sie die EINGABETASTE.

Hinweis: Wenn Sie einen falschen Schlüssel eingegeben haben (der den falschen Web-Engine-Eintrag löscht), beenden Sie das Skript "pdm_edit.pl", *ohne* die Änderungen zu speichern.

Die Web-Engine wird gelöscht und das Web-Engine-Untermenü angezeigt.

Durchführen von Änderungen mit pdm_edit.pl

Sie können das Dienstprogramm "pdm_edit.pl" verwenden, um Ihrem CA Service Desk Manager-System Konverter, Server, Daemons und Aliase hinzuzufügen und sie zu verschieben.

Hinzufügen eines TNG-Konverters

Mit dem Dienstprogramm "pdm_edit.pl" können Sie einem beliebigen Server in Ihrem System einen einzelnen TNG-Konverter hinzufügen.

Hinweis: Wenn der Daemon Manager den TNG-Konverter verwaltet, wird dieser Daemon mit den anderen Daemon gestartet und beendet. Wenn der TNG-Konverter erforderlich ist, um Ereignisse zu erfassen, nachdem die CA Service Desk Manager-Daemons heruntergefahren wurden, kann der TNG-Konverter diese Anfrage nicht erfüllen. Sie müssen TNG-Konverter daher als Service starten und beenden.

So fügen Sie einen TNG-Konverter hinzu:

1. Wählen Sie im Hauptmenü von "pdm_edit.pl" die Option "T" aus, und drücken Sie die EINGABETASTE.
Das TNG-Konverter-Untermenü wird angezeigt.
2. Wählen Sie im Web-Engine-Untermenü "a" aus, und drücken Sie die EINGABETASTE.
Es wird eine Eingabeaufforderung angezeigt, in der Sie den Hostnamen angeben müssen.
3. Geben Sie **primär** für den Primärserver oder den Hostnamen eines Sekundärservers ein.
Es wird eine Eingabeaufforderung angezeigt, in der Sie eine IP-Adresse eingeben müssen.
4. Geben Sie **HOST_IP_REPLACE** ein, wenn sich der TNG-Konverter auf dem primären Server befindet. Geben Sie andernfalls die IP des sekundären Servers ein.
Der TNG-Konverter wird dem Server hinzugefügt.

Hinzufügen eines UNIX-Konverters

Mit dem Dienstprogramm "pdm_edit.pl" können Sie einem beliebigen Server in Ihrem System einen einzelnen UNIX-Konverter hinzufügen.

So fügen Sie einen UNIX-Konverter hinzu:

1. Wählen Sie im Hauptmenü von "pdm_edit.pl" die Option "N" aus, und drücken Sie die EINGABETASTE.
Das UNIX-Konverter-Untermenü wird angezeigt.
2. Wählen Sie "A", aus und drücken Sie die EINGABETASTE.
Es wird eine Eingabeaufforderung angezeigt, in der Sie den Hostnamen angeben müssen.
3. Geben Sie **primär** für den Primärserver oder den Hostnamen eines Sekundärservers ein.
Es wird eine Eingabeaufforderung angezeigt, in der Sie eine IP-Adresse eingeben müssen.
4. Geben Sie **HOST_IP_REPLACE** ein, wenn sich der UNIX-Konverter auf dem primären Server befindet. Geben Sie andernfalls die IP des sekundären Servers ein.
Der UNIX-Konverter wird dem System hinzugefügt.

Verschieben der Anmeldevalidierung

Der Server für Anmeldevalidierung überprüft Benutzeranfragen mit Hilfe des lokalen Betriebssystems. Der Validierungs-Daemon wird standardmäßig auf dem primären Server gestartet, aber Sie können ihn auf einen sekundären Server, auf dem alle Benutzer Betriebssystemkonten haben, oder auf einen Server mit einem anderen Betriebssystemtyp verschieben.

So verschieben Sie die Anmeldevalidierung:

1. Wählen Sie im Hauptmenü von "pdm_edit.pl" die Option "U" aus, und drücken Sie die EINGABETASTE.
Das Untermenü für Benutzervalidierungsserver wird angezeigt.
2. Geben Sie **E** ein, um den Hostnamen des Servers anzugeben, und drücken Sie die EINGABETASTE.
3. Geben Sie **primär** für den Primärserver oder den Hostnamen des Sekundärservers ein.

Die Anmeldevalidierung wird verschoben.

Verschieben einer LDAP-Servers

Der LDAP-Server (Lightweight Directory Access Protocol) ist standardmäßig auf dem primären Server installiert, kann jedoch zu einem beliebigen sekundären Server verschoben werden.

So verschieben Sie den LDAP-Server:

1. Wählen Sie im Hauptmenü von "pdm_edit.pl" die Option "L" aus, und drücken Sie die EINGABETASTE.
Das LDAP-Serveruntermenü wird angezeigt.
2. Geben Sie **E** ein, um den Hostnamen vom Server anzugeben, bzw. geben Sie **primär** für den primären Server oder den Hostnamen des sekundären Servers ein.

Der LDAP-Server wird verschoben.

Hinzufügen von Repository Daemons

Ein Repository Daemon existiert standardmäßig auf dem primären Server, Sie können jedoch weitere hinzufügen.

So fügen Sie Repository-Daemons hinzu:

1. Wählen Sie im Hauptmenü von "pdm_edit.pl" die Option "R" aus, und drücken Sie die EINGABETASTE.

Das Repository Daemon-Untermenü wird angezeigt.

2. Geben Sie **A** ein, um den Hostnamen des Servers anzugeben.
3. Geben Sie **primär** für den Primärserver oder den Hostnamen des Sekundärservers ein.

Der Repository Daemon wird dem Server hinzugefügt.

Erstellen eines Aliasbeispiels

Aliasnamen sind in CA Service Desk Manager optional. Dieses Beispiel veranschaulicht, wie Sie die Erstellung eines Aliasnamens vorbereiten und dann den Aliasnamen erstellen.

Beispiel: Vorbereitung auf die Erstellung eines Aliasnamens

Bevor Sie Aliasnamen erstellen, gehen Sie wie folgt vor:

1. Definieren Sie Objektmanager, und fügen Sie einige Gruppen hinzu. Die Namen der Objektmanager sind "domsrvr:group1:11", "domsrvr", "domsrvr:seattle:12", "domsrvr;seattle:13" und "domsrvr:Tacoma:11".
2. Definieren Sie Web-Engines, und weisen Sie diesen Objektmanager zu. Wenn Sie den Standardwert annehmen, wird dem Objektmanager "domsrvr" zugewiesen.
3. Geben Sie einen regulären Ausdruck ein, der mit einer Gruppe von Objektmanagern übereinstimmt. Wenn die Web-Engine eine Verbindung zu einem beliebigen Objektmanager herstellt, geben Sie "ANY" ein. "ANY" ist ein Standardaliasname. Die Web-Engines und die Java-Clients verwenden die Aliasnamen, um "ANY" oder eine Teilmenge der ausgeführten Objektmanager anzugeben, zu den sie eine Verbindung herstellen können. 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.

Beispiel: Erstellen eines Aliasnamens

Bei diesem Beispiel wird davon ausgegangen, dass Sie einen Objektmanager definiert und mit einer Gruppe namens "Seattle" verknüpft haben. Ist dies nicht der Fall, wird der Aliasname zwar erstellt, aber eine Warnung angezeigt. Diese Warnung gibt an, dass der definierte Aliasname nicht mit einem vorhandenen Objektmanager übereinstimmt.

1. Wählen Sie im Hauptmenü von "pdm_edit.pl" die Option "A" aus, und drücken Sie die EINGABETASTE.

Das Aliasname-Untermenü wird angezeigt.

2. Geben Sie einen Namen für den Alias ein. Geben Sie in diesem Beispiel **SEATTLE** ein.
Sie werden zur Eingabe des regulären Ausdrucks aufgefordert, der mit diesem Aliasnamen verknüpft ist.
3. Geben Sie **/domsrvr:seattle.*** ein. Dies entspricht jedem Objektmanager, dessen Name mit "domsrvr:seattle" beginnt. Sie können diesen Aliasnamen bei der Konfiguration von Web-Engines und Java-Clients verwenden.
4. Speichern Sie die Änderungen und beenden Sie das Dienstprogramm "pdm_edit.pl".
Ein Alias-Installationsskript (mit der Bezeichnung "alias_install.bat" oder "alias_install.sh") wird erstellt.
5. Führen Sie das Alias-Installationsskript auf Ihrem primären Server aus. Damit werden die Aliasnamen erstellt und an alle sekundären Server und Java-Clients übertragen.

Verschieben von Knowledge Daemons

Knowledge Daemons stellen die Knowledge Base für CA Service Desk Manager bereit. Standardmäßig sind sie auf dem primären Server installiert, können jedoch mit dem Dienstprogramm "pdm_edit.pl" auf sekundäre Server verschoben werden.

So verschieben Sie Knowledge-Daemons:

1. Wählen Sie im Hauptmenü von "pdm_edit.pl" die Option "K" aus, und drücken Sie die EINGABETASTE.
Das Untermenü "Knowledge-Daemons" wird angezeigt.
2. Geben Sie **E** ein, um den Host zu ändern.
3. Geben Sie **primary** für den primären Server oder den Namen des sekundären Servers ein.
Die Knowledge-Daemons werden verschoben.

Empfehlungen zum Anpassen der Installation

Ziehen Sie Folgendes in Erwägung, wenn Sie Anpassungen installieren:

- "pdm_edit.pl" erstellt eine Datei vom Typ "pdm_startup.dat". Behalten Sie diese Datei bei, damit Sie Ihre aktuellen Auswahlen bearbeiten können.
- "pdm_edit.pl" erstellt eine Datei vom Typ "pdm_startup.rmt". Sie ersetzt die Datei "pdm_startup.tpl" im Verzeichnis "\$NX_ROOT/pdmconf" auf dem primären Server.

- Wenn Sie einen Servlet-Server wie Tomcat verwenden, ersetzt ein Servlet die CGI-Schnittstelle. Diese Server benötigen die Datei "web.xml.tpl</cs>". "pdm_edit.pl" erstellt jeweils eine Datei "<hostname>-web.xml.tpl" für jeden Webserver. Verwenden Sie die entsprechende Datei, um die Datei "web.xml.tpl" im Verzeichnis "\$NX_ROOT/bopcfg/www/CATALINA_BASE/webapps/CAisd/WEB-INF" auf jedem der Servlet-Server zu ersetzen.
- Wenn Sie einen HTTP-Server wie IIS oder Apache verwenden, müssen Sie im Verzeichnis "NX_ROOT/bopcfg/www/wwwroot" ausführbare Dateien für die CGI-Schnittstellen erstellen, indem Sie die Datei "pdmweb.exe" kopieren und umbenennen. Sie müssen diesen Vorgang für jede CGI-Schnittstelle für Web-Engines und WebDirectors auf jedem Server wiederholen, der einen Webservice hostet.
- Jede Web-Engine benötigt eine eigene Datei "web.cfg". "pdm_edit.pl" führt "web.cfg"-Dateien und die Namen auf, die zum Speichern dieser Dateien auf dem geeigneten Server verwendet werden sollen. Auf dem primären Server sind zum Beispiel sechs von diesen Dateien vorhanden. Nennen Sie eine dieser "web.cfg" und eine andere "primary-web2.cfg". "pdm_edit.pl" erstellt für jede Web-Engine eine separate Beispieldatei "web.cfg". Kopieren Sie diese Dateien in das Verzeichnis "\$NX_ROOT/bopcfg/www" des betreffenden Servers.
- Wenn Sie IIS verwenden und für jede CGI-Schnittstelle Servererweiterungen erforderlich sind, erstellt "pdm_edit.pl" Dateien vom Typ "<hostname>-site.dat". Kopieren Sie diese Dateien auf die betreffenden Server, und benennen Sie sie in "site.dat" im Verzeichnis "\$NX_ROOT/bopcfg/www" um.
- Wenn Sie Aliasnamen definiert haben, führen Sie auf dem primären Server die Datei "alias_install.sh" oder "alias_install.bat" aus.
- Konfigurieren Sie alle sekundären Server neu.
- Konfigurieren Sie den primären Server neu, ohne die Datenbank erneut zu initialisieren.

Speichern Sie, und beenden Sie "pdm_edit.pl".

Sie können die Änderungen in "pdm_edit.pl" speichern und das Dienstprogramm beenden

So speichern und beenden Sie "pdm_edit.pl":

1. Wählen Sie im Hauptmenü von "pdm_edit.pl" "x", und drücken Sie die Eingabetaste.
Sie werden aufgefordert, eine Vorlagendatei auszuwählen. Diese Vorlagendatei dient als Modell für die Datei "web.cfg", die für die Web-Engines automatisch erzeugt werden.
2. Wählen Sie einen der angezeigten Werte. Wählen Sie zum Beispiel "2", um die Datei "web.cfg.tpl" auszuwählen, die momentan auf dem primären Server verwendet wird. Dadurch helfen Sie, sicherzustellen, dass auf dem System installierte Anpassungen in den neuen "web.cfg.tpl"-Beispieldateien erfasst werden.
3. Drücken Sie die Eingabetaste.
Ihre Änderungen sind nun gespeichert, und die Eingabeaufforderung wird angezeigt.

Starten des WebDirectors

Sie können den WebDirector in der Befehlszeile starten, oder die Datei "pdm_startup" so konfigurieren, dass der WebDirector automatisch startet.

So starten Sie den WebDirector:

1. Öffnen Sie eine Eingabeaufforderung.
2. Geben Sie folgenden Befehl ein:

```
webdirector [-S slump_name] [-c cgi]
```
3. Verwenden Sie Variablen folgendermaßen:

slump_name

Gibt den Slump-Namen des WebDirectors an. Der Slump-Name dient zur eindeutigen Identifizierung des WebDirector-Prozesses. Dieses Argument ist nur erforderlich, wenn Sie mehrere WebDirectors starten möchten. Andernfalls wird empfohlen, den Standardwert „web:director“ zu übernehmen.

Cgi

(Optional) Gibt den Namen des CGI-Prozesses an, der für den WebDirector verwendet wird. Wird dieses Argument nicht bereitgestellt, wird der Standardwert "pdmweb_d1.exe" verwendet.

Der WebDirector wird gestartet und sendet eine Meldung an alle aktiven Web-Engines. Die Web-Engines, die diesem WebDirector zugewiesen sind (d. h. diejenigen, für die "UseDirector" gleich "Yes", "AfterLogin" oder "BeforeLogin" ist und "WebDirectorSlumpName" dem Slump-Namen des WebDirectors entspricht), antworten mit ihren Konfigurationseinstellungen. Beim Starten einer Web-Engine, die zur Verwendung des WebDirectors konfiguriert wurde, sendet die Web-Engine ihre Konfigurationseinstellungen an den verknüpften WebDirector. Auf diese Weise kann der WebDirector eine aktuelle Liste aller aktiven Web-Engines führen.

Abwicklung von Benutzersitzungen durch WebDirector

Sie können Benutzern die Verwendung der URL einer beliebigen Web-Engine oder des WebDirectors ermöglichen, um auf CA Service Desk Manager zuzugreifen.

Hinweis: Wenn alle mit einem WebDirector verbundenen Web-Engines mit "UseDirector" gleich "Yes" konfiguriert sind (d. h. diejenigen, für die "AfterLogin" oder "BeforeLogin" nicht eingestellt ist), funktioniert der WebDirector einzig als Lastausgleich.

WebDirector verarbeitet Benutzersitzungen folgendermaßen:

1. Die folgende WebDirector-URL wird für Benutzer veröffentlicht:
Windows und UNIX: `http://hostname/CAisd/pdmweb_d1.exe`
2. Wenn bei einem WebDirector eine Anfrage eingeht, führt er folgende Schritte für die Web-Engine aus:
 - a. Ermittelt, ob sie zur Verarbeitung der Anfrage am besten geeignet ist
 - b. Untersucht die aktuelle Sitzungszahl
 - c. Berechnet die aktuelle Bereitschaft mit Hilfe der folgenden Formel:
$$\text{aktuelle Willingness} = (\text{konfigurierte Willingness}) / (\text{Anzahl der Sitzungen} + 1)$$
3. Der WebDirector leitet die Anfrage an die Web-Engine mit der höchsten aktuellen Bereitschaft um.
4. Die ausgewählte Web-Engine wickelt die gesamte Sitzung von der Anmeldung bis zur Abmeldung ab.

Wenn ein Benutzer in dieser Umgebung versucht, direkt über die eigene URL der Web-Engine auf diese zuzugreifen, sendet die Web-Engine dem WebDirector eine Meldung mit der Bitte um eine Verweisung. Wenn der WebDirector mit der URL einer anderen Web-Engine antwortet, leitet die ursprüngliche Web-Engine die Sitzung zur empfohlenen Web-Engine um.

Einrichten von WebDirector in einer SSL-Umgebung

Ziehen Sie die folgenden Informationen in Erwägung, wenn eine oder mehrere der Web-Engines, die mit einem WebDirector verknüpft sind, mit der "UseDirector AfterLogin" und die übrigen Web-Engines mit "UseDirector BeforeLogin" konfiguriert wurden:

- **UseDirector AfterLogin** - Wenn ein WebDirector eine Anfrage empfängt, bestimmt er die Web-Engine mit der höchsten Bereitschaft zur Verarbeitung der Anfrage, trifft die Auswahl jedoch nur unter den Web-Engines, für die "UseDirector AfterLogin" eingestellt ist. Für die Anmeldung berücksichtigt der WebDirector Web-Engines mit der Bereitschaft null. Wenn eine mit "UseDirector AfterLogin" konfigurierte Web-Engine eine Anfrage empfängt (entweder durch den Verweis einer Web-Engine oder durch einen direkten Benutzerzugriff auf ihre URL), authentifiziert sie den Benutzer nach der vom Zugriffstyp des Benutzers festgelegten Methode. Nach der Authentifizierung des Benutzers bittet die Web-Engine den WebDirector um eine Verweisung. Der WebDirector wählt erneut eine Web-Engine aus, diesmal unter allen mit ihm verbundenen und mit "UseDirector BeforeLogin" konfigurierten Web-Engines (mit Ausnahme der Web-Engines mit der Bereitschaft null). Wenn die authentifizierende Web-Engine den Verweis empfängt, überträgt sie die Sitzung an die empfohlene Web-Engine.
- **UseDirector BeforeLogin** - Wenn ein Benutzer in dieser Umgebung versucht, direkt auf eine mit "UseDirector BeforeLogin" konfigurierte Web-Engine zuzugreifen, sendet die Web-Engine dem WebDirector eine Meldung mit der Bitte um eine Verweisung. Der WebDirector antwortet mit einem Verweis auf eine mit "UseDirector AfterLogin" konfigurierte Web-Engine, und die ursprüngliche Web-Engine überträgt die Anfrage an die empfohlene Web-Engine.

Um WebDirector in einer SSL-Umgebung einzurichten, ist es ratsam, einen der HTTP-Server für Secure Sockets zu konfigurieren und eine einzelne Web-Engine wie folgt mit diesem Server zu verknüpfen:

1. Lesen Sie die Informationen darüber, wie [WebDirector Sitzungen abwickelt](#) (siehe Seite 410), sorgfältig durch, um ein Verständnis dieses Konzepts zu erzielen.
2. Konfigurieren Sie die einzelne Web-Engine mit "UseDirector AfterLogin" und "WillingnessValue" 0.

3. Sie müssen eine oder mehrere zusätzliche Web-Engines konfigurieren, die eine Verbindung zu einem zweiten HTTP-Server herstellen, der das HTTP-Standardprotokoll verwendet.
4. Konfigurieren Sie diese Web-Engines mit "UseDirector BeforeLogin" und "WillingnessValues", die der Kapazität ihrer Host-Computer entsprechen.

Der WebDirector kann dann alle Anmeldungen an den sicheren Server leiten (da Server mit Bereitschaft null weiterhin für die Anmeldung verfügbar sind). Die restliche Sitzung wird aber an eine der anderen Web-Engines verwiesen.

Verbessern der Leistung mit Browser-Caching

Die Web-Schnittstelle von CA Service Desk Manager 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 Benutzers 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 Service Desk Manager-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 Service Desk Manager-Dateiordner. Das ist normalerweise CAisd:
 - a. Klicken Sie auf das Pluszeichen neben dem Server, auf dem die CA Service Desk Manager-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 Service Desk Manager-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 Service Desk Manager". 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 Service Desk Manager-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.

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 416)

Drucken von CA Service Desk Manager-Webseiten

Zum Formatieren von Schaltflächen und Notizbuchregisterkarten verwendet CA Service Desk Manager 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 Service Desk Manager-Menü auswählen, zeigt die gedruckte Seite nur die Ecken der Schaltflächen oder Registerkarten.

So drucken Sie CA Service Desk Manager-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 Service Desk Manager-Webseiten enthalten Hintergrundgrafiken.

So drucken Sie CA Service Desk Manager-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 Service Desk Manager-Webseiten enthalten Hintergrundgrafiken.

Änderung der Konfigurationsdatei

Wenn Sie die CA Service Desk Manager-Web-Schnittstelle installieren, wird eine Beispieldatei "web-cfg" in "\$NX_ROOT/bopcfg/www" installiert, die Sie entsprechend Ihren Bedürfnissen ändern können. Die Datei "web.cfg" selbst enthält hilfreiche Informationen in Form von Kommentaren, die Sie lesen können, wenn Sie die Datei anzeigen.

Hinweis: Einige zusätzliche Konfigurationsvariablen wie "charset" sind auch im Optionsmanager verfügbar. Diese sind über die Registerkarte "Administration" in der Web-Schnittstelle verfügbar. Informationen hierzu 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 Service Desk Manager 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 Service Desk Manager-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 Service Desk Manager-Formularen- Wenn diese Eigenschaft nicht festgelegt ist, können Sie in einem Formular mit der rechten Maustaste klicken, um ein CA Service Desk Manager-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 Service Desk Manager-Webformular anzeigt. Der Wert von „FormTitle“ ergänzt den Titel des betreffenden angezeigten Formulars.

Standard: CA Service Desk Manager

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 Service Desk Manager - 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.

HtmlCacheSize

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 Service Desk Manager 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.

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.

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 Service Desk Manager 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.

SellistCacheExclude

SellistCacheExclude

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.

SellistCacheMax

SellistCacheMax

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.

```
chgcatt(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 hierseil_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 Service Desk Manager-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-

Wert	Beschreibung
	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. 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 Service Desk Manager 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 Service Desk Manager schlagen in der Regel nicht fehl. Jedoch können Workframe-Anforderungen an andere Server (zum Beispiel integrierte Produkte wie Knowledge-Management) fehlschlagen, wenn der Zielservers 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 10: Konfiguration der Option "Automatische Zuweisung"

Dieses Kapitel enthält folgende Themen:

[Automatische Zuweisung](#) (siehe Seite 433)
[Beziehungen bei der automatischen Zuweisung](#) (siehe Seite 434)
[Methoden der automatischen Zuweisung](#) (siehe Seite 434)
[Implementieren von automatischen Zuweisungen](#) (siehe Seite 435)
[Standardgruppe und -zuständiger](#) (siehe Seite 441)
[Aktivieren der automatischen Zuweisung](#) (siehe Seite 441)
[Überschreiben der automatischen Zuweisung](#) (siehe Seite 442)
[Zuweisungssteuerungen](#) (siehe Seite 443)
[Aktivitätsprotokoll](#) (siehe Seite 446)
[Ablaufverfolgung der automatischen Zuweisung](#) (siehe Seite 447)
[Gespeicherte Abfragen](#) (siehe Seite 447)
[Automatisches Zuweisen von Tickets](#) (siehe Seite 448)
[Automatisches Zuweisen von Workflow-Aufgaben](#) (siehe Seite 454)
[Configuration Item-basierte automatische Zuweisungen](#) (siehe Seite 457)

Automatische Zuweisung

Die *automatische Zuweisung* in CA Service Desk Manager 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 457) 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 Service Desk Manager-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 Service Desk Manager-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 436), in denen Sie sie verwenden möchten.
3. Bauen Sie Beziehungen zwischen einem ermittelten Bereich oder einer Kategorie einerseits und den [Analystengruppen](#) (siehe Seite 436) 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 437)gruppen als verfügbar.

Bereiche und Kategorien

Hinweis: Berücksichtigen Sie beim Konfigurieren von Bereichen und Kategorien die Einstellungen für [Standardgruppen und Zuständige](#) (siehe Seite 441).

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.

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 die Anfrage der Standardgruppe und dem Standardzuständigen zugewiesen. Wenn diese Standardwerte nicht definiert sind, wird die Anfrage 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 Gruppendetailseiten 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 Kontakttyp 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 Anfragen, Incidents und Probleme, die diesem Bereich zugeordnet sind, die Registerkarte "Automatische Zuweisung aktiviert" auf der Detailseite für den Anfrage-/Incident-/Problembereich.
- Wählen Sie für Changes, Issues und Workflow-Aufgaben die Registerkarte "Automatische Zuweisung" und aktivieren Sie das Kontrollkästchen "Automatische Zuweisung aktiviert" auf der Detailseite der Change-Kategorie, der Detailseite der Issue-Kategorie und den Detailseiten der CA Workflow-Vorlage.

Hinweis: Klicken Sie auf "Bearbeiten", um das Kontrollkästchen "Automatische Zuweisung aktiviert" sichtbar zu machen.

Beispiel: Automatische Zuweisung für einen Anfrage-/Incident-/Problembereich aktivieren

Dieses Beispiel zeigt, wie die automatische Zuweisung für einen Anfrage-/Incident-/Problembereich aktiviert wird.

1. Wählen Sie auf der Registerkarte "Administration" die Option "Service Desk" > "Anfragen/Incidents/Probleme" "> "Bereiche" aus.

Die Listenseite für den Anfrage-/Incident-/Problembereich wird angezeigt.

2. Klicken Sie auf den Bereich, für den Sie die automatische Zuweisung konfigurieren möchten.

Die Detailseite für den Anfrage-/Incident-/Problembereich wird angezeigt.

3. Klicken Sie auf "Bearbeiten".

Die Seite "Anfrage-/Incident-/Problembereich aktualisieren" wird angezeigt.

4. Wählen Sie die Registerkarte "Automatische Zuweisung" aus, und geben Sie Folgendes in die Felder ein:

Automatische Zuweisungen – 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 Anfrage-/Incident-/Problembereich können Sie Standardwerte definieren, die automatisch in Anfrage-, 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 Service Desk Manager-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 Anfragen
- 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 Service Desk Manager-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 Service Desk Manager 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.

Hinweis: Die Incident- und Problemoptionen sind nur verfügbar, wenn das System für die Verwendung der ITIL-Methode konfiguriert wurde.

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: Anfrage-Mgr

Beschreibung: Macht das Feld "Zuständiger" eines Incident-Tickets obligatorisch.

require_problem_assignee

Anwendung: Anfrage-Mgr

Beschreibung: Macht das Feld "Zuständiger" eines Problem-Tickets obligatorisch.

require_request_assignee

Anwendung: Anfrage-Mgr

Beschreibung: Macht das Feld "Zuständiger" eines Anfrage-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: Anfrage-Mgr

Beschreibung: Macht das Feld "Gruppe" eines Incident-Tickets obligatorisch.

require_request_group

Anwendung: Anfrage-Mgr

Beschreibung: Macht das Feld "Gruppe" eines Anfrage-Tickets obligatorisch.

require_problem_group

Anwendung: Anfrage-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 Service Desk Manager 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 Service Desk Manager-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 Service Desk Manager weitergegeben werden. Diese Datei wird für Integrationen in Webservices, E-Mail und AHD.DLL. verwenden.

Weitere Informationen:

[Keywords](#) (siehe Seite 492)

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.

Ablaufverfolgung der automatischen Zuweisung

In einer komplexen Implementierung der automatischen Zuweisung kann es vorkommen, dass die automatische Zuweisung nicht die Entscheidungen tritt, 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 den folgenden Befehl auf dem Server:

```
pdm_logstat -f auto.pm milestone
```

Um die Ablaufverfolgung zu deaktivieren, verwenden Sie den folgenden Befehl auf dem Server:

```
pdm_logstat -f auto.pm
```

Gespeicherte Abfragen

Zur Überwachung der Verfügbarkeit von Analysten werden zwei gespeicherte Abfragen bereitgestellt. CA Service Desk Manager-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

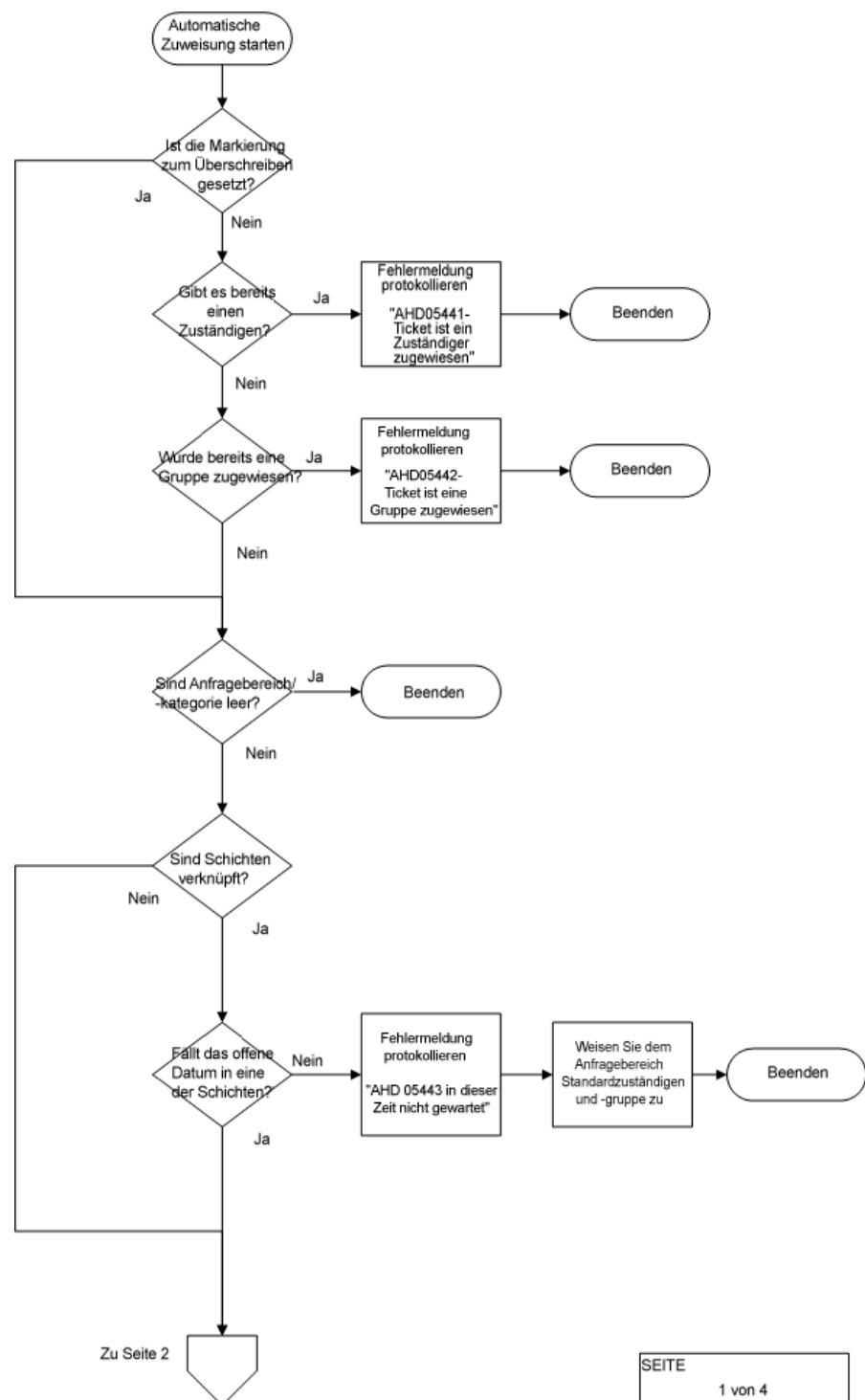
Die Funktion "Automatische Zuweisung" weist Tickets folgendermaßen zu:

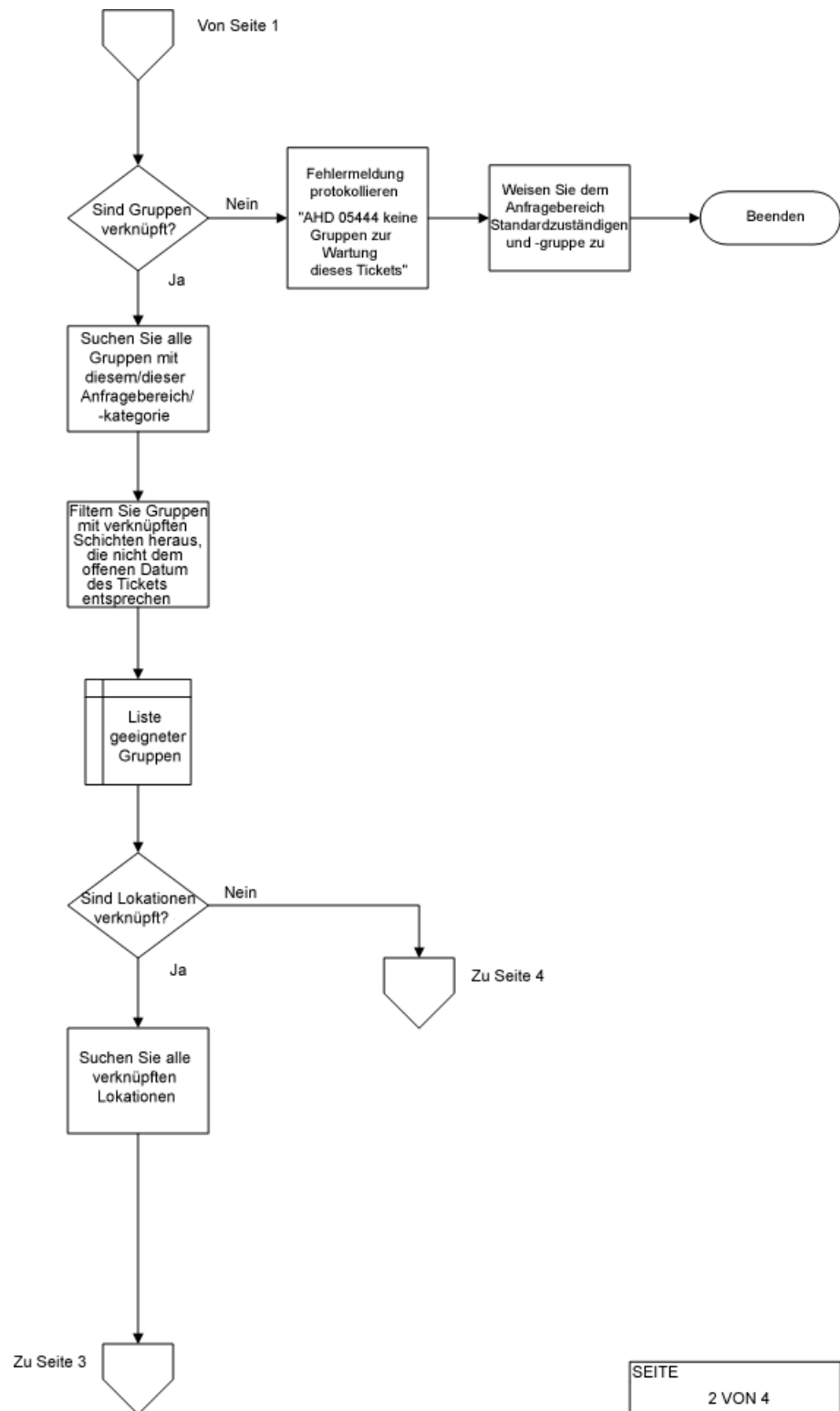
1. Das Speichern eines neuen Tickets löst eine automatische Zuweisung aus.
Wenn ein Bereich oder eine Kategorie nicht für eine automatische Zuweisung konfiguriert ist, wird die Verarbeitung angehalten.
2. Die automatische Zuweisung bestimmt, ob "Autoasg_override" installiert ist.
Ist dies nicht der Fall 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.

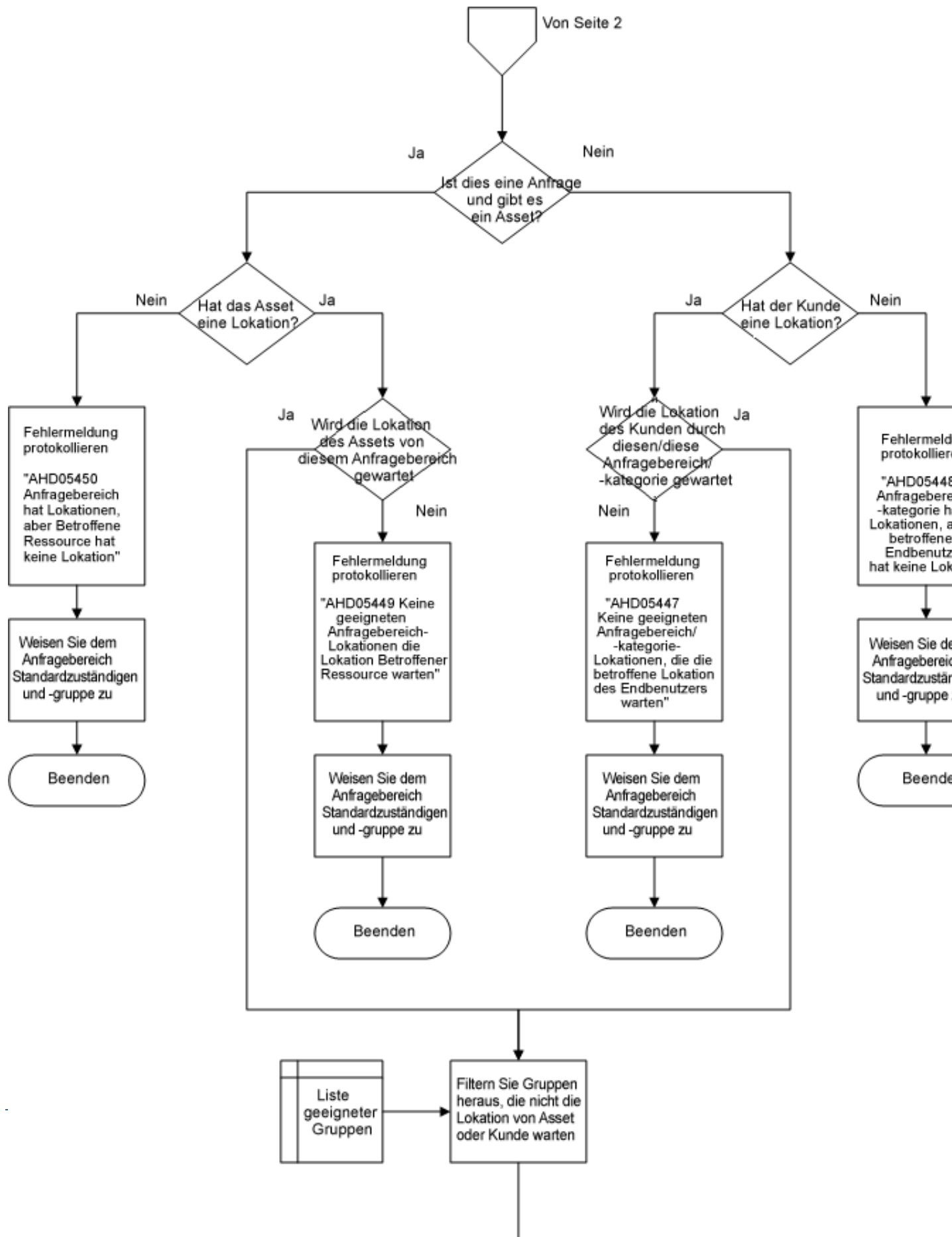
- Wenn Lokationen dem Anforderungsbereich oder der Kategorie zugeordnet sind:

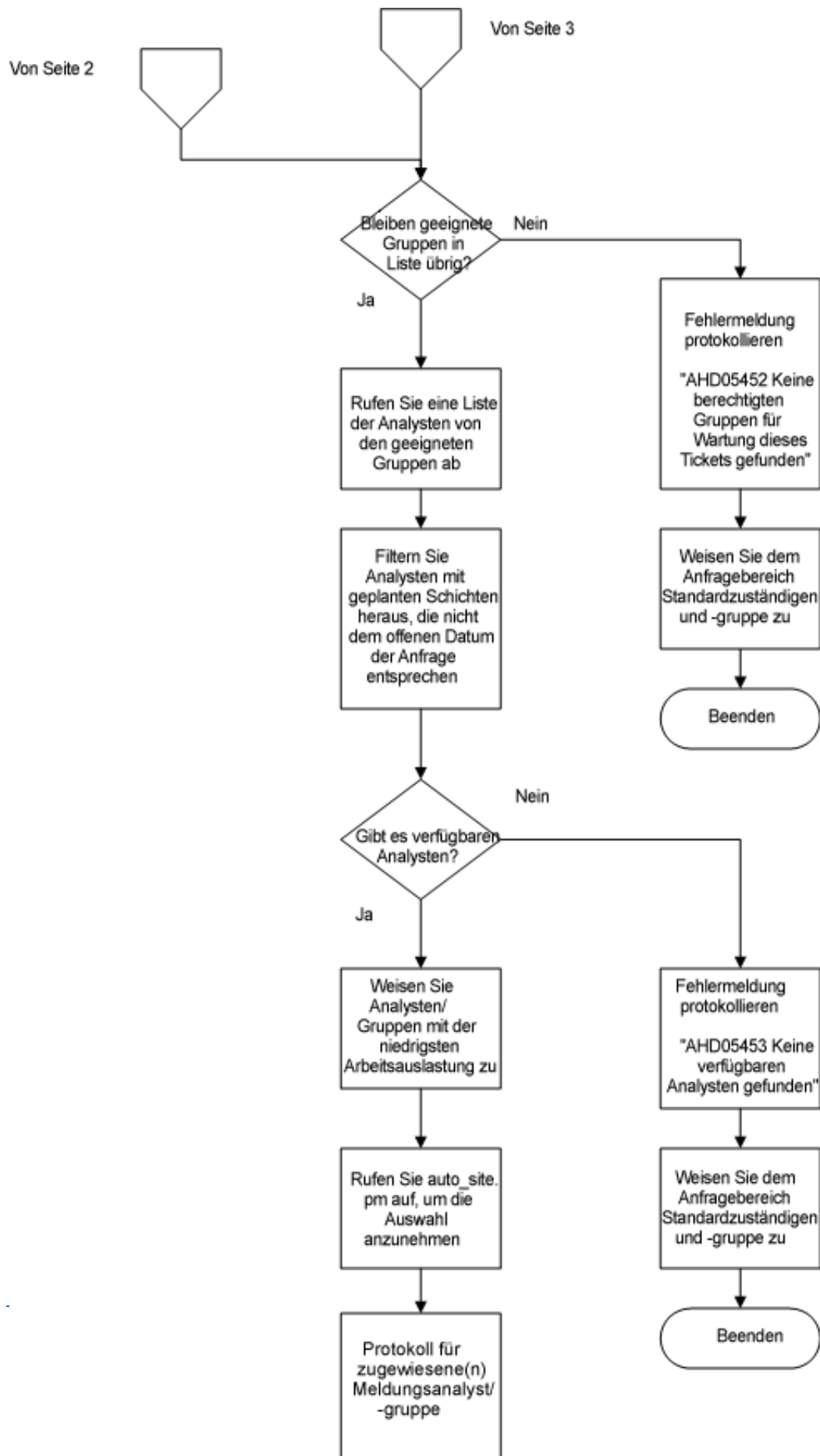
Wenn Lokationen dem Anfragebereich und dem Configuration Item zugeordnet sind (während der automatischen Zuweisung der Anfrage) oder der Kunde keine Lokationen hat, hält die automatische Zuweisung die Verarbeitung an.

7. Die automatische Zuweisung filtert berechnigte 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 berechnigten 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.





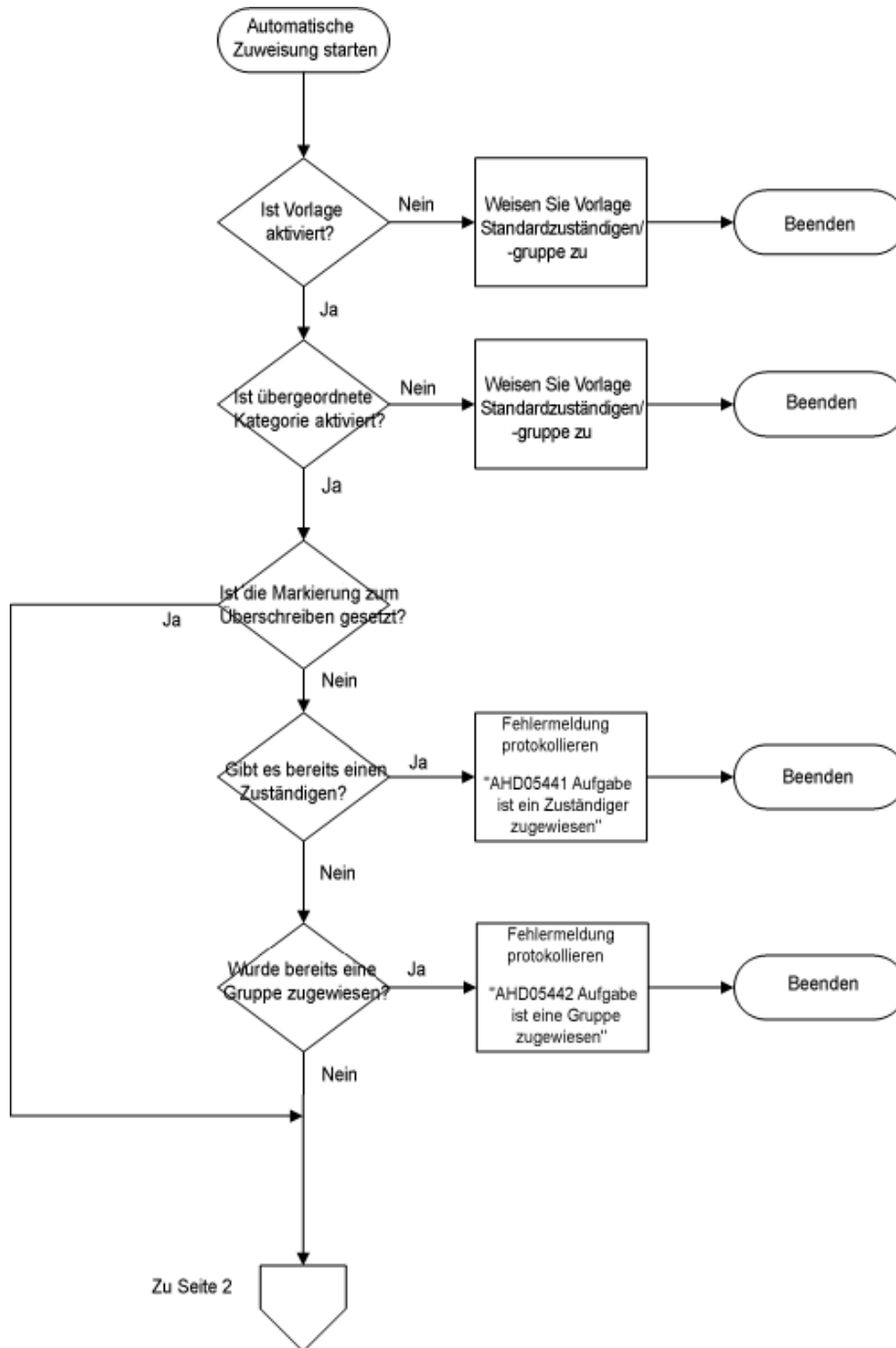


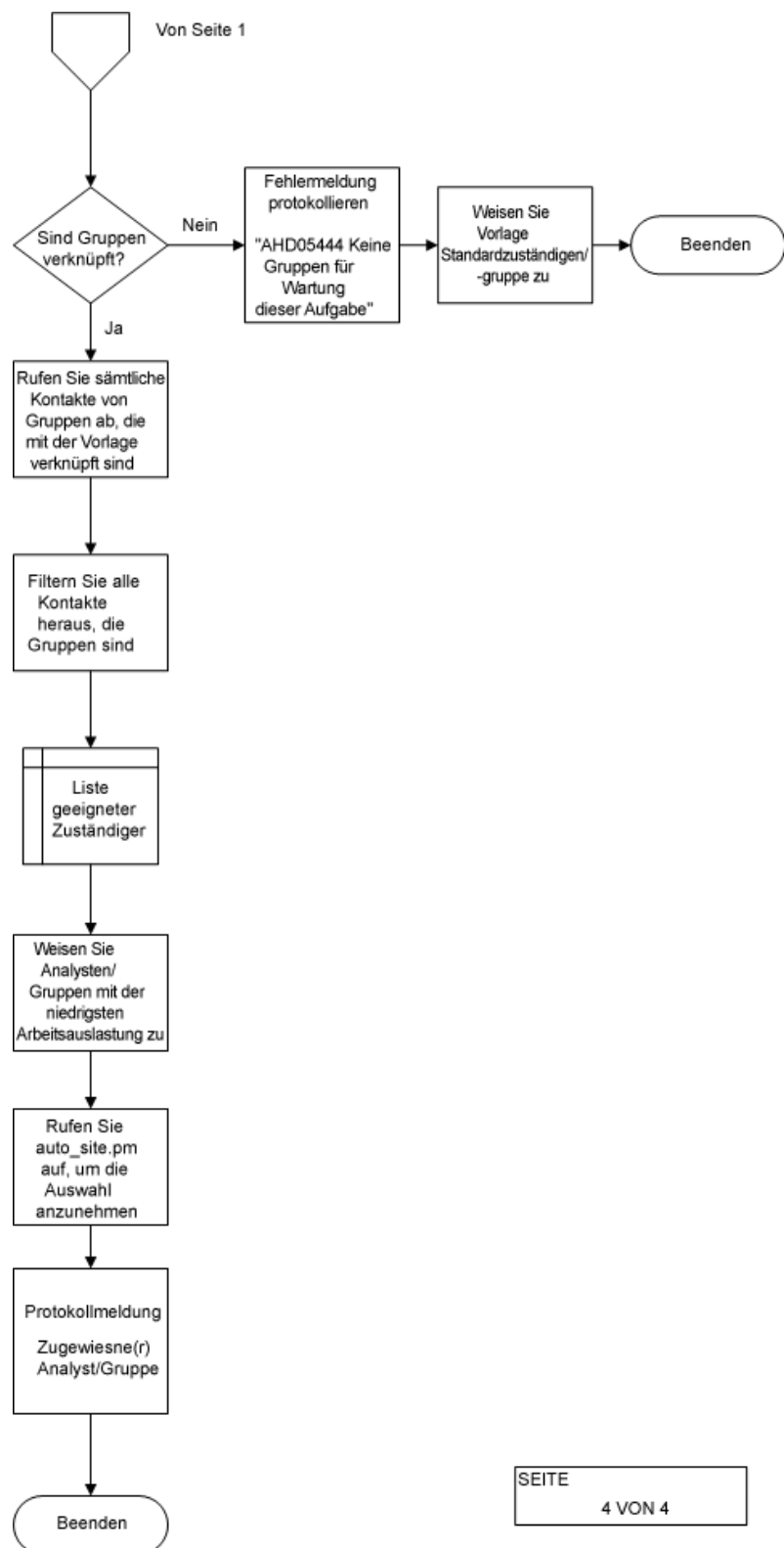


Automatisches Zuweisen von Workflow-Aufgaben

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 Service Desk Manager das Feld "Zuweisbares CI-Attribut" des Bereiches. CA Service Desk Manager 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.

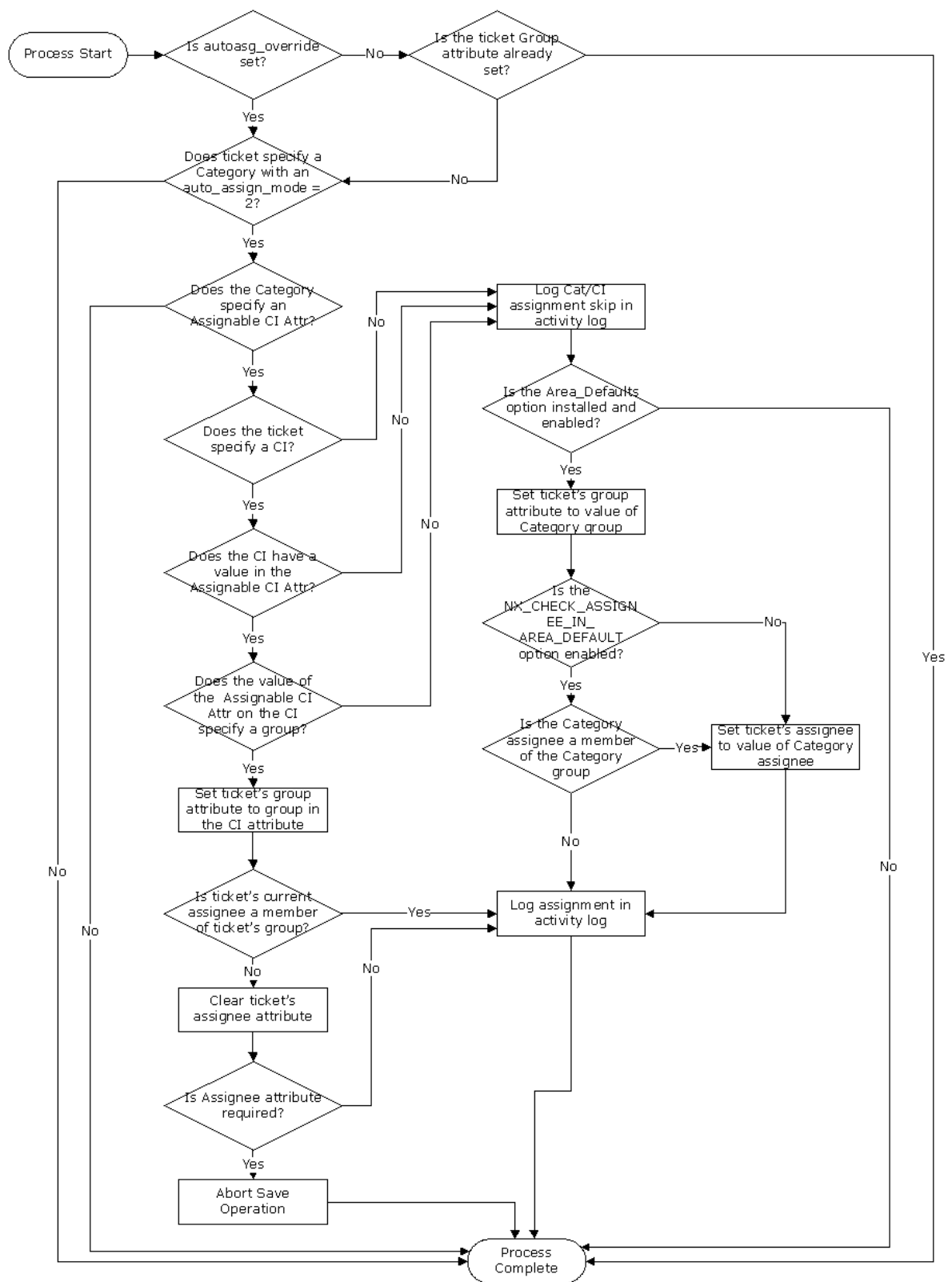
Das folgende Diagramm beschreibt den Prozess für eine auf einem Configuration Item basierende automatische Zuweisung ausführlicher:

1. CA Service Desk Manager 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 Service Desk Manager 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 Service Desk Manager weist der Gruppe das Ticket zu.



Weitere Informationen:

[Überschreiben der automatischen Zuweisung](#) (siehe Seite 442)

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 Service Desk Manager die bestehenden Einstellungen für Verantwortliche und Gruppen, und führt in jedem Fall eine automatische Zuweisung der Tickets durch. Wenn CA Service Desk Manager 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 Service Desk Manager führt eine automatische Zuweisung auf der Basis von Configuration Items durch, und verwendet dabei das im Feld "Zuweisbares CI-Attribut" angegebene Attribut.

Kapitel 11: Verwalten Sie Ihre Datenbank

Dieses Kapitel enthält folgende Themen:

[Datenbankverwaltungsprogramme](#) (siehe Seite 463)
[Auswählen und Konfigurieren der Datenbank](#) (siehe Seite 463)
[Datenbanklader](#) (siehe Seite 464)
[Sichern von Datenbanken](#) (siehe Seite 467)
[Datenbankwiederherstellung](#) (siehe Seite 467)
[Datenbanktabellen-Ersatz](#) (siehe Seite 468)
[Extrahieren von Daten](#) (siehe Seite 468)
[Daten-Dereferenzierung](#) (siehe Seite 470)
[Verwenden des dbadmin-Modus](#) (siehe Seite 473)
[Archivierungs- und Lösungsregeln](#) (siehe Seite 474)

Datenbankverwaltungsprogramme

Sie können Dienstprogramme ausführen, um Ihre Datenbank zu verwalten, während CA Service Desk Manager heruntergefahren ist. Wenn Sie Datenbankverwaltungsprogramme ausführen und als Datenbank nicht das CA Service Desk Manager-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 Service Desk Manager 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 vorgenommenen Änderungen auf der aktuellen Seite zu speichern.

Weiter

Hiermit gehen Sie zur nächsten Seite, nachdem alle vorgenommenen Änderungen auf der aktuellen Seite gespeichert wurden.

Datenbanklader

Das Datenbanklader-Dienstprogramm "pdm_userload" fügt CA Service Desk Manager-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 Service Desk Manager-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 neugestartet 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 CA Service Desk Manager-Server aktiv ist, aber keine Benutzer die Client-Schnittstelle verwenden.

Hinweis: Wenn Sie Datensätze mit Feldern mit Querverweisen hinzufügen müssen, verwenden Sie das Dienstprogramm "pdm_deref.-

Weitere Informationen:

[Daten-Dereferenzierung](#) (siehe Seite 470)

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  
feldname1 feldname4 . . . feldnameN
```

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 1090)

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</cs>", "pdm_userload</cs>" und "pdm_restore</cs>" 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 Service Desk Manager-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 1048)

Datenbankwiederherstellung

Das Dienstprogramm zur Wiederherstellung der Datenbank, pdm_restore, lädt eine von pdm_backup erstellte Ausgabedatei in die CA Service Desk Manager-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 Service Desk Manager-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 Service Desk Manager zugreifen. Mit dem Dienstprogramm "pdm_restore" können Sie die zuletzt gesicherte Kopie Ihrer Datenbank wiederherstellen.

Weitere Informationen:

[pdm_restore – Wiederherstellen einer Datenbank](#) (siehe Seite 1081)

Datenbanktabellen-Ersatz

Das Dienstprogramm pdm_replace ist eine schnelle und einfache Methode, um den gesamten Inhalt einer CA Service Desk Manager-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:

[Erstellen und Nutzen einer Eingabedatei](#) (siehe Seite 465)

[pdm_replace – Ersetzen einer Datenbanktabelle](#) (siehe Seite 1079)

Extrahieren von Daten

Das Dienstprogramm "pdm_extract" extrahiert Daten aus der CA Service Desk Manager-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 Service Desk Manager-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</cs> kompatible Ausgabe
 - CSV-Ausgabe-(Comma Separated Value)
 - Informelle Ausgabe-im Berichtsstil

Weitere Informationen:

[pdm_extract – Extrahieren von Daten aus der Datenbank](#) (siehe Seite 1061)

Verwenden Datenextraktors unter UNIX

Bevor Sie den CA Service Desk Manager-Datenextraktor unter UNIX verwenden, müssen Sie folgende Schritte ausführen:

1. Geben Sie für die Umgebungsvariable \$NX_ROOT den vollständigen Pfadnamen des CA Service Desk Manager-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 Service Desk Manager-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 Service Desk Manager-Datenbank
- CSV-Ausgabe-(Comma Separated Value)
- Informelle Ausgabe-im Berichtsstil

Weitere Informationen:

[pdm_deref – Dereferenzieren von ASCII-Daten](#) (siehe Seite 1053)

Beispiel für das Ausführen von "pdm_deref"

Das folgende Beispiel zeigt, wie man das Hilfsprogramm "pdm_deref" in einem CA Service Desk Manager-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 Service Desk Manager-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"-Eingabedatei, "location.dat", 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", 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</cs> wie folgt aus:

```
pdm_deref -s contact.spec < contact.dat > contact.out
```

Die Ausgabedatei, "contact.out</cs>, 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 Service Desk Manager-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 Service Desk Manager-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 Service Desk Manager 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.

3. 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.

4. Wenn die Bearbeitung abgeschlossen ist, führen Sie `"pdm_halt"` aus, um den dbadmin-Modus zu beenden.
5. Starten Sie das System in gewohnter Weise neu.

Archivierungs- und Lösungsregeln

Sie können die Regeln definieren, die Sie für die Ausführung von Archivierungs- und Lösungsaufgaben für Ihre CA Service Desk Manager-Datenbank verwenden möchten. Sie können vorhandene Regeln modifizieren und aktivieren, anstatt neue zu erstellen.

Hinweis: Wenn Sie bei der Integration mit FAST Dokumente oder Foren manuell gelöscht oder Archivieren und Löschen verwendet haben, werden gelöschte Datensätze in den Suchergebnissen als "Nicht verfügbar" angezeigt. Diese Datensätze werden solange angezeigt, bis CA Service Desk Manager und FAST synchronisiert werden; dies kann einige Minuten in Anspruch nehmen.

Wichtig! Die Standard-Archivierungs- und Lösungsregeln werden auf "Inaktiv" gesetzt. Sie müssen den Suchfilter setzen, um nach inaktiven Regeln zu suchen. Sie können eine Regel ausführen, indem Sie sie aus dem Knoten für Archivierungs- und Lösungsregeln auswählen und auf Säuberungs-Regeln-Knoten und auf "Jetzt ausführen" klicken.

Beispiel: Aktivieren der Regel für das Audit-Protokoll

Sie können die Regel zum Archivieren und Bereinigen der Audit-Protokolleinträge aktivieren und ausführen.

So aktivieren Sie die Regel für das Audit-Protokoll:

1. Navigieren Sie zu "Archivierung und Löschung > Archivierungs- und Lösungsregeln".
Die Seite "Archivierungs- und Lösungsregel - Liste" wird angezeigt.
2. Klicken Sie auf "Filter anzeigen".
Wählen Sie aus der Dropdownliste "Status" die Option "Inaktiv", und klicken Sie auf "Suchen".
Die inaktiven Regeln werden angezeigt.
3. Wählen Sie die Regel für das Audit-Protokoll aus, und klicken Sie auf "Jetzt ausführen".
Der Archivierungs- und Lösungsprozess für die Audit-Protokolleinträge beginnt.

Hinweis: Sie können [die Regel bearbeiten](#) (siehe Seite 478), indem Sie auf die Verknüpfung für das Audit-Protokoll klicken und dann auf "Bearbeiten" klicken.

Ausführen von Archivierungs- und Lösungsregeln

Sie können sowohl aktive als auch inaktive Archivierungs- und Lösungsregeln jederzeit manuell ausführen.

So führen Sie eine Archivierungs- und Lösungsregel über die Listenseite aus:

1. Wählen Sie auf der Registerkarte "Administration" im linken Bereich die Option "Archivieren und Löschen" > "Archivierungs- und Lösungsregeln" aus.
Die Seite "Archivierungs- und Lösungsregel - Liste" wird angezeigt.
2. Wählen Sie die auszuführenden Regeln aus. Klicken Sie hierzu auf das Feld links vom Regelnamen, wählen Sie den Zeitraum in Stunden (1 bis 24), nach dem die Regel beendet werden soll, und klicken Sie auf "Jetzt ausführen".
Eine Meldung wird angezeigt, dass der Archivierungs- und Lösungsprozess gestartet wurde.

3. Klicken Sie auf "OK", um die Meldung zu schließen.

So führen Sie eine Archivierungs- und Lösungsregel über die Detailseite aus:

1. Wählen Sie auf der Registerkarte "Administration" im linken Bereich die Option "Archivieren und Löschen" > "Archivierungs- und Lösungsregeln" aus.

Die Seite "Archivierungs- und Lösungsregel - Liste" wird angezeigt.

2. Wählen Sie die gewünschte Regel durch Klicken auf den Regelnamen aus.

Die Seite "Archivierungs- und Lösungsregel - Detail" wird angezeigt.

3. Wählen Sie den Zeitraum in Stunden (1 bis 24), nach dem die Regel beendet werden soll, und klicken Sie auf "Jetzt ausführen".

Anzeigen von Archivierungs- und Lösungsregeln

Sie können die Zusammenfassungen für jede Archivierungs- und Lösungsregel auf der Seite "Archivierungs- und Lösungsregel - Liste" abrufen. Um diese Seite zu öffnen, wählen Sie auf der Registerkarte "Administration" im linken Bereich die Option "Archivieren und Löschen" > "Archivierungs- und Lösungsregeln" aus.

Sie können einen Filter einrichten, um nur diejenigen Regeln anzuzeigen, die bestimmten Kriterien entsprechen.

Suchen der Liste der Archivierungs- und Lösungsregeln

Sie können Filter einrichten, um nur diejenigen Archivierungs- und Lösungsregeln anzuzeigen, die bestimmten Kriterien entsprechen.

So filtern Sie die Liste der Archivierungs- und Lösungsregeln:

1. Klicken Sie auf der Seite "Archivierungs- und Lösungsregel - Liste" auf "Filter anzeigen".

Im oberen Bereich der Seite werden die Felder des Filters angezeigt.

2. Füllen Sie die Felder so aus, dass nur die gewünschten Regeln angezeigt werden.

3. Klicken Sie auf "Suche".

Die Seite "Archivierungs- und Lösungsregel - Liste" zeigt die Regeln an, die Ihren Filterkriterien entsprechen.

Starten der Archivierung und Löschung mit Hilfe des Schedulers eines Drittanbieters

Sie können den Scheduler eines Drittanbieters verwenden, um eine Archivierungs- und Lösungsregel zu starten und zu beenden. Der Scheduler muss die Ausgabe von Befehlen über eine Befehlszeile unterstützen. Die Datei "arcpur.frg" befindet sich in folgendem Verzeichnis:

```
$NX_ROOT\bopcfg\interp
```

So starten Sie die Archivierung und Löschung mit Hilfe eines Schedulers eines Drittanbieters:

1. Öffnen Sie den Scheduler des Drittanbieters.
2. Legen Sie die Startzeit fest.
3. Führen Sie folgenden Befehl aus:
`bop_cmd -f arcpur.frg "start_arcpur('<rule_name>')"`
4. Legen Sie die Endzeit fest.
5. Führen Sie folgenden Befehl aus:
`bop_cmd -f arcpur.frg "start_arcpur('<rule_name>')"`
Das Archivieren und Löschen ist geplant.

Archivierungs- und Lösungsregeln - Definitionen

Sie können die Regeln definieren, die Sie für die Ausführung von Archivierungs- und Lösungsaufgaben für Ihre CA Service Desk Manager-Datenbank verwenden möchten. Das Produkt bietet einen Satz standardmäßiger Archivierungs- und Lösungsregeln. Sie können vorhandene Regeln modifizieren und aktivieren, anstatt neue zu erstellen.

Erstellen einer Archivierungs- und Lösungsregel

Sie können Regeln einrichten, um automatisch veraltete Datensätze zu archivieren und aus der Datenbank zu entfernen.

So erstellen Sie eine Archivierungs- und Lösungsregel:

1. Wählen Sie auf der Registerkarte "Administration" die Option "Archivierungs- und Lösungsregeln".
Die Seite "Archivierungs- und Lösungsregel - Liste" wird angezeigt.
2. Klicken Sie auf "Erstellen".
Die Seite "Neue Archivierungs- und Lösungsregel erstellen" wird angezeigt.

3. Machen Sie in den Feldern die entsprechenden Angaben.
4. Klicken Sie auf "Speichern".

Die neue Regel wird auf der Seite "Archivierungs- und Lösungsregel - Liste" angezeigt.

Weitere Informationen:

[Archivierungs- und Lösungsregeln - Felder](#) (siehe Seite 478)

[Ausführen von Archivierungs- und Lösungsregeln](#) (siehe Seite 475)

Archivierungs- und Lösungsregeln - Felder

Mit Hilfe der Felder auf den Seiten der Archivierungs- und Lösungsregeln können Sie Definitionen von Archivierungs- und Lösungsregeln definieren und bearbeiten.

Regelname

(Erforderlich) Die eindeutige ID der Regel. Kann bis zu 30 alphanumerische Zeichen umfassen.

Status

(Erforderlich) Zeigt an, ob diese Regel aktiv oder inaktiv ist.

Ablauf

Die Schicht, für die die Regel gilt. Schichten werden vom Administrator definiert.

Rekurrenzintervall

Gibt an, wie oft diese Regel ausgeführt wird, und zwar im Format Stunden:Minuten:Sekunden (HH:MM:SS).

Archiv-Dateiname

Der Name der Datei, in der Sie die veralteten Datensätze speichern möchten. Der Speicherort dieser Datei wird durch die Variable "NX_RULE_ARCHIVE_PATH" gesteuert, die in der Datei "NX.env" gespeichert ist. Mithilfe des Dienstprogramms PDM_LOAD können Sie archivierte Datendateien in der Datenbank wiederherstellen.

Vorgangstyp

Benennt einen der folgenden Vorgangstypen, der die Regel ausführt:

Archive/Purge

Die veralteten Datensätze, die in der im Feld "Archivdateiname" angegeben Datei enthalten sind, aus der Datenbank gelöscht.

Nur Löschung

Veraltete Datensätze werden aus der Datenbank gelöscht, jedoch nicht in die Archivdatei geschrieben.

Nur Archivierung (Testausführung)

Schreibt veraltete Datensätze 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.

Objektname

(Schreibgeschützt) Wird automatisch gemäß Ihrer Auswahl im Feld "Name des konfig. Objekts" angezeigt.

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.

Zum Beispiel archivieren und bereinigen Sie mithilfe der folgenden Abfrage nur zugewiesene inaktive Anfragedatensätze mit einer Priorität von 1.
priority = 1 AND (assignee IS NOT NULL OR group IS NOT NULL) and active = 0

Bearbeiten einer Archivierungs- und Lösungsregel

Sie können eine bereits erstellte Archivierungs- und Lösungsregel bearbeiten.

So bearbeiten Sie eine Archivierungs- und Lösungsregel:

1. Wählen Sie auf der Registerkarte "Administration" die Option "Archivierungs- und Lösungsregeln".
Die Seite "Archivierungs- und Lösungsregel - Liste" wird angezeigt.
2. Wählen Sie die Regel aus, die Sie bearbeiten möchten, und klicken Sie auf den Regelnamen.
Die Seite "Archivierungs- und Lösungsregel - Detail" wird angezeigt.
3. Klicken Sie auf "Bearbeiten".
Die Seite "Archivierungs- und Lösungsregel aktualisieren" wird angezeigt.
4. Bearbeiten Sie die Felder nach Bedarf.

5. Klicken Sie auf "Speichern".

Ihre Bearbeitungen werden gespeichert, und die Seite "Archivierungs- und Lösungsregel - Liste" wird geöffnet.

Weitere Informationen:

[Archivierungs- und Lösungsregeln - Felder](#) (siehe Seite 478)

[Ausführen von Archivierungs- und Lösungsregeln](#) (siehe Seite 475)

Archivierungs- und Lösungsverlauf

Sie können eine Zusammenfassung der Verlaufsdaten für jede einzelne Archivierungs- und Lösungsregel anzeigen.

So zeigen Sie den Archivierungs- und Lösungsverlauf an:

1. Navigieren Sie auf der Registerkarte "Administration" zu "Archivierung und Löschung" und dann zu "Archivierungs- und Lösungsverlauf".

Die Seite "Archivierungs- und Lösungsverlauf - Liste" wird angezeigt. Diese Liste zeigt für jede Ausführung der Regel einen Eintrag an.

2. Folgende Felder stehen zur Verfügung:

Regelname

Zeigt den Namen der Regel an, die in der Verlaufsliste verwendet wird.

Startzeit

Zeigt den Zeitpunkt an, an dem die Regel gestartet wurde.

Endzeit

Zeigt den Zeitpunkt an, an dem die Ausführung der Regel beendet wurde.

Gelöschte Hauptobjekte

Zeigt die Hauptobjekte an, die von der Regel gelöscht wurden. Beispiel: Aufrufanfrage.

Gelöschte untergeordnete Objekte

Zeigt die untergeordneten Objekte an, die von der Regel gelöscht wurden. Beispiel: Aktivitätsprotokolle einer Aufrufanfrage

3. (Optional) Klicken Sie auf "Filter anzeigen" und definieren Sie die Filterkriterien, um die Liste möglicher Informationen zu beschränken.
4. Klicken Sie auf einen Regelnamen, wenn Sie die Konfiguration der Regel überprüfen wollen.

Die Seite "Archivierungs- und Lösungsregel - Detail" wird angezeigt.

Filtern der Liste der Archivierungs- und Lösungsverläufe

Sie können die Liste der Archivierungs- und Lösungsverläufe filtern, um nur die gewünschten Einträge anzuzeigen.

So filtern Sie die Liste der Archivierungs- und Lösungsverläufe:

1. Klicken Sie auf der Seite "Archivierungs- und Lösungsverlauf - Liste" auf "Filter anzeigen".

Im oberen Teil der Seite werden die Felder des Filters angezeigt.

2. Füllen Sie die Felder so aus, dass nur die von Ihnen gewünschten Einträge angezeigt werden:

Regelname

Wählen Sie den Namen der Archivierungs- und Lösungsregel aus, deren Verlauf Sie anzeigen möchten.

Frühestes Startdatum

Geben Sie das früheste Datum und die früheste Uhrzeit ein, um den Beginn eines bestimmten Zeitraums zu definieren, für den Sie die Einträge des Verlaufs anzeigen möchten.

Spätestes Startdatum

Geben Sie das früheste Datum und die früheste Uhrzeit ein, um den Beginn eines bestimmten Zeitraums zu definieren, für den Sie die Einträge des Verlaufs anzeigen möchten.

Frühestes Enddatum

Geben Sie das früheste Datum und die früheste Uhrzeit ein, um das Ende eines bestimmten Zeitraums zu definieren, für den Sie die Einträge des Verlaufs anzeigen möchten.

Spätestes Enddatum

Geben Sie das späteste Datum und die späteste Uhrzeit ein, um das Ende eines bestimmten Zeitraums zu definieren, für den Sie die Einträge des Verlaufs anzeigen möchten.

Hinweis: Um das Feld "Weitere Suchbegriffe" anzuzeigen, klicken Sie auf das Wasserhahn-Symbol. Dieses Feld ist nur für erfahrene Benutzer gedacht, die mit SQL und Majic umgehen und bestimmte weitere Suchargumente angeben können, die im Standard-Suchbereich nicht zur Verfügung stehen. Um ein weiteres Suchargument anzugeben, geben Sie eine SQL WHERE-Klausel in dieses Feld ein.

3. Klicken Sie auf "Suche".

Die Seite "Archivierungs- und Lösungsverlauf - Liste" zeigt die Einträge an, die Ihren Filterkriterien entsprechen.

Verarbeitung von Anhängen (arcpur)

Anhangdatensätze werden in der Datenbank gespeichert, und Dateianhänge werden im Repository-Verzeichnis abgelegt. Wenn Sie Anhangdatensätze in der Datenbank archivieren und löschen, werden sie als gelöscht gekennzeichnet, können aber nicht entfernt werden. Diese Datensätze sind für den Repository-Daemon notwendig, um die Anhänge aufzufinden.

Festlegen des Archivtyps

Sie können auf der Registerkarte "Administration" den Archivtyp für Anhänge in einem Repository festlegen.

So legen Sie den Archivtyp fest:

1. Navigieren Sie zu "Anhangsbibliothek" > "Repositories".
Die Seite "Repositories" wird angezeigt.
2. Klicken Sie mit der rechten Maustaste auf ein Repository (beispielsweise "Service Desk") und wählen Sie "Ansicht".
Die Seite "Repository - Detail" wird angezeigt.
3. Klicken Sie auf "Bearbeiten".
Wählen Sie eine der folgenden Optionen aus dem Dropdownmenü "Archivtypen":

Keine

Es wird kein Archivierungs- und Löschvorgang durchgeführt.

Archivierung und Löschung

Veraltete Datensätze werden in die Datei geschrieben, die im Feld "Archivdateiname" angegeben wurde, und aus der Datenbank gelöscht.

Nur Löschung

Veraltete Datensätze werden aus der Datenbank gelöscht, jedoch nicht in die Archivdatei geschrieben.

4. Klicken Sie auf "Speichern".
Die Seite "Repository - Detail" wird angezeigt, und Ihre Änderungen werden dargestellt.

Hinweis: Sie können Archivierung und Löschung nicht mit Knowledge-Management verwenden. Diese Funktion wird nur für CA Service Desk Manager unterstützt.

Festlegen des Archivpfads

Sie können auf der Registerkarte "Administration" den Archivpfad für Anhänge festlegen.

So legen Sie den Archivtyp fest:

1. Navigieren Sie zu "Anhangsbibliothek" > "Repositorys".
Die Seite "Repositorys" wird angezeigt.
2. Klicken Sie mit der rechten Maustaste auf ein Repository (wie Service Desk) und wählen Sie "Ansicht".
Die Seite "Repository - Detail" wird angezeigt.
3. Klicken Sie auf "Bearbeiten".
Geben Sie den Pfad in das Feld für den Archivpfad ein.
Das Standardverzeichnis lautet:
`$NX_ROOT/site/attachments/default/archived`
4. Klicken Sie auf "Speichern".
Die Seite "Repository - Detail" wird angezeigt, und Ihre Änderungen werden dargestellt.

Wiederherstellen von archivierten Daten

Wenn Sie archivierte Daten wiederherstellen, sollten Sie die Daemons im Modus "dbadmin" mit dem Hilfsprogramm "pdm_d_mgr" starten. Der Modus "Dbadmin" erlaubt den beschränkten Zugriff, so dass Sie "pdm_load" sicher ausführen können, um archivierte Daten wiederherzustellen.

Im Folgenden ist beschrieben, wie archivierte Daten wiederhergestellt werden:

1. Schließen Sie CA Service Desk Manager.
2. Starten Sie die Daemons mit dem folgenden Befehl im Modus "dbadmin":
`C:\>pdm_d_mgr -s DBADMIN`
3. Suchen Sie die archivierte Datei. Die Datei befindet sich standardmäßig unter `$NX_ROOT/site/data/archive`.
4. Wenden Sie "pdm_load" auf die Datei an. Beispiel:
`pdm_load -a -f 2004611T1726_Call_Request.dat`

5. Wenn beim Laden ein Problem auftritt, überprüfen Sie die Befehlszeile und das Protokoll auf Fehler. Arcpur.log-Dateien können in \$NX_ROOT/log gefunden werden.

Hinweis: Die Größenbeschränkung von arcpur.log-Dateien 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.

6. Führen Sie "pdm_halt" aus.

Die Daemons werden so geschlossen.

7. Starten Sie CA Service Desk Manager neu.

Hinweis: Nachdem der Datensatz wiederhergestellt ist, wird er im nächsten Archivierungs- und Löszyklus archiviert und gelöscht.

8. (Optional) 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 Archivierungs- und Lösregeln.

Archivieren und Löschen von KPI-Daten

Es gibt vordefinierte Archivierungs- und Lösregeln für das Archivieren und Löschen von KPI-Daten. Navigieren Sie auf der Registerkarte "Administration" zu "Archivierung und Löschung" und dann zu "Archivierungs- und Lösregeln". Filtern Sie dann die Liste, indem Sie nach inaktiven Regeln suchen. Sie können eine der folgenden Regeln auswählen und diese auf "Aktiv" setzen:

- KPI_Data(SQL)
- KPI_Data(Gespeicherte Abfrage)
- KPI_Data(System)
- KPI_Ticket_Data

Eine optionale Konfigurationsregel kann in den Dateien "arcpur_cfg.xml" und "itil_arcpur_cfg.xml" erstellt werden, um die Tabelle "KPI_Ticket_Data" zu archivieren und zu löschen.

Die Dateien befinden sich in den folgenden Verzeichnissen:

- arcpur_cfg.xml
\$NX_ROOT\site\cfg\
- itil_arcpur_cfg.xml
\$NX_ROOT\site\cfg\

Wenden Sie die folgenden Methoden an, um die Tabelle "KPI_Ticket_Data" zu archivieren und zu löschen:

Tabelle "KPI_Ticket_Data"

- Wenden Sie "end_time" (last_mod_dt) in der Tabelle "KPI_Ticket_data" an, um zu entscheiden, ob ein Datensatz archiviert oder gelöscht werden muss.
- 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.

Die Tabelle "KPI_Ticket_Data" hat keinen SREL-Bezug zu Ticket-Tabellen 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.

Nachdem Sie die Konfigurationsregeln für alle Ticket-Objekte hinzugefügt haben, starten Sie den CA Service Desk Manager-Dienst neu. Diese Konfigurationsregeln werden zu auswählbaren Konfigurationsobjektnamen im Formular "Archivierungs- und Lösungsregeln - Detail".

Archivieren und Löschen von Knowledge-Management-Foren

Sie können Archivierungs- und Lösungsregeln verwenden, um gelöschte Foren in der Datenbank zu bereinigen. Sie können eine neue Archivierungs- und Lösungsregel erstellen, um nur Dokumente vom Typ Forum zu archivieren und zu löschen.

Hinweis: Wenn Sie keine neue Archivierungs- und Lösungsregel erstellen, kann die vorhandene Knowledge-Dokumentregel alle gelöschten Dokumente (auch die Dokumente vom Typ Forum) archivieren und löschen.

So erstellen Sie Regeln, um Foren zu archivieren und zu bereinigen:

1. Navigieren Sie auf der Registerkarte "Administration" zu "Archivierung und Löschung" und dann "Archivierungs- und Lösungsregeln"

Die Seite "Archivierungs- und Lösungsregel - Liste" wird angezeigt.

2. Klicken Sie auf "Neu erstellen".

Die Seite "Neue Archivierungs- und Lösungsregel erstellen" wird angezeigt.

3. Tun Sie Folgendes:

- Wählen Sie im Dropdown-Feld "Name des konfig. Objekts" die Option "Knowledge-Dokument".
- Fügen Sie dem Feld "Zusätzlichen Abfrage" die Zuweisung "KS_TYPE=20" hinzu.

4. Klicken Sie auf "Speichern".

Die neue Archivierungs- und Lösungsregel wurde erstellt.

Archivieren und Löschen mit FAST ESP

Führen Sie nach dem Archivieren und Löschen von Tickets "pdm_k_reindex" aus, um FAST ESP mit den gelöschten Datensätzen zu synchronisieren. Andernfalls werden diese Datensätze auf der Benutzeroberfläche als nicht verfügbar angezeigt.

Beispiel: Ausführen von "pdm_k_reindex" zum Synchronisieren von FAST ESP mit gelöschten Issues

Führen Sie folgenden Befehl aus:

```
pdm_k_reindex sync factory:iss
```


Kapitel 12: Verwenden der Text-API

Dieses Kapitel enthält folgende Themen:

[Text-API](#) (siehe Seite 489)

[Die Konfigurationsdatei](#) (siehe Seite 503)

Text-API

Die *Text-API* ist eine Schnittstelle, über die Sie textbasierte Objekte in der CA Service Desk Manager-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 Benutzer zugreifen können.

Wichtig! Für CA Service Desk Manager müssen alle Eingaben im UTF-8-Format vorliegen; andernfalls können Daten beschädigt werden. Mit dem [Dienstprogramm "pdm_unconv"](#) (siehe Seite 1087) 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 501)

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.

Weitere Informationen:

[pdm_text_cmd – Befehlszeilenschnittstelle für Text-API](#) (siehe Seite 1084)

CA Network and Systems Management-Schnittstelle

Wenn CA NSM und CA Service Desk Manager 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 Service Desk Manager-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 Service Desk Manager weitergegeben werden. Diese Datei wird für Integrationen in Webservices, E-Mail und AHD.DLL. verwenden.

Weitere Informationen:

[Keywords](#) (siehe Seite 492)

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.

Keywords

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.
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": <pre>UPDATE_DESC_IS_LOG</pre> 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.

Schlüsselwort	Beschreibung
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 Benutzer-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 Benutzer-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 Kontaktdatensatzes abgeglichen.
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.

Schlüsselwort	Beschreibung
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 1084)

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 501) 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:

An

Gibt den Mailboxnamen an, der dem für den berechtigten Benutzer eingerichteten CA Service Desk Manager-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").

3. 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 Benutzer (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:

1. 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.

2. 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
Anforderung	%REQUEST_ID	Ref_num
Chg_ref_num	%CHANGE_ID	Chg_ref_num
Issue	%ISSUE_ID	Ref_num

3. Erstellen oder aktualisieren Sie eine Benachrichtigungszeichenfolge, die der Regel entspricht.
4. Erstellen oder aktualisieren Sie eine Meldungsvorlage, die die Benachrichtigungszeichenfolge 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 Benutzer 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 Service Desk Manager übergeben werden.

Weitere Informationen:

[Keywords](#) (siehe Seite 492)

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.

Standardwerte

In der Datei "text_api.cfg" gibt es mehrere Abschnitte [..._DEFAULTS], einen für jede Schnittstelle, die die Text-API verwendet (zum Beispiel [EMAIL_DEFAULTS] für die E-Mail-Schnittstelle und [CMD_DEFAULTS] für die Befehlszeilenschnittstelle). Diese Abschnitte [..._DEFAULTS] definieren Standardwerte für Felder und Eigenschaften, die erforderlich sind, wenn der Benutzer sie nicht direkt angibt.

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 Benutzer 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, Anfrage oder Kontakt.

Weitere Informationen:

[Konvertierungsmethoden](#) (siehe Seite 501)

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 13: Verwalten der Versionskontrolle

Hinweis: In diesem Kapitel bezieht sich "Client" entweder auf einen Client oder auf einen sekundären Server.

Dieses Kapitel enthält folgende Themen:

[Funktionsweise der Versionskontrolle](#) (siehe Seite 509)

[Versionskontrolldateien](#) (siehe Seite 510)

[Versionskontrolldateien des primäre Servers](#) (siehe Seite 510)

[Sekundärer Server und Client-Steuerdateien](#) (siehe Seite 511)

[Versionskontrolle für die Anpassung von Installationen](#) (siehe Seite 511)

[Servermodi für Versionskontrolle](#) (siehe Seite 512)

[Syntax für Versionsverwaltungsdateien](#) (siehe Seite 514)

Funktionsweise der Versionskontrolle

Die Versionskontrolle von CA Service Desk Manager hilft Ihnen, Systemanpassungen zu verwalten, die Clients und sekundäre Server betreffen. Sie können die Versionskontrolle auf Client-Installationen und sekundären Serverinstallationen verwenden.

Die Versionskontrolle funktioniert folgendermaßen:

1. Wenn ein Client eine Verbindung zu einem Server herstellt, sendet er eine Liste seiner der Kontrolle unterliegenden Komponenten an den Server.
2. Der Server vergleicht die Liste mit seiner eigenen Hauptliste.
3. Wenn der Server Unterschiede feststellt, kann er Folgendes unternehmen:
 - den Client benachrichtigen
 - den Verbindungsversuch fehlschlagen lassen
 - den Client auf die richtige Version der der Kontrolle unterliegenden Komponenten aktualisieren

Hinweis: Die Versionskontrolle ist kein System zur Bereitstellung von Software. Die Upgradefunktion ist lediglich eine Methode, um geringfügige Synchronisierungsprobleme zwischen Client und Server zu beheben.

Versionskontrolldateien

CA Service Desk Manager verwaltet zwei Sätze der Versionskontrolldateien. Eine Gruppe bezieht sich auf sekundäre Server und die andere auf alle Clients. Eine kontrollierte Komponente kann eine Datei, ein Verzeichnis oder die Umgebungsvariablendatei "client_nx.env" darstellen. Eine Komponente kann auch generisch sein; d. h. sie ist nicht mit einem 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. Bei nicht übereinstimmenden Versionen von generischen Komponenten erfolgt keine automatische Aktualisierung. Eine Nichtübereinstimmung führt immer zu einem Client-Fehler und muss manuell behoben werden.

Versionskontrolldateien des primäre Servers

Die Versionskontrolle besteht auf dem CA Service Desk Manager-Server aus einer ausführbaren Datei namens "pdm_ver_nxd" und zwei Versionskontrolldateien namens "server_default.ver" und "server_secondary.ver". Die Serveroption „ver_ctl“ bestimmt, wie die Versionskontrolle auf Versionsunterschiede zwischen installierten Komponenten auf dem Server und dem Client reagiert. Die Standardeinstellung der Optionsmanager-Option "ver_ctl" AKTUALISIEREN, was die Versionskontrolle dazu veranlasst, eine Aktualisierung durchzuführen, wenn eine Abweichung festgestellt wird.

"pdm_ver_nxd" validiert Versionsanfragemeldungen von Clients, indem die Daten in der Anfrage mit den folgenden Versionsverwaltungsdateien verglichen werden:

- server_default.ver
- server_secondary.ver
- server_custom.ver
- server_secondary_custom.ver

Wenn "pdm_ver_nxd" eine Diskrepanz bei den Komponentenversionen festgestellt, wird eine Meldung zum Problem protokolliert und, da UPGRADE aktiviert ist, der Client aufgerüstet. Der Inhalt der Benachrichtigungsmeldung hängt von der Einstellung der Option „ver_ctl“ ab.

Wenn Sie möchten, können Sie die folgenden beiden *benutzerdefinierten* Versionskontrolldateien erstellen und pflegen, um Anpassungen zu verwalten:

- server_secondary_custom.ver
- server_custom.ver

Sekundärer Server und Client-Steuerdateien

Die Versionskontrolle auf einem sekundären Server oder Client von CA Service Desk Manager besteht aus einer ausführbaren Datei (pdm_ver) und einer Versionsverwaltungsdatei (secondary.ver). Wenn Sie möchten, können Sie zur Verwaltung von Anpassungen eine zweite Versionskontrolldatei namens "server_secondary_custom.ver" erstellen und pflegen.

Die Clientsoftware umfasst eine ausführbare Datei, pdm_ver, und eine Standardversionsdatei, default.ver. Die Versionskontrolle erstellt automatisch eine zweite Versionsdatei (custom.ver) auf dem Client, wenn auf dem Server die Datei server_custom.ver vorhanden ist. Die zwei Client-Versionsdateien verfolgen die Versionen der auf dem Client installierten Standardkomponenten und angepassten Komponenten.

Die Standardeinstellung der Optionsmanager-Option "ver_ctl" AKTUALISIEREN, was die Versionskontrolle dazu veranlasst, eine Aktualisierung des Sekundärservers durchzuführen, wenn eine Abweichung festgestellt wird. Die Versionsprüfung wird nur für sekundäre Server und Remote-Clients durchgeführt (die Versionskontrolle für Clients, die auf dem primären Server laufen, ist nicht notwendig, da der Server die Masterkopien aller Komponenten enthält). Die Versionskontrolle wird immer in Bezug auf den primären Server durchgeführt. Wenn ein sekundärer Server oder Client startet, liest er seine Versionsdateien und sendet dem primären Server eine Meldung, in der alle installierten Komponenten und ihre Versionen aufgeführt sind. Wenn es eine Diskrepanz bei der Komponentenversion gibt, ermittelt der Server seine Antwort, indem er die Einstellung der Option "ver_ctl" prüft. Die Serverantwort teilt dem Client mit, ob die Verbindung fortgesetzt oder beendet wird oder Komponenten aufgerüstet werden.

Note: Die meisten Clients empfangen einen Download von Dateien und Optionsvariablen bei ihrem anfänglichen Start. Dies reflektiert die Optionen, die vom Administrator gewählt wurden, als der Server konfiguriert und Optionen installiert wurden.

Versionskontrolle für die Anpassung von Installationen

Wenn Sie Ihren CA Service Desk Manager-Client anpassen, können Sie mit der Versionskontrolle die Installation der Anpassungen auf den Clients überwachen und kontrollieren. Erstellen Sie hierzu die Datei "server_custom.ver" (oder "server_secondary_custom.ver" für sekundäre Server), die Ihre Anpassungen beschreibt.

Zur Prüfung der Komponentenversionen auf den Clients verwendet die Versionskontrolle zwei Versionsdateien unabhängig voneinander ("server_default.ver" und "server_custom.ver"). Sie sollten Ihre Komponenten so entwerfen, dass eine Datei nicht von zwei oder mehr Komponenten gesteuert wird. Die Versionskontrolle verarbeitet jede Komponente getrennt. Die Versionskontrolle prüft eine Datei jedes Mal, wenn sie auf eine Komponente trifft, die die Datei steuert. Dies führt manchmal zu unerwarteten Ergebnissen, wenn Versionsnummer oder Datum nicht übereinstimmen.

Führen Sie die folgenden Schritte aus, um die Installation von Anpassungen auf den Clients mit Hilfe der Versionskontrolle zu überwachen und zu kontrollieren:

1. Erstellen Sie die Datei "server_custom.ver" in einem der folgenden Verzeichnisse:
 - Linux - \$NX_ROOT/site/mods/server_custom.ver
 - Windows: installation-directory\site\mods\server_custom.ver
2. Fügen Sie für jede Ihrer Änderungen "server_custom.ver" mit Hilfe der folgenden Setups Komponenten hinzu:
 - Erstellen Sie dir_ctl-Komponenten, um die Versionskontrolle auf Verzeichnisebene zu implementieren. Bei diesem Setup wird davon ausgegangen, dass alle Dateien im Verzeichnis dieselbe Version haben und gleichzeitig aktualisiert werden. Dies minimiert den Verwaltungsaufwand für "server_custom.ver", kann aber manchmal dazu führen, dass Dateien aktualisiert werden, die auf dem Client bereits auf dem neuesten Stand sind.
 - Erstellen Sie file_ctl-Komponenten, um die Versionskontrolle auf Dateiebene zu implementieren. Dieses Setup bietet eine bessere Dokumentation und Kontrolle, kann aber die Größe der Datei "server_custom.ver" erhöhen.
3. Aktualisieren Sie die Versionsnummer in "server_custom.ver", wenn Sie eine angepasste Komponente ändern. Anhand der Versionsnummer erkennt die Versionskontrolle Clients mit unterschiedlicher Version.

Servermodi für Versionskontrolle

Die Serveroption „ver_ctl“ bestimmt, wie die Versionskontrolle auf Versionsunterschiede zwischen installierten Komponenten auf dem Server und dem Client reagiert. Sie stellen diese Option mit dem Optionsmanager ein.

Die Option „ver_ctl“ kann einen der folgenden Werte haben:

BENACHRICHTIGEN

(Windows-Client) Fordert den Benutzer auf beim Feststellen eines Versionsunterschieds fortzufahren oder den Vorgang zu beenden.

(Linux-Client) Protokolliert einen Versionsunterschied. Allerdings wird die Initialisierung immer vom Client abgeschlossen. Es werden keine Dateien geändert, um die Diskrepanz zu korrigieren.

FEHLGESCHLAGEN

Beendet den Client, wenn ein Versionsunterschied erkannt wird. Der Benutzer kann CA Service Desk Manager nicht verwenden, bis der Client manuell aktualisiert wird.

DEAKTIVIEREN

Ignoriert Versionsunterschiede. Alle Clients können eine Verbindung herstellen.

Hinweis: Clients können ihre eigene Option "ver_ctl" auf "DEAKTIVIEREN" einstellen, um die Versionskontrolle zu umgehen.

AKTUALISIEREN

Fordert den Client auf, die betroffenen Komponenten auf die richtige Version zu aktualisieren, wenn ein Versionsunterschied festgestellt wird. Wenn das Upgrade erfolgreich ist, bleibt die Client-Verbindung bestehen. Andernfalls wird der Client beendet. Die Upgrade-Methode hängt vom Versionskontrolltyp der Komponente ab.

Gültige Einstellungen sind folgende:

Einstellung	Beschreibung
dir_ctl	Anhand der vom Server bereitgestellten Kopien fügt der Client im Verzeichnis Dateien hinzu, aktualisiert oder löscht Dateien. Das Verzeichnis selbst wird nie.
file_ctl	Anhand der vom primären Server bereitgestellten Kopie fügt der Client die Datei hinzu, aktualisiert oder löscht die Datei.
nxenv_ctl	Der Client aktualisiert seine Datei "NX.env</cs>".
ver_ctl	Eine ver_ctl-Komponente kann nicht aufgerüstet werden. Eine Diskrepanz bei dieser Art von Komponente bewirkt, dass der Client beendet wird, ohne eine Verbindung zum Server herzustellen.

Syntax für Versionsverwaltungsdateien

Jede Versionsverwaltungsdatei beschreibt eine oder mehrere Komponenten. Eine Komponente kann eine Datei, ein Verzeichnis oder die Umgebungsvariablendatei "client_nx.env" darstellen. Eine Komponente kann auch generisch sein; d. h. sie ist nicht direkt mit einem externen Objekt verbunden.

Hinweis: Um weitere Informationen über die Struktur und die Syntax der Versionskontrolldateien zu erhalten, sehen Sie sich die auf Ihrem System installierten ver-Dateien an. Diese Dateien befinden sich in Ihrem System im Standort-Unterverzeichnis des Installationshauptverzeichnisses von CA Service Desk Manager. Diese Dateien enthalten nützliche Kommentare und Beispieleinstellungen, die Ihnen helfen können.

Verwenden Sie die folgende Syntax, um jede Komponente zu definieren. Elemente in *Kursiv*schrift 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, yyyyymmdd"
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"
```

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 liefern, um eine Maske für Dateien im Verzeichnis anzugeben, die aufgerüstet werden sollen, wenn ein Upgrade erforderlich ist. 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 Service Desk Manager-Umgebungsvariablen gespeichert werden. CA Service Desk Manager-Versionskontrolle und der Optionsmanager pflegen diese Datei automatisch. Es gibt genau eine nxenv_ctl-Komponente, und ihr Komponentename 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:

- SUN4SQL
- 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 50MVB000900 50W7T000900

! Release GA45 45MW000900 50WTT000900

Die Reihenfolge gibt an, dass GA50 neuer ist als GA45.

[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.

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.
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 Service Desk Manager.

o_mode="owner-mode"

Gibt Dateizugriffsberechtigungen für den Eigentümer der Datei an.

g_mode="group-mode"

Gibt Dateizugriffsberechtigungen für Benutzer in der Dateieigentümergruppe an (wird nur für UNIX-Clients verwendet).

w_mode="world-mode"

Gibt Dateizugriffsberechtigungen für Benutzer 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 einen 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.

Aufheben der Kontrolle einer Komponente

Sie müssen unter Umständen die Kontrolle für eine Komponente aufheben. Wenn Sie jedoch die Komponente einfach aus der Datei "server_default.ver" des primären Servers löschen, werden die zugehörigen Dateien ebenfalls gelöscht. Stattdessen können Sie einen *uncontrol*-Block in der Datei "server_default.ver" definieren. Dadurch können Sie die Komponente löschen, ohne die zugehörigen Dateien auf den Clients ebenfalls zu löschen. Diese Anweisungen haben folgende Form:

```
! uncontrol component-name
```

Diese Anweisung gibt an, dass die betreffende Komponente nicht mehr der Kontrolle unterliegt. Clients, die eine Verbindung zu diesem Server herstellen, müssen diese Komponente aus ihrer Versionsdatei entfernen. Außerdem müssen die Clients auch die mit dieser Komponente verbundenen Dateien entfernen. Sie können den uncontrol-Block entfernen, nachdem alle Clients mindestens ein Mal eine Verbindung erfolgreich hergestellt haben.

Hinweis: Sie sollten alle Clients mit dem neuesten Versionskontroll-Client aktualisieren. Ältere Versionskontroll-Clients können nicht der Kontrolle unterliegende Komponenten ignorieren.

Kapitel 14: Verwalten von Konfigurationselementen

Dieses Kapitel enthält folgende Themen:

[Verwenden der Web-Schnittstelle](#) (siehe Seite 521)
[Konfigurationselemente: Kontakt, Standort und Organisation](#) (siehe Seite 526)
[CI-Beziehungen](#) (siehe Seite 530)
[Versionskontrolle](#) (siehe Seite 539)
[Anzeigen von CI-Attributen in anderen CA-Produkten](#) (siehe Seite 569)
[Verwenden des CMDBf-Viewers](#) (siehe Seite 570)
[CMDB Visualizer](#) (siehe Seite 570)
[Hinzufügen von ermittelten Assets](#) (siehe Seite 574)
[Asset- und CI-Markierungen](#) (siehe Seite 575)
[Abstimmung von CIs](#) (siehe Seite 576)
[Verwalten bereitgestellter Transaktionen](#) (siehe Seite 598)
[CA CMDB-Datenwartung](#) (siehe Seite 624)

Verwenden der Web-Schnittstelle

Je nach Ihrer Rolle können Sie unter Verwendung der folgenden Funktionen Benutzer- und Administrationsaufgaben auf Configuration Items (CIs) ausführen:

- Sie können über Scoreboards Benutzerprozesse 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 Benutzer- und Administrationsaufgaben zur Anzeige von CIs und Relationen zwischen CIs

Weitere Informationen:

[Anzeigen von Configuration Items](#) (siehe Seite 522)
[Erstellen von Configuration Items](#) (siehe Seite 522)
[Aktualisieren von Configuration Items](#) (siehe Seite 523)
[Zuordnen eines Wartungsfensters zu einem CI](#) (siehe Seite 524)
[Anzeigen von zugeordneten Change-Fenstern](#) (siehe Seite 524)
[Anzeigen des Konfigurationselement-Verlaufs](#) (siehe Seite 525)
[Deaktivieren von Konfigurationselementen](#) (siehe Seite 525)
[Neu aktivieren von Konfigurationselementen](#) (siehe Seite 526)

Anzeigen von Configuration Items

Mit dem Scoreboard können Sie ein Konfigurationselement öffnen und Informationen darüber anzeigen.

So öffnen Sie ein Konfigurationselement und zeigen es an:

1. Klicken Sie im Scoreboard auf "Suchen" > "Configuration Items".
Das Konfigurationselement-Suchfenster wird angezeigt.
2. Geben Sie die Suchkriterien ein, und klicken Sie auf "Suchen".
Die Konfigurationselement-Liste erscheint und zeigt eine Liste der Suchergebnisse an.
3. (Optional) Klicken Sie auf ein Konfigurationselement 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 Konfigurationselement 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 Konfigurationselement ein.
3. Geben Sie im Feld "Klasse" eine Klasse für das Konfigurationselement 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 Konfigurationselement zutreffen.

Hinweis: Für das Erstellen eines Konfigurationselements 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.

Hinweis: Sie können automatisch neue Configuration Items generieren und die Attributfelder ausfüllen, indem Sie die im Lieferumfang von CA CMDB enthaltenen Federation-Adapter verwenden. Mit den Adaptern können Sie Configuration Item-Daten aus anderen Datenquellen in CA CMDB einschließen.

Aktualisieren von Configuration Items

Mit dem Scoreboard können Sie ein Konfigurationselement ändern.

So ändern Sie ein Konfigurationselement:

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 Seite "Konfigurationselement-Detail".
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 Seite "Konfigurationselement-Detail".
2. Klicken Sie auf die Registerkarte "Wartungsfenster".
Die zugeordneten Wartungsfenster werden gezeigt.

Anzeigen des Konfigurationselement-Verlaufs

Sie können den Verlauf eines Configuration Items anzeigen.

So zeigen Sie den Verlauf eines Konfigurationselements an:

1. Suchen Sie nach dem Konfigurationselement, 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 Konfigurationselements 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 Konfigurationselement, 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 Konfigurationselement, 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 Dropdownliste "Aktiv" aus. Klicken Sie auf "Speichern".

Ein Meldungsfenster wird angezeigt, das die Statusänderung bestätigt. Das Konfigurationselement wird in der Liste der aktiven Konfigurationselemente angezeigt.

Konfigurationselemente: Kontakt, Standort und Organisation

Eine CA CMDB-Installation kann für *Basisobjekte* folgende CIs definieren: Kontakte, Lokationen und Organisationen. Diese Konfigurationselemente können entsprechend verwaltet werden. Zudem können ggf. Beziehungen mit anderen Konfigurationselementen 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 für ein Basisobjekt](#) (siehe Seite 527)

[Wählen eines Basisobjekts für ein Konfigurationselement](#) (siehe Seite 527)

[Bearbeiten von Configuration Item-Details für ein Basisobjekt](#) (siehe Seite 528)

[Bearbeiten von Konfigurationselement-Attributen für ein Basisobjekt](#) (siehe Seite 529)

[Erstellen eines Basisobjekt-Konfigurationselements mit Hilfe von GRLoader](#) (siehe Seite 529)

Erstellen eines CI für ein Basisobjekt

Mit dem Scoreboard können Sie ein Konfigurationselement aus einem Basisobjekt erstellen.

So erstellen Sie ein Konfigurationselement aus einem Basisobjekt:

1. Wählen Sie unter "Datei" die Option "Neues Konfigurationselement" aus.
Die Seite "Neues Configuration Item erstellen" wird angezeigt.

2. Füllen Sie die verschiedenen Felder für das Konfigurationselement aus. Name und Klasse sind erforderlich. Klicken Sie auf "Fortsetzen".

Hinweis: Die allgemeinen Konfigurationselement-Attribute Hostname, Seriennummer, MAC-Adresse und DNS-Name sind irrelevant für ein Konfigurationselement 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 Konfigurationselement

Sie können ein Basisobjekt für ein Konfigurationselement wählen.

So wählen Sie ein Basisobjekt für ein Konfigurationselement:

1. Wählen Sie ein Konfigurationselement 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 darstellt 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 Konfigurationselement-Attributen für ein Basisobjekt

Sie können die Konfigurationselement-Attribute für ein Basisobjekt bearbeiten.

So bearbeiten Sie die Attribute für ein Konfigurationselement:

1. Wählen Sie ein Konfigurationselement 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 zum Aktualisieren des Objekts 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-Konfigurationselements 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, dass ein CI gelesen und eingefügt worden ist.

Beispiel: Erstellen eines Konfigurationselements aus einem vorhandenen Kontakt

Im folgenden Beispiel wird ein Konfigurationselement 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-Beziehungen

Die Funktionen von CA Service Desk Manager 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 531)
[Erstellen eines Beziehungstyps](#) (siehe Seite 531)
[Verwalten von CI-Beziehungen](#) (siehe Seite 532)
[Erstellen von CI-Beziehungen](#) (siehe Seite 533)
[Anzeigen von Beziehungen für ein Konfigurationselement](#) (siehe Seite 534)
[Deaktivieren von CI-Beziehungen](#) (siehe Seite 534)
[Neuaktivieren einer CI-Beziehung](#) (siehe Seite 534)
[Deaktivieren von CI-Beziehungen \(Listebearbeitung\)](#) (siehe Seite 535)
[Deaktivieren von CI-Beziehungen mit Hilfe von GRLoader](#) (siehe Seite 536)
[Erneutes Aktivieren von CI-Beziehungen mit Hilfe von GRLoader](#) (siehe Seite 537)
[Löschen von CI-Beziehungen aus der Datenbank](#) (siehe Seite 538)
[CI-Beziehungs-Verlauf und -Vergleich](#) (siehe Seite 538)

CI-Beziehungstypen

CA Service Desk Manager bietet eine Liste mit vordefinierten Beziehungstypen, die zum Beschreiben einer Beziehung oder Zuordnung von Konfigurationselementen benutzt werden kann. Wie die Beziehung angegeben wird, hängt davon ab, auf welchem Konfigurationselement sich konzentriert wird. Zum Beispiel *unterstützt* ein übergeordnetes Element ein untergeordnetes Konfigurationselement, 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 in der *Technischen Referenz von CA CMDB*.

Erstellen eines Beziehungstyps

Sie können Beziehungstypen erstellen und sie für das Erstellen und Aktualisieren von Beziehungen verfügbar machen.

So erstellen Sie einen Beziehungstyp:

1. Öffnen 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 auf dieser 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 Konfigurationselement, 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 Konfigurationselement 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 Konfigurationselement suchen.

7. Klicken Sie auf "Speichern".

Die Beziehung wird erstellt.

Anzeigen von Beziehungen für ein Konfigurationselement

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 Seite "Konfigurationselement-Detail".
Die Seite "Konfigurationselement-Detail" wird im schreibgeschützten Modus angezeigt.
2. Klicken Sie auf "Bearbeiten".
Die Seite "Konfigurationselement-Detail" 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 Konfigurationselemente 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 Konfigurationselement
 - Untergeordnetes Konfigurationselement
 - 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 Referenzhandbuch zu CA CMDB*.

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 Konfigurationselement
 - Übergeordnetes Konfigurationselement
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 Referenzhandbuch zu CA CMDB*.

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. Die Versionskontrolle bietet folgende Funktionen zur Steuerung der IT-Infrastruktur:

- Erstellen von *Snapshots*, die automatisch aufgezeichnet werden, sobald der Wert eines CI-Attributs geändert wird. Wenn sich beispielsweise die Speichergröße eines Computers ändert, wird ein Snapshot erstellt, mit der der gesamte Status dieses Hardware-CI aufgezeichnet wird. Mit Hilfe der Versionskontrolle kann die Momentaufnahme angezeigt werden, wobei angegeben wird, welche Attribute des Konfigurationselements sich geändert haben. Zudem kann die Momentaufnahme mit allen anderen früheren Momentaufnahmen dieses Konfigurationselements verglichen werden. Diese Informationen sind äußerst wichtig, wenn Sie die Auswirkung von Änderungen der Verfügbarkeit und Leistungsfähigkeit eines CI verstehen möchten.
- Erstellen von *Meilensteinen*. Bei Meilensteinen handelt es sich um Momentaufnahmen für bestimmte Zwecke, die mit einer benutzerdefinierten Bezeichnung wie etwa **Erster Tag der Produktion** oder **Baseline Januar** aufgezeichnet werden. Solche Bezeichnung können zum schnelleren Auffinden bestimmte Snapshots beitragen.
- Vergleichen eines CI mit einem anderen CI, das als Standard fungiert. Für den Vergleich kann jedes als Standard verwendet werden. Es wird jedoch empfohlen, bestimmte 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-Konfigurationselemente freigegebene, dynamische Baselines für Ihre Konfigurationselemente dar.

Wichtig! Ein Standard-CI darf niemals Werte für ein Attribut enthalten, das zur CI-Abstimmung verwendet wird.

Die Versionskontrolle zeichnet sich durch folgende Merkmale aus:

- Automatische Erfassung aller Änderungen an Konfigurationselementen
- 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, benutzerdefinierten Meilensteinen oder einem Standard-CI
- Automatische Snapshots, wenn CA Service Desk Manager-Change-Tickets ihren Status ändern
- Erweiterte Filter- und Vergleichsfunktion mit Druck- und CSV-Export-Unterstützung

Weitere Informationen:

[Verwenden von Versionskontrolle](#) (siehe Seite 540)

[Datensätze für gemeinsame Assets und CI-Audit-Kontrolle](#) (siehe Seite 541)

[Terminologie der Versionskontrolle](#) (siehe Seite 541)

[Datenquellen für Versionskontrollen](#) (siehe Seite 545)

[CA SDM Change Management-Integration](#) (siehe Seite 546)

[CA APM-Integration](#) (siehe Seite 547)

[CI-Versionsmanagement](#) (siehe Seite 548)

[CA SDM Change Management](#) (siehe Seite 568)

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 jener CI-Umgebung änderte. Die Versionskontrolle zeigt neben dem aktuellen Fehlerstatus auch den Status zu einem beliebigen früheren Zeitpunkt an. Dadurch können Sie die beiden Statuswerte vergleichen, 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 Status eines CI jederzeit im Lebenszyklus vom Änderungsmanagement mit seinem Familien-Standard-CI vergleichen. Dadurch wird gewährleistet, dass das CI übereinstimmt. Außerdem können Attribute, die überarbeitet werden müssen, identifiziert werden.

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", die die CA APM-Audit-Kontrollinformationen enthält, ist nur für CIs/Assets aus CA CMDB-Familien verfügbar. Assets, die nicht CA CMDB-Familien angehören, werden nicht angezeigt.

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 Konfigurationselements identifizieren und vergleichen.

Beispiel: Versionsvergleich

Bei einem Konfigurationselement 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:

[Status](#) (siehe Seite 542)

[Versionen](#) (siehe Seite 542)

[Snapshots](#) (siehe Seite 542)

[Kategorien](#) (siehe Seite 543)

[Meilensteine](#) (siehe Seite 543)

[Standard-Konfigurationselemente](#) (siehe Seite 544)

Status

Im Kontext der Versionskontrolle stellt der *Status* eines Konfigurationselements alle Attributwerte dieses Konfigurationselements zu einem bestimmten Zeitpunkt dar. Der Status eines Konfigurationselements kann das Ergebnis von Änderungen an Attributen durch mehrere MDRs sein.

Versionen

Eine *Version* ist eine identifizierte Instanz eines Konfigurationselements innerhalb einer Produktgliederung oder Konfigurationsstruktur. Versionen werden dazu genutzt, den Änderungsverlauf zu verfolgen und zu protokollieren.

Snapshots

Ein *Snapshot* stellt einen vollständigen Status eines Konfigurationselements zu einem bestimmten Zeitpunkt dar. Mit einem typischen Konfigurationselement sind viele Snapshots verknüpft. Ein Snapshot vereint alle Änderungen an einem Konfigurationselement, die innerhalb einer Minute vorgenommen wurden. Wenn ein Konfigurationselement beispielsweise innerhalb einer Minute mehrere Male aktualisiert (bearbeitet und gespeichert) wird, wird ein einziger Snapshot erstellt, 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. Damit Sie besonders wichtige Zeitpunkte finden, ermöglicht CA CMDB eine aussagekräftige Kennzeichnung von Snapshots. Diese benannten Snapshots heißen Meilensteine.

Jede Mal, wenn eine Änderung an einem CI vorgenommen wird, wird automatisch ein Snapshot erstellt, ohne manuell eingreifen zu müssen. Alle Änderungen am CI werden von der Versionskontrolle erfasst. Dabei ist es egal, ob sie mit der Benutzeroberfläche erstellt wurden oder auf ein MDR zurückgehen und mit Hilfe von GRLoader oder CA CMDB-Webservices in 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-Konfigurationselement* wird in der Kategorie "Klassifikation" angezeigt.
- *Beziehungen* werden in der Kategorie "Beziehung" angezeigt.

Meilensteine

Als *Meilenstein* wird der Snapshot eines Konfigurationselements bezeichnet, der auf Wunsch benannt wird. Er wird erstellt, um ein Ereignis, einen logischen Messpunkt oder eine Ansammlung von Änderungen zu kennzeichnen. Er enthält den aktuellen Status des Konfigurationselements zu dem Zeitpunkt, an dem der Snapshot erstellt wurde. Mit Meilensteinen können Sie schnell bedeutende Ereignisse im Verlauf eines CI identifizieren und zu ihnen navigieren. Bei der Erstellung eines Meilensteins wird auch ein entsprechender "Datum"-Snapshot erstellt.

Meilensteine sind Konfigurationselement-spezifisch und werden nicht gemeinsam genutzt. Wenn Sie einen Meilenstein für ein Objekt einer hohen Ebene, zum Beispiel einen Dienst, erstellen, erstellen die Unterkomponenten dieses Objekts Meilensteine nicht automatisch. Um einen Meilenstein für ein Objekt mit mehreren Unterkomponenten zu übernehmen, ist es ratsam, mehrere unabhängige Meilensteine zu 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.

Standard-Konfigurationselemente

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-Konfigurationselemente besitzen. Eine Familie verfügt beispielsweise über Standard-Konfigurationselemente namens "Standard-Testserver", "Standard-Produktionsserver", "Standard-Annahmeserver". Es ist empfehlenswert, dass Sie Ihre Standard-Konfigurationselemente so benennen, dass Sie sie leicht suchen und als Standard-Konfigurationselemente identifizieren können.

Da ein Standard-Konfigurationselement auch selbst ein Konfigurationselement 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-Konfigurationselementen

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 dann generiert, wenn ein CI durch eine Komponente erstellt oder geändert wird, die die Audit-Protokollfunktion unterstützt. 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 Konfigurationselemente 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 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 Service Desk Manager-Change-Verlauf:** Ein Snapshot wird automatisch für alle CIs erstellt, die einem Change-Ticket zugeordnet sind. Wenn das Konfigurationselement 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.

Hinweis: Bei CIs, die in CA Service Desk 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 Service Desk Manager-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 einer Change-Anfrage 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 einer Change-Anfrage) 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 Konfigurationselement 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 Asset Portfolio Management-Auditinformationen 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 Konfigurationselement-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 547)

CA APM-Integrationsfunktionen

CA CMDB 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 Service Desk Manager-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 Momentaufnahmen, Meilensteine und andere Ansichten anzeigen und verwalten, indem die Registerkarte "Versionskontrolle" verwendet wird. Der linke Bereich dient zum Navigieren, der rechte Fensterbereich zum Anzeigen der CI-Details und des Audit-Protokolls. Wenn Sie eine Momentaufnahme oder einen Meilenstein in der linken Fensterhälfte auswählen, zeigt das rechte Fensterhälfte die Attributwerte dieses CI-Status, -Ereignisses 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.

Nur aktuelle Daten anzeigen

Wenn ein CI viele Snapshots oder Beziehungen aufweist, können Sie nur die jüngsten Daten der Versionskontrolle auswählen, um die Zeit zu reduzieren, die für die Anzeige benötigt wird. Die Meldung "Nur neueste Daten laden?" signalisiert die Anzeigengrenze, und Sie können folgendermaßen fortfahren:

- Klicken Sie auf "Abbrechen", um alle Daten anzuzeigen.
- Klicken Sie auf "OK", um nur die aktuellsten Snapshots in den Ansichten "Grundlegend" und "Erweitert" anzuzeigen.

Hinweis: Ein Verlauf, der das MDR, "Zuletzt geändert von" und die Benutzer-ID zeigt, wird nicht für übersprungene Snapshots angezeigt. Bei Snapshots für Daten vor der Installation von CA CMDB r12.5 können Daten zum MDR und zu "Zuletzt geändert von" fehlen.

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 Service Desk Manager bzw. CA CMDB erstellt wurden. Ihre ursprünglichen CI-Attributwerte werden nicht angezeigt. Beziehungen, die mit die in Vorversionen von CA Service Desk Manager 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 Konfigurationselement-Verlaufs

Sie können den Verlauf eines Configuration Items anzeigen.

So zeigen Sie den Verlauf eines Konfigurationselements an:

1. Suchen Sie nach dem Konfigurationselement, 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 Konfigurationselements 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 Konfigurationselements

1. Wählen Sie ein Konfigurationselement 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 Konfigurationselement 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 CI-Daten](#) (siehe Seite 564)

Integrierte CA SDM- und CA APM-Protokolle

Neben solchen Änderungen, die mit Hilfe der CA CMDB-Funktionen gemacht wurden, enthält das CI-Protokoll auch Aktualisierungsereignisse von CA Service Desk Manager-Changeticket-Aktivitäten und von CA APM-Aktualisierungen.

Weitere Informationen:

[CA APM-Integration](#) (siehe Seite 547)

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. 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 Referenzhandbuch zu CA CMDB*.

- Aktualisierungen eines Konfigurationselement-Attributs durch mehr als ein MDR werden identifiziert. Dies kann vorkommen, wenn mehrere MDRs unabhängig voneinander Daten zur Definition eines Konfigurationselements liefern.
- Das maßgebliche Quell-MDR wird identifiziert.

Hinweis: Protokolleinträge, die in CA Service Desk oder früheren Versionen von CA CMDB erstellt wurden, enthalten die Information "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 benutzerdefinierten 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 Konfigurationselement 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 Referenzhandbuch zu CA CMDB*.

Beispiel: Verwenden von GRLoader zur Einrichtung eines Meilensteins

Das folgende GRLoader-Beispiel erstellt den Meilenstein **Geschäftsjahresende 2008**.

```
<ci>
<name>Server1 </name>
<milestone>Geschäftsjahresende 2008</milestone>
</ci>
```

Erstellen eines Standard-Konfigurationselements

Ein Standard-Konfigurationselement können Sie wie jedes andere Konfigurationselement erstellen.

So erstellen Sie in der Benutzeroberfläche ein Standard-Konfigurationselement:

1. Wählen Sie im Menü "Datei" die Option "Neues Konfigurationselement 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-Konfigurationselements zu einem Konfigurationselement

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-Konfigurationselement einer Familie einem Konfigurationselement mit Hilfe der Seite "Konfigurationselement-Detail" zu:

1. Wählen Sie ein Konfigurationselement aus, und klicken Sie auf "Bearbeiten".
Die Seite "Configuration Item aktualisieren" wird angezeigt.
2. Klicken Sie auf das Symbol neben dem Feld "Standard-Konfigurationselement".
Die Konfigurationselement-Liste wird angezeigt.
3. Legen Sie ein Konfigurationselement als Standard-Konfigurationselement fest. Klicken Sie auf "Speichern".
Das Standard-Konfigurationselement wurde zugewiesen.

So weisen Sie das Standard-Konfigurationselement einer Konfigurationselement-Liste mit Hilfe der Funktion "In Liste bearbeiten" zu:

1. Weisen Sie den Suchfilter im Scoreboard oder in der Registerkarte "Administration" an, ein einziges Konfigurationselement oder mehrere Konfigurationselemente in der Detailliste anzuzeigen, und klicken Sie auf "Suchen".
Die Konfigurationselemente, 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 Konfigurationselemente wird angezeigt.

3. Wählen Sie in einer Zeile ein Konfigurationselement aus, das Sie als Standard-Konfigurationselement festlegen möchten.

Die Zeile wird nun farbig hervorgehoben.

4. Klicken Sie auf das Symbol neben dem Feld "Standard-Konfigurationselement".

Die Konfigurationselement-Liste wird angezeigt.

5. Legen Sie ein Konfigurationselement als Standard-Konfigurationselement fest. Klicken Sie auf "Speichern". Das Konfigurationselement wird aktualisiert. Möchten Sie alle Konfigurationselemente in der Liste aktualisieren, klicken Sie auf "Alle ändern".

Sie können das Standard-Konfigurationselement entweder einem einzelnen Konfigurationselement zuweisen ("Speichern"), oder es allen Konfigurationselementen 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 Referenzhandbuch zu CA CMDB*.

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 Benutzers 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 benutzerdefinierten 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-Konfigurationselement ein Standard-Konfigurationselement zugewiesen, können Sie dieses Standard-Konfigurationselement ebenfalls in diesem Ordner sehen.

Meilenstein

Listet alle benutzerdefinierten Meilensteine auf, was der Basisansicht entspricht. Wurde dem Fokus-Konfigurationselement ein Standard-Konfigurationselement zugewiesen, können Sie dieses Standard-Konfigurationselement ebenfalls in diesem Ordner sehen.

Die Attribute von Standard-Konfigurationselementen werden als Strukturknoten mit einem Marker "Standard-Konfigurationselement" dargestellt. Werte für Standard-Konfigurationselemente werden nur für Attribute angezeigt, für die ein Standardwert für Konfigurationselemente 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.

Partnerkonfigurationselement

Status und Datum

Der Beziehungstyp definiert die Art der Beziehung, z. B. "wird enthalten von", "ist Host für" oder "kommuniziert mit".

Als Partnerkonfigurationselement wird der Name des Konfigurationselements 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-Konfigurationselement 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-Anfragenummer, 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.

So zeigen Sie Snapshot-Details an:

1. Öffnen Sie das CI auf der Benutzerschnittstelle, 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 oder Standard-CI 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 Konfigurationselements angezeigt.

Hervorhebung (fett) von Werten

Zeigt an, dass ein Attribut oder eine Beziehung seit der letzten Snapshotaufnahme geändert wurde. In der Detailansicht eines Standard-Konfigurationselements 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 Detailbeitrag des Konfigurationselements im Kontext starten.

Hinweis: Für in CA Service Desk oder früheren CA CMDB-Versionen erstellte CIs sind möglicherweise keine MDR- und "Geändert von"-Informationen 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. Dies kann vorkommen, wenn mehrere MDRs unabhängig voneinander Daten zur Definition eines Konfigurationselements liefern.

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 Konfigurationselements zu einem bestimmten Datum sehen:

1. Wählen Sie ein Konfigurationselement aus, und rufen Sie anschließend die Seite "Konfigurationselement - Detail" auf.
2. Klicken Sie auf die Registerkarte "Versionskontrolle".

Die Standardansicht für das Konfigurationselement wird angezeigt.

3. Wählen Sie das gewünschte Datum aus.

Auf der rechten Seite der Anzeige sehen Sie nun den Status des Konfigurationselements 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 Konfigurationselements zu einem bestimmten Datum sehen:

1. Wählen Sie ein Konfigurationselement aus, und rufen Sie anschließend die Seite "Konfigurationselement - 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 Konfigurationselements 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 Konfigurationselement aus, und rufen Sie anschließend die Seite "Konfigurationselement - 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 Konfigurationselement-Snapshots

Sie können den Snapshot eines CI für ein bestimmtes Datum drucken.

So drucken Sie den Konfigurationselement-Snapshot eines bestimmten Datums:

1. Wählen Sie ein Konfigurationselement 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 CI 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 Konfigurationselement-Meilensteinen

Sie können den Meilenstein eines CI für ein bestimmtes Datum drucken.

So drucken Sie den Konfigurationselement-Meilenstein eines bestimmten Datums:

1. Wählen Sie ein Konfigurationselement 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 CI-Daten

Über die Seite "Versionskontrolle in CSV exportieren" können Sie die CI-Momentaufnahme- und Protokollinformation in eine CSV-Datei (Comma Separated Value, durch Kommata getrennten 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 Konfigurationselement aus, und klicken Sie auf die Registerkarte "Versionskontrolle".
2. Rufen Sie die gewünschte Ansicht für das CI auf, z. B. "Protokoll anzeigen", Snapshot-Vergleich, Meilenstein usw.
3. Klicken Sie auf "Exportieren".

Das Fenster "Versionskontrolle in CSV exportieren" wird für Ihre CI-Ansicht geöffnet.

4. Wählen Sie über das Kontextmenü oder die Tastatur alle Elemente aus.
5. Verwenden Sie die Funktionen "Ausschneiden" und "Einfügen", um die Daten des CIs aus der formatierten Seite in eine CSV-Datei oder in eine Anwendung von Drittanbietern zu übertragen. Sie können die Daten beispielsweise in eine Excel-Kalkulationstabelle exportieren.

Die CI-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 Konfigurationselements bestimmt seine Attribute. Wenn Sie ein *familienpezifisches* Attribut und anschließend die Familie des CI ändern, dann besitzt danach das CI dieses von Ihnen geänderte *familienpezifische* 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 Konfigurationselement 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 Konfigurationselement-Familie wird von Familie 1 zu Familie 2 geändert. Mit dieser Änderung stehen dem Konfigurationselement 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 Konfigurationselement-Familie wird zurück auf Familie 1 geändert. Mit dieser Änderung stehen dem Konfigurationselement 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 Konfigurationselement aus, und rufen Sie anschließend die Seite "Konfigurationselement - 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 Konfigurationselement aus, und rufen Sie anschließend die Seite "Konfigurationselement - 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" und dann in "Geschlossen" ändert, wird für jedes verknüpfte 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 eine Change-Anfrage 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-Anfragedaten 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 Konfigurationselement 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 die Change-Anfrage.

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 die Change-Anfrage.
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 Konfigurationselement.
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 Service Desk Manager 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 Service Desk Manager können Sie Ihre IT-Komponenten (*Konfigurationselemente* 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.

CA verwendet ein Modell für über- und untergeordnete Elemente, um die Beziehungen zwischen Konfigurationselementen zu definieren. Alle Konfigurationselemente, 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 572)

[Visualizer-Administration](#) (siehe Seite 573)

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.

Die Verwaltungsoberfläche von Visualizer bietet folgende Registerkarten:

Registerkarte "Visualizer-Konfiguration"

Ermöglicht die Einstellung des Servers und der Display-Informationen zu Configuration Items.

Registerkarte "Beziehung - Stil"

Definiert die grafischen Eigenschaften von Beziehungen.

Hinweis: Diese Seite ist auf einem Visualizer-Sekundärserver deaktiviert.

Die Registerkarte "Configuration Item-Status"

Definiert die grafischen Eigenschaften von Configuration Items.

Hinweis: Diese Seite ist auf einem Visualizer-Sekundärserver deaktiviert.

Registerkarte "Filter"

Erstellt, bearbeitet und löscht Filter zur Analyse von Configuration Items.

Hinweis: Diese Seite ist auf einem Visualizer-Sekundärserver deaktiviert.

Registerkarte "Symbolkonfiguration"

Ordnet dem entsprechenden Symbolbild eine CI-Familie zu, wenn CMDB Visualizer von Version r11.2 auf r12.5 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 suchen Sie ein ermitteltes Asset und fügen es hinzu:

1. Zeigen Sie die Seite "Configuration Items - Liste" an.
Wird die Liste nicht im rechten Fenster angezeigt, erweitern Sie den Knoten "Konfigurationselemente" in der Baumstruktur "Navigation", und klicken Sie auf "Alle".
2. Klicken Sie auf die Schaltfläche "Ermittelte Anlagen".
Das Fenster "Ermittelte Assets - Suche" wird angezeigt.
3. Klicken Sie auf "Suchen". Eine Liste der ermittelten Anlagen wird nun angezeigt.
4. 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.
5. Füllen Sie alle verbleibenden Felder aus, die für das neue Konfigurationselement von Bedeutung sind. Klicken Sie anschließend auf "Fortfahren".
Hinweis: Für das Erstellen eines Configuration Items werden nur die Werte "Name" und "Klasse" benötigt.
6. 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 Konfigurationselement speichern und anzeigen möchten.
7. 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 Service Desk Manager 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

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.

Jeder dieser Ansätze hat unterschiedliche Stärken und Schwächen.

Weitere Informationen:

[MDR-basierte Abstimmung](#) (siehe Seite 577)

[Identifizieren und Lösen von mehrdeutigen CIs](#) (siehe Seite 579)

[Überprüfen und Ändern von eingehenden Daten mit dem Transaktionsarbeitsbereich \(TWA\)](#) (siehe Seite 592)

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 Service Desk Manager 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 CMDB. Wenn das MDR seine föderierten Asset-IDs wiederverwendet, kann es unabsichtlich zu einer CI-Datenüberlagerung kommen.

Weitere Informationen:

[MDR-Abstimmungs-Methodologie](#) (siehe Seite 577)

[MDR-Abstimmungsattribute](#) (siehe Seite 578)

MDR-Abstimmungs-Methodologie

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 Service Desk Manager, 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 keine ID oder föderierten identifizierenden Attribute angegeben werden, verwendet die CI-Transaktion die Identifikationsattribute, wie im vorherigen Abschnitt beschrieben.

MDR-Abstimmungsattribute

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 Lösen 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 Service Desk Manager 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.

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 mehrdeutiger 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 Sie die identifizierenden Merkmale.
 - Schließen Sie ein CI aus der Mehrdeutigkeitsverwaltung aus.
 - Lehnen Sie eine CI Aktualisierung ab, indem Sie das CI deaktivieren.
 - Ersetzen eines CIs

Weitere Informationen:

[Beispiel für CI-Mehrdeutigkeit](#) (siehe Seite 579)

[Identifizieren mehrdeutiger CIs und Überprüfen der Gültigkeit ihrer identifizierenden Attribute](#) (siehe Seite 581)

[Lösen von mehrdeutigen CIs](#) (siehe Seite 589)

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 582)

[Anzeigen mehrdeutiger Transaktionen über die Registerkarte "Administration"](#) (siehe Seite 587)

[Anzeigen mehrdeutiger CIs über das Scoreboard](#) (siehe Seite 588)

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 Service Desk Manager 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 Service Desk Manager-Webclient und navigieren Sie zu den Listen der mehrdeutigen CIs oder mehrdeutigen CI-Transaktionen, um die Mehrdeutigkeit zu verwalten.

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 585).

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-Schlüsselwort:	Werte	Hinweise
-m	(keine)	twa, ci, all	(Erforderlich) Nur Befehlszeile twa = Mehrdeutigkeit nur für TWA berechnen. ci = Mehrdeutigkeit nur für Cls berechnen. all = Mehrdeutigkeit für Cls 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	Konfigurationselement	<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.

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).

Anzeigen mehrdeutiger CIs über das Scoreboard

Nach dem Ausführen des Dienstprogramms "cmdb_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 Service Desk Manager-Scoreboard den Ordner "CMDB"
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).

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 Benutzer 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.

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 Service Desk Manager-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 auch die CI-Transaktionen validieren, um die Erstellung neuer CIs zu vermeiden, wenn ein vorhandenes CI aktualisiert werden sollte. 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 Sie die identifizierenden Attribute.
 - Geben Sie das Ziel-CI an.

Weitere Informationen:

[Beispiel für CI-Transaktionsmehrdeutigkeit](#) (siehe Seite 594)

[Identifizieren von mehrdeutigen CI-Transaktionen](#) (siehe Seite 596)

[Lösen von mehrdeutigen CI-Transaktionen](#) (siehe Seite 597)

[Verwalten bereitgestellter Transaktionen](#) (siehe Seite 598)

[Transaktionsarbeitsbereich](#) (siehe Seite 599)

[Auffüllen des Transaktionsarbeitsbereichs](#) (siehe Seite 601)

[Aktualisieren von Daten im TWA über die Web-Schnittstelle](#) (siehe Seite 613)

[Manuelle Abstimmung](#) (siehe Seite 615)

[Laden von Transaktionen in die CMDB](#) (siehe Seite 617)

[TWA-Administration](#) (siehe Seite 619)

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)

Folgende vier CIs residieren in 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 582) berechnen.

Weitere Informationen finden Sie unter [Überprüfen und Ändern von eingehenden Daten mithilfe des Transaktionsarbeitsbereichs \(TWA\)](#) (siehe Seite 592).

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 Service Desk Manager-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 592).

Transaktionsarbeitsbereich

Mit dem Transaktionsarbeitsbereich (TWA) in CA Service Desk Manager 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 601) 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 606), 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 592).

3. Ändern Sie die Daten. Sie können den TWA über die folgenden Quellen ändern:

CA Service Desk Manager-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 Service Desk Manager 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 620).
- 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

Es ist Ihre Aufgabe, den Transaktionsarbeitsbereich aufzufüllen. Wir empfehlen Ihnen, sich mit CA Services zur weiteren Hilfestellung bei diesem Prozess in Verbindung zu setzen.

Eingabedaten können aus zahlreichen Quellen stammen, z. B.:

- CA-Produkte wie CA Cohesion ACM oder CA Spectrum, die Daten mittels GRLoader importieren
- Jedes andere MDR, das Daten mittels GRLoader importiert
- CA CMDB (in Produktion)
- Microsoft Excel-Kalkulationstabellen
- Datenbanktabellen
- Ein von einem Anbieter ausgewähltes ETL-Tool

Weitere Informationen finden Sie unter [Datenbankeinschränkungen](#) (siehe Seite 623).

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 606). Wird GRLoader im Modus "In TWA laden" ("-littwa" oder "-littwar") ausgeführt, werden die Datenwerte nicht validiert.

Der Parameter "-littwai" (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 -l ttw
```

Weitere Informationen:

[XML-Eingabe](#) (siehe Seite 603)

[Suche](#) (siehe Seite 604)

[Datumsformat](#) (siehe Seite 605)

[EMPTY](#) (siehe Seite 605)

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 607)

[TWA-SQL-Spaltennamen](#) (siehe Seite 608)

[Einfügen neuer Datensätze in den TWA](#) (siehe Seite 610)

[Verwenden von ODBC-Treibern](#) (siehe Seite 611)

[CI-Kennungen im TWA](#) (siehe Seite 611)

[Festlegen des Transaktionsstatus](#) (siehe Seite 612)

[Freigeben von Tabellen für CA Service Desk Manager](#) (siehe Seite 612)

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 619).

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 Service Desk Manager 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 Service Desk Manager 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 Service Desk Manager-Server zur gleichen Zeit durchgeführt werden können, in der das Tool zur Massенbearbeitung ausgeführt wird.

Unbedingt beachten

- Nur CA Service Desk Manager-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 Service Desk Manager-Servers ändern. IDs von 2.000.000.001 bis etwa 4 Milliarden sind für die Verwendung von CA Service Desk Manager 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"
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 Service Desk Manager

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 614)

[Verwalten von mehrdeutigen CI-Transaktionen](#) (siehe Seite 615)

[Manuelle Abstimmung](#) (siehe Seite 615)

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")

Nachdem Sie eine einzelne Transaktion gespeichert haben, klicken Sie auf die Registerkarte "Abstimmung" für diese Transaktion, um zu überprüfen, dass keine Mehrdeutigkeit bezüglich des geplanten Ziel-CIs vorliegt. Wenn eine Mehrdeutigkeit vorliegt, [geben Sie ein Ziel-CI an](#) (siehe Seite 598). Wenn die Dateneingabe beendet ist, können [das Datenladen simulieren](#), (siehe Seite 606) um die Daten 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 601) 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 598). Sobald Sie mit der Eingabe aller Daten fertig sind, können Sie [das Laden der Daten simulieren](#) (siehe Seite 606), 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 592).

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 mit dem Transaktionsarbeitsbereich \(TWA\)](#) (siehe Seite 592).

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 601) 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 606).

Weitere Informationen:

[So vermeiden Sie Datenregression](#) (siehe Seite 618)

[Filtern nach Change-Nummer](#) (siehe Seite 619)

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.

WARNUNG! 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 620)
[Archivieren und Löschen des TWA](#) (siehe Seite 621)
[TWA-Befehlsoptionen für GRLoader](#) (siehe Seite 621)
[TWA-Optionen für die GRLoader-Konfigurationsdatei](#) (siehe Seite 622)
[Verwenden des TWA mit CA Cohesion ACM](#) (siehe Seite 623)
[Datenbankeinschränkungen](#) (siehe Seite 623)

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 Service Desk Manager 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 Service Desk Manager 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.

-I

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 R008739 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 benutzerdefinierte 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 624)

[Ändern der Familie/Klasse eines einzigen Konfigurationselements](#) (siehe Seite 625)

[Ändern der Familie/Klasse einer Liste von Konfigurationselementen](#) (siehe Seite 625)

[Ändern von Konfigurationselement-Familien oder Konfigurationselement-Klassen mit GRLoader](#) (siehe Seite 626)

[Erweitern von CA CMDB](#) (siehe Seite 627)

CA CMDB-Strukturen für Familie und Klasse

In CA CMDB stehen Ihnen standardmäßig bestimmte Konfigurationselement-Familien sowie deren CI-Klassen zur Verfügung.

Hinweis: Weitere Informationen zur Standard-Struktur für Familien/Klassen in CA CMDB finden Sie hier: *CA CMDB Technisches 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 Konfigurationselements

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 Konfigurationselement aus, das Sie ändern möchten.
2. Klicken Sie auf "Bearbeiten".
Die Seite "Konfigurationselement aktualisieren" öffnet sich.
3. Ändern Sie den Wert "Klasse" des Konfigurationselements. Legen Sie eine Klasse für das Konfigurationselement 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 Konfigurationselementen

Sie können die Familie und Klasse einer Liste von CIs ändern.

So ändern Sie die Familie/Klasse einer Liste von Konfigurationselementen:

1. Klicken Sie unter "Konfigurationselement-Liste" auf "Filter anzeigen".
2. Füllen Sie ein oder mehrere der Suchfelder aus, und suchen Sie die Konfigurationselemente, die Sie bearbeiten möchten.
3. Klicken Sie auf "Suche".
Unter "Konfigurationselement-Liste" werden nun alle Konfigurationselemente angezeigt, die Ihren Suchkriterien entsprechen.
4. Klicken Sie auf "In Liste bearbeiten".
Unter "Konfigurationselement-Liste" werden nun alle Felder angezeigt, in denen Sie für sämtliche ausgewählte Konfigurationselemente 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 Konfigurationselement-Liste, werden die aktualisierten Konfigurationselemente angezeigt

Ändern von Konfigurationselement-Familien oder Konfigurationselement-Klassen mit GRLoader

Sie können die Familie und Klasse für ein CI mit GRLoader ändern.

So ändern Sie Konfigurationselement-Familien oder Konfigurationselement-Klassen mit GRLoader:

1. Generieren Sie einen XML-Code, um das Konfigurationselement-Attribut zu ändern.
2. Öffnen Sie in GRLoader das Konfigurationselement, das Sie ändern möchten.
3. Führen Sie nun den XML-Code in GRLoader aus, um das Konfigurationselement-Attribut zu ändern.

Die Familie und Klasse für ein CI werden geändert.

Beispiel: Festlegen der Klasse eines geöffneten Konfigurationselements auf "Dokument"

Im folgenden Beispiel sehen Sie ein XML-Fragment, das für ein geöffnetes Konfigurationselement die Klasse *Dokument* festlegt.

```
<ci>
  <name>Dokument Nr. 1
  <class>Dokument
</ci>
```

Wichtig! Versuchen Sie nicht, gleichzeitig Familie und Klasse eines Konfigurationselements zu ändern. Möchten Sie beides ändern, müssen Sie zwei separate Konfigurationselement-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 629).
- Erweitern aller CI-Familien durch Hinzufügen eines allgemeinen Attributs. Weitere Informationen finden Sie unter [Hinzufügen allgemeiner Attribute](#) (siehe Seite 629).
- 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 631).
- Hinzufügen einer neuen Familie mit Hilfe einer vorhandenen Erweiterungstabelle und ihrer Attribute. Eine neue Familie bietet eine alternative Möglichkeit zur Organisation oder Klassifizierung von CIs. Weitere Informationen finden Sie unter [Definieren einer neuen CI-Familie](#) (siehe Seite 631).

- Wenn die vorhandene Klassen- oder die Familienstruktur nicht Ihren Anforderungen entspricht, können Sie mit einem Mindestsatz 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 632).

Wichtig: Das Erweitern von CA CMDB setzt besondere Kenntnisse von CA CMDB-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 629).

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 630) 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 Service Desk Manager-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 635).

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 636).

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 632) 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 631) 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 632) 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 631) 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

Die Verfahren zum Definieren neuer Familien und Klassen finden Sie im vorherigen Abschnitt.

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 634) 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.htmlpl** 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 635) fort. Um Metadaten für ein neues Attribut auf dem Formular zu definieren, fahren Sie mit dem Abschnitt [Erstellen von Metadaten](#) (siehe Seite 636) 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.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 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 630).

Die Strukturen für Ihre neue Erweiterungstabelle sind jetzt eingerichtet. Fahren Sie mit [Definieren einer neuen CI-Familie](#) (siehe Seite 631) 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.html**.
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.html**.
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.html**.
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.

Kapitel 15: 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 641)

[MDR Launcher](#) (siehe Seite 643)

[Definieren einer URL zum Starten eines MDR](#) (siehe Seite 644)

[Einrichten eines CA APM-MDR-Providers](#) (siehe Seite 646)

[Starten im Kontext von CA CMDB an CA APM](#) (siehe Seite 647)

[Eigenschaften von Configuration Items, die MDR-Zusammenschluss unterstützen](#) (siehe Seite 647)

[CA Cohesion ACM MDRs](#) (siehe Seite 650)

[CI-Import in CA CMDB mit GRLoader](#) (siehe Seite 654)

[Namenskonventionen und Einschränkungen für Configuration Items](#) (siehe Seite 655)

[Namenskonventionen für system_name](#) (siehe Seite 656)

[Verwenden des CMDBf-Viewers](#) (siehe Seite 657)

[Aktualisieren von Metadateiendateien für die CMDBf-Zuordnung](#) (siehe Seite 658)

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 Service Desk Manager?

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 Service Desk Manager

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.

So richten Sie einen CA APM-MDR-Provider ein:

1. Melden Sie sich in der Web-Schnittstelle als Administrator an.
2. Klicken Sie auf die Registerkarte "Administration". Wählen Sie im Administrationsbrowser die Option CA CMDB >, "MDR-Management" > "MDR-Liste" aus.
3. Klicken Sie auf "Neu erstellen", um das CA APM-MDR festzulegen.
Die MDR-Providerdefinition wird angezeigt.
4. 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 r12.5 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.

5. 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 Benutzer 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-r12.5. 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:

- ein 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 r12.5 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-Zielsystem 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.

Name der Schaltfläche

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

Gemeinsamer geheimer Schlüssel

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*.

CI-Import in CA CMDB mit GRLoader

Wenn Sie ein CI mit GRLoader laden, müssen in der XML die folgenden Felder ausgefüllt werden, damit MDR gestartet werden kann:

- <mdr_class>
- <mdr_name>
- <federated_asset_id>

Die Werte für <mdr_name> und <mdr_class> in der XML müssen genau 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.

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 Apache1aus  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 Service Desk Manager 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 Attributvergleichen 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 659)

[Ausblenden von Attributen des MDR-Providers](#) (siehe Seite 660)

[Definieren von MDR-Attributen ohne CA CMDB-Entsprechungen](#) (siehe Seite 661)

[Definieren von Metadaten des CMDBf-Datenanbieters](#) (siehe Seite 661)

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 16: Change Management

Dieses Kapitel enthält folgende Themen:

[Change Management in CA Service Desk Manager](#) (siehe Seite 663)
[Change-Management-Komponenten](#) (siehe Seite 664)
[Anzeigen des Change-Kalenders](#) (siehe Seite 665)
[CAB-Zuständigkeiten](#) (siehe Seite 666)
[Zuständigkeiten des Change Managers](#) (siehe Seite 667)
[Definieren der Aufgaben für die Rolle des Change Managers](#) (siehe Seite 669)
[Change-Kategorien, Status und Risikoebenen](#) (siehe Seite 670)
[Anzeigen des Change-Scoreboards](#) (siehe Seite 671)
[Definieren von gespeicherten Abfragen für Changes](#) (siehe Seite 671)
[Konfigurieren von Change Manager-Optionen](#) (siehe Seite 673)
[Change-Kalender](#) (siehe Seite 673)
[So planen Sie Changes:](#) (siehe Seite 688)
[So planen Sie Change-Fenster:](#) (siehe Seite 693)
[Konfliktanalyse und Konflikterkennung](#) (siehe Seite 697)
[CA Workflow-Visualisierung](#) (siehe Seite 698)
[Change-Management-Prozessdefinition für CA Workflow](#) (siehe Seite 700)
[CAB-Konsole und Berichterstattung](#) (siehe Seite 721)
[Risikobewertung](#) (siehe Seite 727)
[Auswirkungs-Explorer](#) (siehe Seite 731)

Change Management in CA Service Desk Manager

Change Management für CA Service Desk Manager 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-Anfragen 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-Ereignissen](#) (siehe Seite 673), einschließlich aller geplanten, fehlgeschlagenen und laufenden Change-Anforderungen für CIs und Services in einer konfigurierbaren [Kalenderansicht](#) (siehe Seite 688), an. Der Kalender zeigt darüber hinaus Ausfallfenster an, in denen keine Changes erfolgen dürfen. Benutzer 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 694) 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-Anfragen an. Diese Funktion wird vom Change Manager verwendet.

CAB-Konsole und Berichterstattung

Zeigt ein [Dashboard](#) (siehe Seite 721) an, das schnelle Online-Genehmigungen der Changes, die eine CAB-Genehmigung erfordern, ermöglicht.

In CA Service Desk Manager kann der Change Manager Berichte mit Details über die vorgeschlagenen Change-Anfragen für die CAB-Überprüfung generieren und diese Berichte elektronisch an alle CAB-Mitglieder verteilen.

Hinweis: Benutzer 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 jede abgesendete Change-Anfrage 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 731) auf Anfrage zu ermöglichen. Diese Funktion wird vom Change Manager verwendet.

Anzeigen des Change-Kalenders

CA Service Desk Manager 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-Anfragen 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 667)

Funktionsweise der CAB-Prozessdefinitionen

Die CAB ist dafür verantwortlich, alle größeren Changes an Produktionssystemen zu überprüfen. CAB-Mitglieder werden darüber benachrichtigt, dass eine Change-Anfrage ihre Genehmigung erfordert, und sie führen folgende Schritte aus:

1. Sie lassen alle Change-Anfragen auflisten, die das CAB überprüfen muss
2. Sie öffnen die CAB-Konsole und zeigen der Informationen an, die in der Anfrage enthalten sind
3. Sie prüfen Geschäftsrechtfertigung, Implementierungsplan, Configuration Items und die begleitende, mit der Anfrage 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 die Change-Anfrage aktualisiert wurde.

Weitere Informationen:

[CAB-Zuständigkeiten](#) (siehe Seite 666)

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-Anfragen 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 Anfrager, zu benachrichtigende Personen, Genehmigende, Implementierer und Support-Gruppen

Weitere Informationen:

[Funktionsweise der Rolle des Changes Managers](#) (siehe Seite 668)

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-Anfragen 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-Anfragen für die CAB-Überprüfung und das elektronische Verteilen der Berichte an alle CAB-Mitglieder
4. Durchführen von Echtzeit-Überprüfungen aller Change-Anfragen 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 Service Desk Manager 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. Benutzer können ihre zugewiesenen und nicht zugewiesenen Datensätze nach Priorität sortiert anzeigen.

So zeigen Sie das Change-Scoreboard an:

1. Navigieren Sie im CA Service Desk Manager-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 "Suche".
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 Service Desk Manager 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 721)

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 Liste der Optionen 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-Ereignissen mit Zeiten für den Beginn und das Ende der Implementierung. Mit dieser Kalenderansicht des Change-Zeitplans können Analytiker und Manager rasch erkennen, wann Ereignisse 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 "Ausfallfenster". Navigieren Sie tiefer in eine Wochen- oder Tagesansicht, oder zeigen Sie Einblendinformationen an, um die einzelnen Fensterdetails zu sehen.

Weitere Informationen:

[Hinzufügen von Ablaufplaninformationen zu einem Change – CA](#) (siehe Seite 674)

[iCalendar-Ereignis-Vorlagen](#) (siehe Seite 674)

[Exportieren von Ablaufplänen in iCalendar](#) (siehe Seite 675)

[Ablaufplan-Ansichten](#) (siehe Seite 676)

[Konfigurieren von Planungsansichten](#) (siehe Seite 678)

Hinzufügen von Ablaufplaninformationen zu einem Change – CA

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 Service Desk Manager benutzt, um neue Changes der Kategorie zu initialisieren.

Startdatum des Ablaufplans

Gibt das Startdatum des Changes an.

Dauer

Gibt die Dauer des Änderungsauftrags 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-Ereignis-Vorlagen

iCalendar-Ereignis-Vorlagen kontrollieren die Informationen, die in das iCalendar-Format exportiert wird.

Die folgenden vordefinierten Vorlagen werden mit CA Service Desk Manager installiert:

- Change-Ablaufplan
- Knowledge-Ablaufplanerstellung
- Knowledge-Ablaufplan abgelaufen

- Knowledge-Ablaufplanüberprüfung
- Knowledge-Ablaufplanstart

Hinweis: Sie können die vordefinierten iCalendar-Ereignisvorlagen 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 Ereignissen. Eine Erhöhung des Standardwerts (1000) könnte zu einer Systeminstabilität führen. Wenn Sie versuchen, mehr Ereignisse zu exportieren als in "SchedExpMaximum" angegeben, erscheint eine Meldung mit einer Ablehnung Ihrer Exportanfrage.

Exportieren von Ablaufplänen in iCalendar

Das iCalendar-Format ist ein Industriestandard zum Austausch von Kalenderinformationen. Er ermöglicht das Importieren von Change-Ablaufplänen in eine Vielzahl von weit verbreiteten Kalenderanwendungen, wie Microsoft Outlook und Lotus Notes.

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 abgespeichert haben, importieren Sie sie über die Schnittstelle des Kalenderprogramms.

Wichtig! Es werden die Daten der aktuellen Ansicht exportiert. Wenn Sie einen benutzerdefinierten 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 Ereignissen. Eine Erhöhung des Standardwerts (1000) könnte zu einer Instabilität des Systems führen. Wenn Sie versuchen, mehr Ereignisdatensätze als in "SchedExpMaximum" angegeben zu exportieren, erscheint die Meldung, dass Ihre Exportanfrage abgelehnt wird.

4. Geben sie den Speicherort ein, wo sie die iCalendar-Datei ablegen wollen.

Eine iCalendar-Datei, die alle Ereignisse der aktuellen Ansicht enthält, wird an dem angegebenen Speicherort abgelegt.

Ablaufplan-Ansichten

CA Service Desk Manager 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.

Diese Ansicht zeigt Changes innerhalb von Gruppen an. Jeder Eintrag enthält einen oder mehrere Changes und Sie können genauere Informationen über die Changes einer Gruppe abfragen, indem Sie den Mauszeiger über diese Gruppe bewegen, durch Drücken von "Alt+Pfeil nach rechts" wenn die Gruppe ausgewählt ist oder durch Klicken auf die Gruppe, um den Inhalt in einer n-Tage-Ansicht 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 Ereignis 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 Ereignis an. Wenn es kein Informationsfenster gibt, navigiert es zum nächsten höheren Datum (vergleichbar mit "Umschalt+Pfeil nach rechts").

Pfeiltaste nach unten

Navigiert zum nächsten Ereignis in der aktuellen Zelle. Wenn es keine Ereignisse in der aktuellen Zelle gibt, oder wenn bereits das letzte Ereignis ausgewählt ist, navigiert es zum Datum in der nächsten Zelle nach unten (vergleichbar mit "Umschalt+Pfeil nach unten").

Pfeiltaste nach oben

Navigiert zum vorherigen Ereignis in der aktuellen Zelle. Wenn kein Ereignis 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\`

"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 Benutzer 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 Benutzer eine Ansicht mit einem oder mehr Tagen außerhalb des Datenauswahlbereichs des Suchfilters auswählt. Bei der Festlegung des Werts auf 0 muss der Benutzer 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 Service Desk Manager 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 Service Desk Manager nur die erste maxGroups-1 an und ersetzt die letzte durch einen ["..nn zusätzliche Changes"-Hyperlink](#), über den der Benutzer 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 Ereignissen 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 Service Desk Manager-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-CIs 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 Service Desk Manager 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 "#FF000" 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 Ereignisse im Ablaufplan. Ändern Sie diese Funktion, wenn Sie neue Gruppenobjekte anzeigen möchten. Die vordefinierten Gruppenobjekte werden standardmäßig angezeigt.

CA Service Desk Manager ruft "setSchedEvents()" je einmal für jedes Objekt (Change oder Knowledge-Dokument) auf, das über den Suchfilter des Ablaufplans ausgewählt wurde. Die Funktion erstellt Ereignisse für das Objekt durch Aufrufen einer zweiten Funktion, schedEvent(), und deren Übergabe an die Gruppen-ID, das Startdatum und Enddatum des Ereignisses.

Die Funktion kann eine beliebige Anzahl von Ereignissen (einschließlich Null) für ein Objekt erstellen. Die Standardfunktion "setSchedEvents()" für den Change-Kalender ("list_chgsched.html") erstellt je ein Ereignis 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 Ereignis 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 Änderungsauftrag.
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 Service Desk Manager 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 679)

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 *Ausfallfenster* 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 Service Desk Manager 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.

Ausfallfenster

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 Unternehmensereignis oder eine kritische Geschäftszeit, wie z. B. das Ende des Geschäftsjahres, verweisen. Im Allgemeinen sollten geplante Changes nur außerhalb von Sperrfenstern auftreten.

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-Ausfallfensters

Das folgende Beispiel zeigt, wie Sie ein Ausfallfenster erstellen, das darauf hinweist, dass Changes nicht in dieser bestimmten Zeitperiode geplant werden dürfen. Dieses Ausfallfenster soll 48 Stunden dauern und jeden Freitag um 18.00 Uhr beginnen.

So erstellen Sie ein Ausfallfenster:

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_Ausfallfenster** als Fensternamen ein.
- b. Wählen Sie den Typ "Ausfall" 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 Ausfallfenster 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 Ausfallfenster.
5. Aktualisieren Sie die "Change-Fenster - Liste".
6. Öffnen und aktualisieren Sie den Change-Kalender.

Das Ausfallfenster wird im Ablaufplan angezeigt.

Erstellen eines globalen Wartungsfensters

Über die Seite "Fenster - Liste" können Sie ein globales Wartungsfenster erstellen und anzeigen.

So erstellen Sie ein globales Wartungsfenster:

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 r12.5".

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 r12.5" 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 Service Desk Manager-Change-Management-Funktionen:
 - Risikobewertungsumfrage
 - Geschäftsfall
 - Konfliktanalyse
 - Auswirkungsanalyse
 - Schließungscodes
 - Statuscodes
 - Change-Typ
 - CAB- und CAB-Zustimmungs-Flags

Weitere Informationen:

[CA Workflow](#) (siehe Seite 279)

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 702) zu Aktivitätsknoten, Unteraktivitäten und Benachrichtigungen.
2. Erstellen Sie die [CAB- und Implementierungsgruppen](#) (siehe Seite 704), die für die Verwaltung des Change-Vorgangs verantwortlich sind.
3. [Erstellen Sie Kontakte](#) (siehe Seite 705), und weisen Sie diese den CAB- oder Implementierungsgruppen zu.
4. [Konfigurieren Sie E-Mail-Benachrichtigungen](#) (siehe Seite 703) für die Change Management-Vorgangsdefinition.
5. Wenn Sie nicht den standardmäßigen Tomcat-Server-Port 8090 verwenden, [konfigurieren Sie den Tomcat-Server](#) (siehe Seite 706) für die entsprechende Kommunikation zwischen CA Workflow und CA Service Desk Manager.
6. [Konfigurieren Sie einen oder mehr Change-Kategorien](#) (siehe Seite 707) die Change-Management-Vorgangsdefinition zu benutzen.
7. [Installieren Sie die Option "Kategorie-Standardwerte"](#) (siehe Seite 708) 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 Service Desk Manager- und CA EEM-Namen übereinstimmen.
- Der Gruppenname in CA Service Desk Manager muss außerdem mit dem Gruppenordnernamen in CA EEM übereinstimmen.
- Jede Gruppe muss mehr als ein Mitglied haben.
- Die Gruppenmitglieder in CA Service Desk Manager und CA EEM stimmen überein. Wenn z. B. die CAB-Gruppe von CA Service Desk Manager vier Mitglieder hat, hat die CAB-Gruppe von CA EEM dieselben Mitglieder.

Hinweis: Informationen zum Erstellen von CA Service Desk Manager- 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 Service Desk Manager:
 - **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:

[Zuweisen von CAB-Gruppen](#) (siehe Seite 724)

[Verwalten von CAB-Gruppen](#) (siehe Seite 722)

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 704) 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 Service Desk Manager- 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 Service Desk Manager 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 auf Sie 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 Service Desk Manager 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 Service Desk Manager-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 Service Desk Manager 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.

CI

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 713) ab, die beschreibt, wie sich der Change auf Server, Anwendungen und Benutzer 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 714) 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 715) 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 714).

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 718) 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 720) (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:

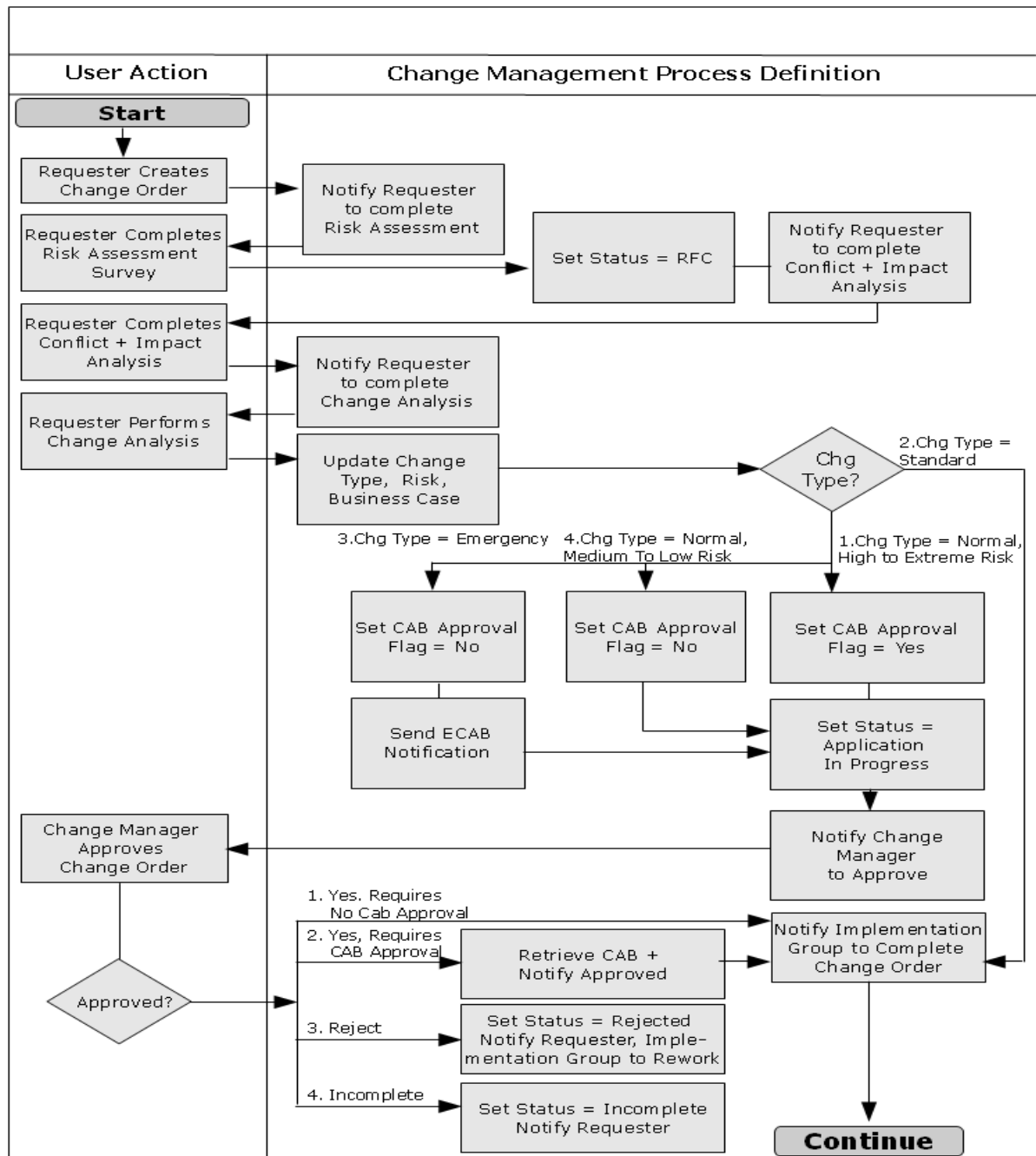
[Einrichten der Change Management-Vorgangsdefinition](#) (siehe Seite 702)

[So implementieren Sie die Risikoumfrage:](#) (siehe Seite 728)

[Anzeigen von Standardrisikoumfragen](#) (siehe Seite 728)

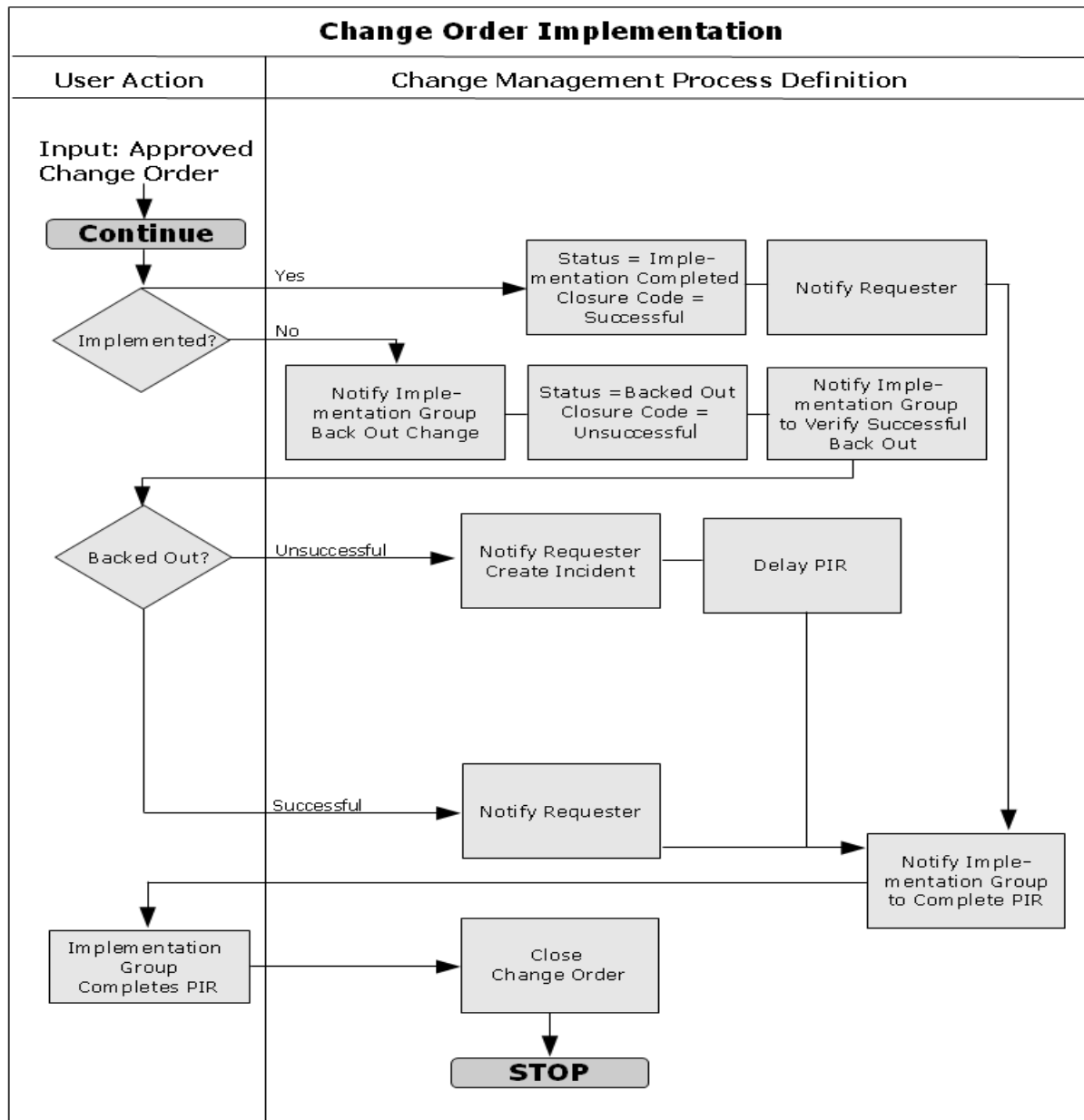
Verwalten von Change-Genehmigungen durch die CM-Vorgangsdefinition

Das folgende Diagramm zeigt, wie die [Change Management-Vorgangsdefinition](#) (siehe Seite 708) 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 708) 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 730)

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 731)

[Starten von CMDB Visualizer im Auswirkungs-Explorer](#) (siehe Seite 734)

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 667)

[CAB-Zuständigkeiten](#) (siehe Seite 666)

[CAB-Genehmigungen](#) (siehe Seite 724)

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.

So implementieren Sie einen Change

1. Melden Sie sich als Mitglied der Implementierungsgruppe bei CA Service Desk Manager an, und öffnen Sie den Change.

Das Fenster "Change - Detail" wird angezeigt.

2. Klicken Sie auf der Registerkarte "Workflow-Aufgaben" auf die Verknüpfung "Implement Change Order" (Change implementieren).

Die Seite "Aufgabenliste" wird angezeigt.

3. Klicken Sie auf der Registerkarte "Aufgaben" auf die Verknüpfung "Perform" (Ausführen).

Die Seite "Perform Tasks" (Aufgaben ausführen) wird angezeigt.

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 angezeigt.

7. Klicken Sie auf der Registerkarte "Aufgaben" auf die Verknüpfung "Perform" (Ausführen).

Die Seite "Implementation Complete" (Implementierung vollständig) wird angezeigt.

8. Beantworten Sie die Fragen auf der Registerkarte "Impl 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 "Changes – 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 Service Desk Manager 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-Anfragen kann das CAB die Anfrage bearbeiten, indem es sie direkt genehmigt oder an eine geeignete Gruppe eskaliert bzw. verweist.

Der Change Manager kann die Funktionalität von CA Service Desk Manager 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 Service Desk Manager finden Sie unter "Erzeugen von Berichten" in der *Online-Hilfe*.

Weitere Informationen:

[Verwalten von CAB-Gruppen](#) (siehe Seite 722)

[Zuweisen von CAB-Gruppen](#) (siehe Seite 724)

[CAB-Genehmigungen](#) (siehe Seite 724)

[Ändern der CAB-Konsoleneigenschaften](#) (siehe Seite 725)

[Change Management-Berichterstattung](#) (siehe Seite 726)

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 ($\geq$).
6. Klicken Sie auf "OK".

Die ausgewählten Kontakte werden zur Mitgliederliste auf der rechten Seite verschoben.

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 Service Desk Manager" > "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:

[Change- und Issue-Kategorien](#) (siehe Seite 303)

[Area Defaults](#) (siehe Seite 444)

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 725)

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-Berichterstellung

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-Anfragen 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 Benutzer 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 Benutzer die geeigneten Antworten aus und sendet die Befragung ab. Die evaluierte Risikoebene basiert auf den Schweregraden der Antworten, die vom Benutzer ausgewählt werden.

Weitere Informationen:

[Anzeigen von Standardrisikoumfragen](#) (siehe Seite 728)

[Bereitstellen eines Risikoumfrage-Beispiels](#) (siehe Seite 729)

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 Service Desk Manager 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 Benutzer 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 Benutzer 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=D0_RISK_SURVEY+KEEP.UsingURL=1
```

hostname

Gibt den Hostnamen des CA Service Desk Manager-Servers an.

port

Gibt den Port an, an dem CA Service Desk Manager 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 verbundenen Changes an.

Das folgende Beispiel zeigt eine Beispiel-URL:

```
http://hostname:8080/CAisd/pdmweb.exe?CNT_ID=21A7CC606A3011DEA39AA8010000A800+CRID=400009+OP=D0_RISK_SURVEY+KEEP.UsingURL=1
```

Wichtig! Wenn Sie den Parameter *KEEP.UsingURL=1* nicht der dynamischen URL hinzufügen, erhält der Benutzer 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 instanziiieren.

6. Als ein Teil des CA Workflow-Prozesses wird ein Benutzer einer Aufgabe zugewiesen, um die Risikoumfrage abzuschließen. Der Benutzer klickt auf die URL, wie bereits beschrieben.
7. Der Benutzer loggt sich über die URL in CA Service Desk Manager ein und wird direkt zur Risikoumfrage für den Change geleitet.
8. Der Benutzer 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 732)

[Untersuchen von angehängten CIs](#) (siehe Seite 732)

[Anzeigen von CIs in Auswirkungs-Explorer](#) (siehe Seite 733)

[Hinzufügen von verwandten CIs zu Changes](#) (siehe Seite 733)

[Anzeigen der Liste der nachfolgenden Elemente des CI](#) (siehe Seite 734)

[Starten von CMDB Visualizer im Auswirkungs-Explorer](#) (siehe Seite 734)

[Konfigurieren von Auswirkungs-Explorer](#) (siehe Seite 735)

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 17: Verwalten von CA Business Intelligence-Berichten

Dieses Kapitel enthält folgende Themen:

[CA Business Intelligence-Berichte](#) (siehe Seite 737)
[Berichterstellungsszenarios](#) (siehe Seite 738)
[Berichtskomponenten](#) (siehe Seite 739)
[Berichtsdatenflussdiagramm](#) (siehe Seite 742)
[Anzeigen von Berichten in InfoView](#) (siehe Seite 743)
[Sicherheit und Autorisierung](#) (siehe Seite 743)
[Verweisen eines vorhandenen CA Business Intelligence-Servers auf einen CA Service Desk Manager-Server](#) (siehe Seite 748)
[Einrichten der Datenaufteilungssicherheit für die Berichterstellung](#) (siehe Seite 751)
[Replizierte Datenbank für Offline-Berichterstellung](#) (siehe Seite 754)
[Rollenbasierte Berichte](#) (siehe Seite 754)
[Webbasierte Berichte](#) (siehe Seite 764)
[Dashboard-Berichte](#) (siehe Seite 768)
[Ad-hoc-Berichte](#) (siehe Seite 769)
[KPIs \(Kritische Prozess-Indikatoren\)](#) (siehe Seite 777)
[Schreiben von CA Business Intelligence-Berichten](#) (siehe Seite 789)

CA Business Intelligence-Berichte

CA Business Intelligence ist eine webbasierte Komponente, die die Business Objects-Technologie mit CA Service Desk Manager und verschiedenen verbreiteten Datenquellen vereint, z. B. SQL Server, Oracle und Open Database Connectivity (ODBC).

CA Business Intelligence verwendet BusinessObjects Enterprise XI als Standard-Berichtssystem. Vordefinierte Berichte werden für CA Service Desk Manager, Knowledge-Management und Support-Automatisierung bereitgestellt.

Mit CA Business Intelligence können Benutzer die folgenden Aufgaben ausführen:

- 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 Benutzer
- Planen der Ausführung von Berichten zu bestimmten Zeiten
- Verwenden von Dashboard-Berichten zur Überwachung von täglichen Vorgängen für alle CA Service Desk Manager-Ticket-Typen.

Hinweis: Der Zugriff auf die Berichterstellung ist durch die CA Service Desk Manager-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 Service Desk Manager können autorisierte Benutzer für ihre Rolle definierte Berichte anzeigen und dann auf die Schaltfläche "InfoView" klicken, um ihre persönlichen Berichte in BusinessObjects InfoView zu verwalten. CA Service Desk Manager 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 Service Desk Manager, 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 Benutzer, die problemlos einfache Berichte erstellen möchten, ohne Abfragen zu schreiben.

- **Dashboard-Berichterstellung:** Über Dashboard-Berichte können Sie laufend den Status für CA Service Desk Manager-Ticket-Typen (Anfrage/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 Service Desk Manager 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 <cabl> 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 Service Desk Manager entwickelt oder bereitgestellt.

Sie können die folgenden Komponenten verwenden, um die CA Business Intelligence-Berichtsumgebung zu verwalten, zu überwachen und zu konfigurieren:

- **CA Service Desk Manager Datenbank/Domsrvr/ODBC-Treiber:** Die Berichtsdaten werden in einer SQL Server- oder Oracle-CA Service Desk Manager-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 Service Desk Manager verbunden ist. Alle CA Service Desk Manager-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 Service Desk Manager arbeitet.

Hinweis: Weitere Informationen zur Absicherung von Datenpartitionen für Ihre Berichtsumgebung finden Sie unter [Absichern von Datenpartitionen bei der Berichterstellung](#) (siehe Seite 743).

- **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 Benutzerzugriffs- sowie Ordnerberechtigungen für InfoView zuweisen. Benutzer-Genehmigungen, Rollen und Authentifizierungsoptionen müssen mit der CMC eingerichtet werden.

Hinweis: Bevor Sie CA Business Intelligence verwenden, müssen Sie Benutzerberechtigungen, Rollen und Authentifizierungsoptionen einrichten. Weitere Informationen über Sicherheitseinstellungen finden Sie unter [Sicherheit und Authentifizierung](#) (siehe Seite 743).

- **BusinessObjects-Universum:** Bezeichnet die Klassen (Tabellen] und Objekte (Spalten), die in Berichten verwendet werden. Das CA Service Desk Manager-Universum wird während der Installation ebenfalls installiert und konfiguriert. Sobald die Installation abgeschlossen ist, wird verschiedenen Gruppen und Benutzern die Verbindung mit einem Universum in CA Service Desk Manager zugewiesen.
- **Designer:** Dies ist eine Komponente in BusinessObjects, mit der Sie das CA Service Desk Manager-Universum ändern können, welches eine Metaebene zwischen CA Service Desk Manager-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 Service Desk Manager- 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 Service Desk Manager-Benutzern 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 ist auf Benutzer zugeschnitten, die problemlos einfache Berichte erstellen möchten, ohne Abfragen zu schreiben.

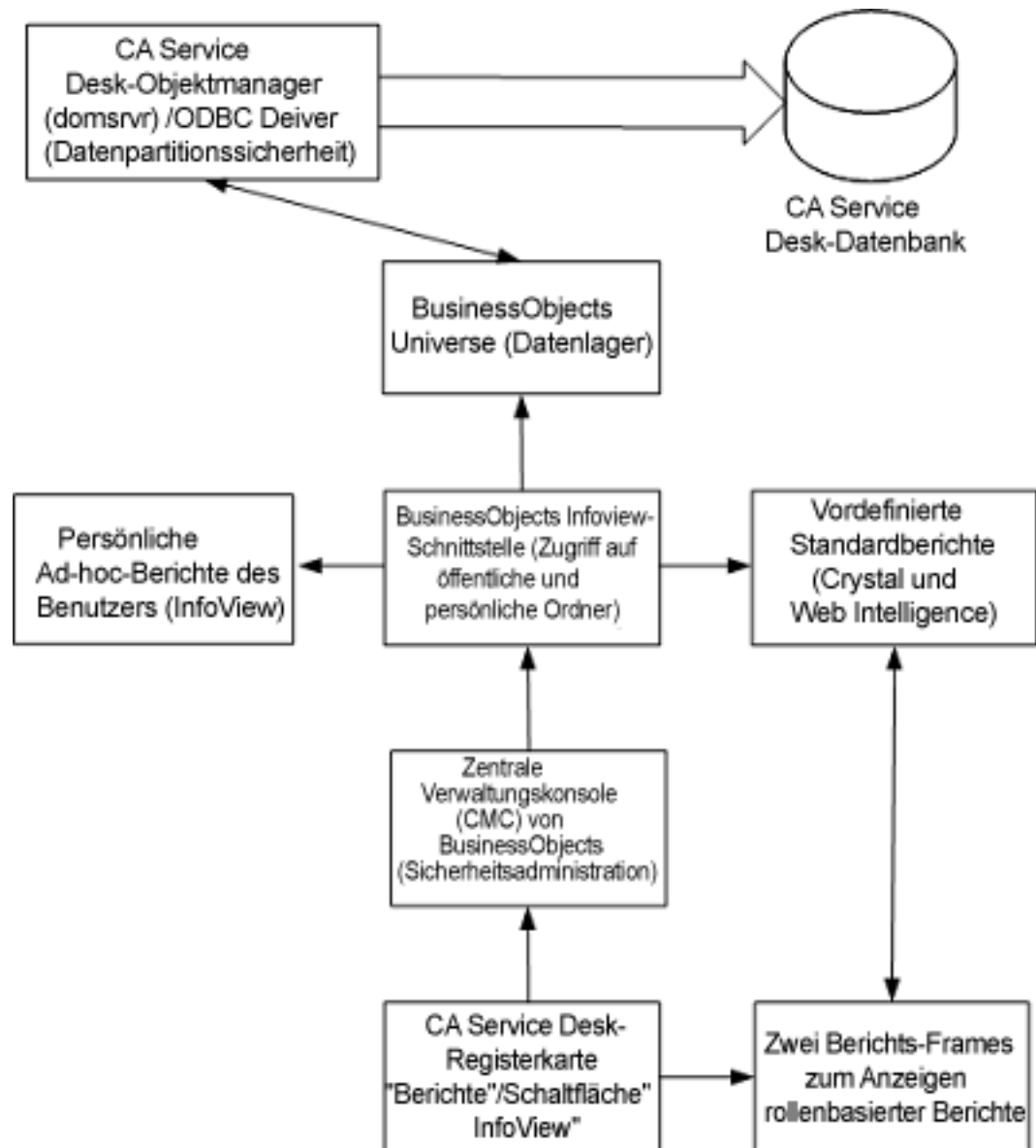
Hinweis: Beispiel für die Anwendung von Ad-hoc-Berichten finden Sie unter [Ad-Hoc-Berichte](#) (siehe Seite 769).
- **Dashboard-Berichte:** Über Dashboard-Berichte können Sie laufend den Status für CA Service Desk Manager-Ticket-Typen (Anfrage/Incident/Problem, Change oder Issue) in BusinessObjects InfoView überwachen. Jeder Bericht enthält Analysedaten über Mitarbeiter, die bei der Arbeit mit aktiven Tickets beste Leistungen erbringen. So können Sie den Fortschritt überwachen.

- **CA Service Desk Manager-Registerkarte "Berichte":** Auf der Registerkarte "Berichte" können befugte Benutzer ihre rollenbasierten Berichte in CA Service Desk Manager 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 764).

Berichtsdatenflussdiagramm

Das folgende Diagramm veranschaulicht für CA Business Intelligence in Integration mit BusinessObjects Enterprise den Datenfluss zwischen einzelnen Komponenten und deren Ausführung:



Anzeigen von Berichten in InfoView

Die vordefinierten CA Service Desk Manager-Berichte, die in BusinessObjects InfoView angezeigt werden, befinden sich in öffentlichen Ordnern. Sie können einen Ordner erweitern, um Unterordner anzuzeigen. Jeder Bericht enthält Verknüpfungen, die es Benutzern ermöglichen, Berichte und den Verlauf anzuzeigen sowie Berichte zu planen und zu bearbeiten, wie in dem folgenden Beispiel gezeigt.

	Titel	Zuletzt ausgeführt	Typ	Eigentümer	Instanzen
☐	Asset List	Noch nie ausgeführt	Crystal Reports-Bericht	Administrator	0

[Verlauf](#) | [Zeitgesteuert verarbeiten](#) | [Eigenschaften](#) | [Ändern](#)
 This report shows the Resource Family (Hardware, Software etc), the type of Asset (keyboard, modem, etc), the serial number for that Asset, a more detailed description of the Asset.

Hinweis: Weitere Informationen zur Verwendung von Berichten in InfoView finden Sie im *Benutzerhandbuch zu BusinessObjects InfoView*.

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 Benutzern und zum Zuordnen dieser Benutzer 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 Benutzern in CA Service Desk Manager zugewiesen.

Der Administrator kann sich bei der BusinessObjects-CMC anmelden und die Standardeinstellungen jederzeit ändern. Benutzer bekommen Zugriff auf InfoView-Ordner und der Zugriff richtet sich danach, zu welcher CA Business Intelligence-Gruppe sie gehören.

Gruppen und Benutzer

Die in der untenstehenden Tabelle aufgeführten Gruppen werden während der Konfiguration von CA Business Intelligence dem Central Management Server (CMS) hinzugefügt. Sie beziehen sich auf CA Service Desk Manager-Rollen mit den gleichen Namen. Während der Konfigurationsphase von CA Business Intelligence stand ein optionales Kontrollkästchen zur Verfügung, um anzugeben, ob Beispielbenutzer dem CMS hinzugefügt werden sollen. Wenn es ausgewählt wurde, schließt Ihre Standard-CMS-Konfiguration einen Beispielbenutzer für jede Gruppe ein. In CMC können Sie diese Beispielbenutzer als Modelle verwenden, wenn Sie Benutzerberechtigungen und Authentifizierungsoptionen für Ihre Berichtsumgebung festlegen.

Gruppenname	Benutzername
Change Manager	Change Manager-Benutzer
Kundenservicemanager	Kundenservicemanager-Benutzer
Knowledge-Manager	Knowledge Manager-Benutzer
Knowledge-Analyst	Knowledge-Analyst-Benutzer
CA Service Desk-Manager	CA Service Desk-Manager-Benutzer
Incident Manager	Incident Manager-Benutzer
Problem Manager	Problem Manager-Benutzer

Hinweis: Diese Beispielbenutzer gibt es nur, wenn sie während der Konfiguration von CA Business Intelligence angelegt wurden.

Universum und Verbindungen mit einem Universum

Die Standardkonfiguration umfasst auch die Sicherheitsrichtlinien für den Zugriff auf das CA Service Desk Manager-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

Gruppenname	Zugriffsebene
Incident Manager	Vollzugriff
Problem Manager	Vollzugriff

Berichtsordner

Die Standardkonfiguration umfasst eine Reihe von Ordnern mit vordefinierten Berichten für CA Service Desk Manager und Knowledge-Management. Jede CA Service Desk Manager-Gruppe ist so konfiguriert, dass sie Zugriff auf eine Teilmenge dieser Ordner hat.

Ordnername	Gruppenname	Zugriffsebene
Aggregat	■ Change Manager	■ Anzeigen
	■ Kundenservicemanager	■ Anzeigen
	■ Knowledge-Manager	■ Kein Zugriff
	■ Knowledge-Analyst	■ Kein Zugriff
	■ CA Service Desk-Manager	■ Vollzugriff
	■ Incident Manager	■ Anzeigen
	■ Problem Manager	■ Anzeigen
Asset	■ Change Manager	■ Nach Bedarf ansehen
	■ Kundenservicemanager	■ Anzeigen
	■ Knowledge-Manager	■ Kein Zugriff
	■ Knowledge-Analyst	■ Kein Zugriff
	■ CA Service Desk-Manager	■ Vollzugriff
	■ Incident Manager	■ Anzeigen
	■ Problem Manager	■ Anzeigen
Change (schließt alle Unterordner ein)	■ Change Manager	■ Vollzugriff
	■ Kundenservicemanager	■ Kein Zugriff
	■ Knowledge-Manager	■ Kein Zugriff
	■ Knowledge-Analyst	■ Kein Zugriff
	■ Service Desk-Manager	■ Anzeigen
	■ Incident Manager	■ Anzeigen
	■ Problem Manager	■ Anzeigen

Ordnername	Gruppenname	Zugriffsebene
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	■ Anzeigen
	■ Problem Manager	■ Kein Zugriff
Knowledge-Management	■ Change Manager	■ Kein Zugriff
	■ Kundenservicemanager	■ Anzeigen
	■ Knowledge-Manager	■ Vollzugriff
	■ Knowledge-Analyst	■ Anzeigen
	■ Service Desk-Manager	■ Ablauf
	■ Incident Manager	■ Anzeigen
	■ Problem Manager	■ Anzeigen
Survey	■ Change Manager	■ Kein Zugriff
	■ Kundenservicemanager	■ Kein Zugriff
	■ Knowledge-Manager	■ Anzeigen
	■ Knowledge-Analyst	■ Kein Zugriff
	■ Service Desk-Manager	■ Vollzugriff
	■ Incident Manager	■ Anzeigen
	■ Problem Manager	■ Anzeigen
Störungs- und Problemmanagement	■ Change Manager	■ Kein Zugriff
	■ Kundenservicemanager	■ Kein Zugriff
	■ Knowledge-Manager	■ Anzeigen

Ordnername	Gruppenname	Zugriffsebene
	■ Knowledge-Analyst	■ Kein Zugriff
	■ 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".

Anzeigen

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.

erweiterte Ansichten

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 Ordnebenen 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 745)

Verweisen eines vorhandenen CA Business Intelligence-Servers auf einen CA Service Desk Manager-Server

Wenn Sie über einen existierenden CA Business Intelligence-Server verfügen, können Sie mit ihm auf einen CA Service Desk Manager-Server verweisen. Hierfür sind folgende Schritte erforderlich:

1. [Erstellen Sie eine neue ODBC-Datenquelle](#) (siehe Seite 749).
2. [Konfigurieren Sie das Universe](#) (siehe Seite 750).
3. [Exportieren Sie das Universe](#) (siehe Seite 750).
4. Starten Sie InfoView, um die Verbindung zu überprüfen.

Erstellen einer ODBC-Datenquelle

Sie können mit dem ODBC-Datenquellenadministrator eine ODBC-Datenquelle 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 Service Desk Manager 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" und "Importieren".
Die Seite "Import Universe" (Universum importieren) wird angezeigt.
3. Navigieren Sie, wählen Sie Ihr CA Service Desk Manager-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 Service Desk Manager connection" (CA Service Desk Manager-Verbindung bearbeiten) wird angezeigt.
6. Geben Sie Benutzernamen und Kennwort des berechtigten CA Service Desk Manager-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 Service Desk Manager-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 Service Desk Manager-*Datenpartitionssicherheit* eingeschränkt. Alle CA Service Desk Manager-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 Service Desk Manager arbeitet.

Verwenden Sie dazu die folgenden Tools:

- **BusinessObjects Central Management Console (CMC):** Ermöglicht die Verwaltung von Authentifizierungen und Genehmigungen für Benutzer von BusinessObjects Enterprise.
- **BusinessObjects Designer:** Ermöglicht die Änderung des Universums von CA Service Desk Manager, Knowledge-Management, CMDB und Support-Automatisierung, welches eine Metaebene zwischen CA Service Desk Manager-Schema und Reporting-Tools darstellt.
- **CA Service Desk Manager Sicherheit und Rollenverwaltung:** Zum Einrichten der Datenaufteilungssicherheit, mit der Sie die Daten bestimmen, auf die die Benutzer zugreifen können.

Weitere Informationen:

[Hinzufügen von berechtigten CA Service Desk Manager-Benutzern zur CMC](#) (siehe Seite 752)

[Definieren der Universe-Datenbank-Anmeldeinformationen](#) (siehe Seite 752)

[Einrichten von Datenaufteilungen](#) (siehe Seite 753)

Hinzufügen von berechtigten CA Service Desk Manager-Benutzern zur CMC

Die Verbindung mit dem Universum wird standardmäßig so konfiguriert, dass beim Datenzugriff der berechnigte Benutzer und das Kennwort von Service Desk verwendet werden. Dieser Benutzer sollte dem CMC als ein neuer CA Business Intelligence-Benutzer hinzugefügt werden. Es gibt zwei Gründe für das Hinzufügen dieses Benutzers. 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 Service Desk Manager-Registerkarte "Berichte" testen. Für die Registerkarte "Berichte" muss der Benutzer sowohl in CA Service Desk Manager als auch in CA Business Intelligence definiert sein.

Verwenden Sie die Anleitungen im *Implementierungshandbuch*, um Ihre CA Service Desk Manager-Benutzer dem CMC hinzuzufügen und das CA Service Desk Manager-Konto für berechnigte Benutzer zu konfigurieren.

Definieren der Universe-Datenbank-Anmeldeinformationen

Das Universum muss die Datenbank-Anmeldeinformationen verwenden, die mit dem BusinessObjects-Benutzerkonto 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. Wählen Sie im Startmenü die Option "BusinessObjects XI Release2" > "BusinessObjects Enterprise" > "Designer" aus.
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 Service Desk Manager, 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" und dann auf "Text Connection", und bearbeiten Sie die nacheinander angezeigten Dialogfelder "Universumverbindung".
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 194).

Replizierte Datenbank für Offline-Berichterstellung

Um potenziellen Leistungsproblemen vorzubeugen, die sich auf die mit CA Service Desk Manager 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 Service Desk Manager präsentiert rollenbasierte Berichte in zwei Berichterstellungsrahmen auf der Registerkarte "Berichte". Jeder Rahmen bietet grafische Ansichten, mit denen die Benutzer 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 Benutzer 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

Hier können Sie den Zugriff der Rolle auf die einzelnen CA Service Desk Manager-Funktionsbereiche definieren.

Web-Schnittstelle

Hier können Sie die Web-Schnittstelle für die Rolle durch Definieren der Webseiten und der Inhalte der Online-Hilfe anpassen, auf die die Benutzer zugreifen können.

Knowledge-Management

Hier können Sie die Knowledge-Management-Berechtigungen für die Rolle angeben.

KT-Dokumentsichtbarkeit

Hier können Sie angeben, welchen Dokumentstatus die Rolle anzeigen darf (zum Beispiel "Entwurf", "Deaktiviert" und "Veröffentlicht").

Registerkarten

Hier können Sie die Registerkarten definieren, die angezeigt werden, wenn ein dieser Rolle zugewiesener Benutzer bei CA Service Desk Manager angemeldet ist.

Berichts-Webformulare

Hier können Sie die Berichts-Webformulare definieren, die für diese Rolle verfügbar sind.

'Los'-Ressourcen

Hier können Sie angeben, welche Datensatztypen in der Dropdown-Liste "Go" 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 Service Desk Manager genehmigt wurde, wird er in den öffentlichen Abschnitt in InfoView verschoben und steht befugten Benutzern damit zur Verfügung. Um den Bericht zu CA Service Desk Manager hinzuzufügen, muss der Administrator einige zusätzliche Schritte ausführen.

Sie können neue, in CA Business Intelligence erstellte Berichte auf der CA Service Desk Manager-Registerkarte "Berichte" anzeigen. Verwenden Sie dazu die folgenden Tools:

- Web-Screen Painter
- Rollenverwaltung

Führen Sie zuvor Folgendes aus:

- Installieren und konfigurieren Sie CA Business Intelligence für die Zusammenarbeit mit CA Service Desk Manager.

Hinweis: Weitere Informationen zur Installation finden Sie im *Implementierungshandbuch* und im *CA Business Intelligence-Installationshandbuch*.

- Die Benutzerberechtigungen, die Rollen und die [Authentifizierungsoptionen](#) (siehe Seite 743) für Ihre Berichterstellungsumgebung sind eingerichtet.

Weitere Informationen:

[Schritt 1: Erstellen von zwei Webformular-Datensätzen zum Aufrufen von neuen Berichten](#) (siehe Seite 757)

[Schritt 2: Erstellen einer Multiframe-Seite und Zuweisen der neuen Berichte](#) (siehe Seite 758)

[Schritt 3: Erstellen Sie eine Startseite für die Registerkarte "Berichte".](#) (siehe Seite 760)

[Schritt 4: Erstellen Sie einen Datensatz für die Registerkarte "Berichte" und weisen Sie die Startseite zu.](#) (siehe Seite 761)

[Schritt 5: Weisen Sie den Datensatz der Registerkarte einem Rollendatensatz zu.](#) (siehe Seite 762)

[Schritt 6: Erstellen Sie eine Startseite für die Schaltfläche "InfoView".](#) (siehe Seite 762)

[Schritt 7: Weisen Sie die Startseite der Schaltfläche "InfoView" dem Datensatz der Registerkarte "Berichte" zu.](#) (siehe Seite 763)

Schritt 1: Erstellen von zwei Webformular-Datensätzen zum Aufrufen von neuen Berichten

Standardmäßig enthält die Registerkarte "Berichte" zwei Berichterstellungs-Frames, mit deren Hilfe berechtigte Benutzer 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 eingegeben 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 Service Desk Manager-Benutzer 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 Service Desk Manager 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.

Anzeigenname

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 Benutzer 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 Benutzer 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.

Schritt 6: Erstellen Sie eine 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 Service Desk Manager 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: Allgemeine Informationen zur Verwendung von vordefinierten Berichten finden Sie in der *Online-Hilfe*. Beachten Sie auch das *Benutzerhandbuch zu BusinessObjects InfoView*.

Weitere Informationen:

[Business Objects InfoView-Schnittstelle](#) (siehe Seite 764)

[Navigieren zu Berichten](#) (siehe Seite 765)

[InfoView-Voreinstellungen](#) (siehe Seite 765)

[Planen von Berichten](#) (siehe Seite 766)

[Einrichten der Datenanalyse](#) (siehe Seite 767)

[Speichern und Verteilen von Berichten](#) (siehe Seite 767)

Business Objects InfoView-Schnittstelle

Über die Registerkarte "CA Service Desk Manager-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 Service Desk Manager auf die Schaltfläche "InfoView".
- Wählen Sie im Startmenü die Option "BusinessObjects XI Release2 > 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 Service Desk Manager".
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.

Hinweis: Weitere Informationen zum Festlegen von Einstellungen und zur Verwendung von Berichten finden Sie im *Benutzerhandbuch zu BusinessObjects InfoView*.

InfoView-Voreinstellungen

Benutzer 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.

Hinweis: Weitere Informationen zum Definieren von Voreinstellungen finden Sie im *Benutzerhandbuch zu BusinessObjects InfoView*.

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 Dokumentenergebnisse 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 Service Desk Manager-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 Anfragen.

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 Benutzern und Gruppen teilen.

Hinweis: Weitere Informationen zur Datenanalyse finden Sie im *Benutzerhandbuch zu BusinessObjects InfoView*.

Speichern und Verteilen von Berichten

InfoView-Benutzer 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 Service Desk Manager genehmigt wurde, wird er in den öffentlichen Abschnitt verschoben und steht autorisierten Benutzern 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.

Hinweis: Weitere Informationen zur Veröffentlichung und Verteilung von Berichten finden Sie im *Benutzerhandbuch zu BusinessObjects InfoView*.

Dashboard-Berichte

Sie können Dashboard-Berichte verwenden, um tägliche Vorgänge für alle CA Service Desk Manager-Tickets (Anforderung/Incident/Problem, Change oder Issue) 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 Service Desk Manager in einer einzigen Ansicht anzeigen. Über das Unternehmens-Dashboard gibt Ihnen wichtige Informationen über tägliche Vorgänge für alle Ticket-Typen (Anforderung/Incident/Problem, Change oder Anforderung) nach Priorität, Analyst, Kategorie oder Gruppe.

Hinweis: Wenn Sie mit Dashboard-Berichten arbeiten, können Sie die InfoView-Funktionen verwenden, die im Abschnitt "Arbeiten mit Dashboard und Analyse" im *BusinessObjects-Enterprise-InfoView-Benutzerhandbuch* beschrieben sind.

Anzeigen von Berichten im Dashboard für den Einsatz im Unternehmen (Operational Dashboard)

Berechtigte Benutzer können vordefinierte Dashboard-Berichte in BusinessObjects InfoView anzeigen lassen. Welche Ordner und Berichte Sie im InfoView sehen, hängt von dem Konto ab, über das Sie sich einloggen und von den Rechten, die Ihnen vom Administrator gewährt wurden.

Hinweis: Die Anmeldeinformationen erhalten Sie von Ihrem Administrator.

So lassen Sie einen Bericht im Dashboard für den Einsatz im Unternehmen (Operational Dashboard) anzeigen

1. Klicken Sie auf der Registerkarte "Berichte" in CA Service Desk Manager auf die Schaltfläche "InfoView", und melden Sie sich mit Ihren Anmeldeinformationen bei InfoView an.

InfoView wird in Ihrem Webbrowser angezeigt.

2. Wählen Sie in der InfoView-Symbolleiste die Option "Dashboards" > "Unternehmens-Dashboards" > "Service Desk Manager – Tägliche Vorgänge".

Im Navigationsbereich werden Ordner und Objekte angezeigt.

3. Wählen Sie "Öffentliche Ordner" > "CA-Berichte" > "Dashboard für den Einsatz im Unternehmen" (Operational Dashboard).

Die folgenden Ordner werden angezeigt: Change, Incident, Issue, Problem, Anforderung.

4. Wählen Sie den entsprechenden Bericht aus.

Die Dashboard-Optionen werden im rechten Fensterbereich angezeigt.

5. Doppelklicken Sie auf den Titel, um einen Bericht anzuzeigen.

Der Bericht kann nun angesehen werden.

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.

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-Benutzerhandbuch* 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 Service Desk Manager-Universum 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 Service Desk Manager-Universum auswählen.
2. Das Universe ist der CA Service Desk Manager-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 Service Desk Manager-Standard-Universe 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*.

Weitere Informationen:

[Beispiel: Anzeigen aller offenen Anfragen mit Priorität 1 und 2 für alle Benutzer](#) (siehe Seite 771)

[Beispiel: Anzeigen aller offenen Anfragen, deren Status nicht "In Bearbeitung" ist.](#) (siehe Seite 773)

[Beispiel: Anzeigen aller in den letzten 30 Tagen geschlossenen Anfragen für Benutzer, deren Nachname mit "C" beginnt.](#) (siehe Seite 775)

Beispiel: Anzeigen aller offenen Anfragen mit Priorität 1 und 2 für alle Benutzer

In diesem Beispiel legen Sie Eingabewerte fest, die vor der Erstellung des Berichts zusätzliche Daten erfassen.

Beispiel: Anzeigen aller offenen Anfragen mit Priorität 1 und 2 für alle Benutzer

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 Service Desk Manager 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 "Anfrage", "Anfrage - 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".
 - Zusammenfassung
 - 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 "Anfrage - Detail", wenn Sie fertig sind.
 - Statussymbol
 - Prioritätssymbol
6. Erweitern Sie den Ordner "Abfragefilter", 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 Listepfeil im Statussymbol-Objekt. 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 Benutzer-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 Benutzernamen 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 Anfragen mit Priorität 1 & 2" für alle Benutzer 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 Anfragen, 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 Anfragen, deren Verarbeitungsstatus 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 Service Desk Manager 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 "Anfrage", "Anfrage - 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.
 - Zusammenfassung
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 "Anfrage - Detail".
6. Erweitern Sie den Ordner "Abfragefilter", 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 Listepfeil 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 Anfragen an, deren Status *nicht* "In Bearbeitung" ist.

Beispiel: Anzeigen aller in den letzten 30 Tagen geschlossenen Anfragen für Benutzer, deren Nachname mit "C" beginnt.

In diesem Beispiel geben Sie die Eingabewerte für das Schließdatum und den Nachnamen des Kunden an. Basierend auf diesen Werten werden alle geschlossenen Anfragen zurückgegeben.

Beispiel: Anzeigen aller in den letzten 30 Tagen geschlossenen Anfragen für Benutzer, 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 Service Desk Manager 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 "Anfrage", "Anfrage - 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
- Zusammenfassung

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 Anfragen für Benutzer, 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.

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 Service Desk Manager-Web-Schnittstelle. Die von KPIs erstellten Daten werden in der CA Service Desk Manager-Datenbank gespeichert und sind zum Erstellen webbasierter Berichte verfügbar.

Hinweis: Neben der Definition von KPI-Abfragen können Sie den KPI-Daemon so konfigurieren, dass CA Service Desk Manager-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 Service Desk Manager 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 Service Desk Manager 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", "bpvirtddb" 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 Service Desk Manager-Prozesse zusammenzustellen.

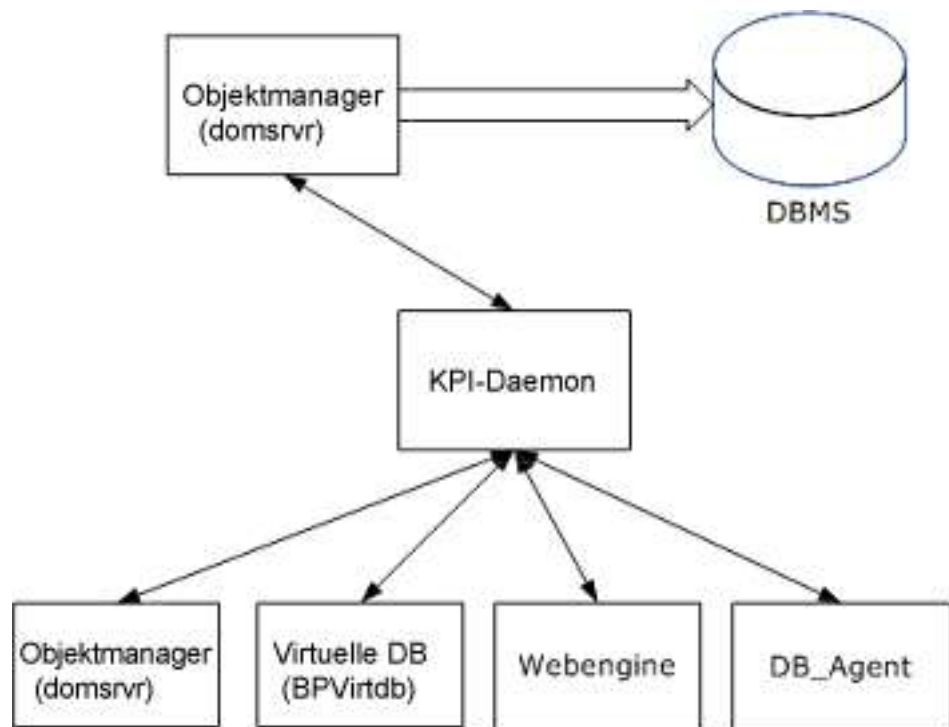
Die folgenden Prozessstypen werden unterstützt:

- **domsrvr:** CA Service Desk Manager-Objektmanager (Serverprozess) Der Objektmanager speichert auch für Clients verschiedene Datensätze und Tabellen im Zwischenspeicher.
- **bpvirtddb:** Der BOP Virtuelle Datenbankserver ermöglicht die Verwendung mehrerer Objektmanager in der CA Service Desk Manager-Umgebung. Alle Objektmanager, die auf Primär- oder Sekundärservern ausgeführt werden, verbinden sich mit der virtuellen Datenbank, die über den Zugriff auf Datenbank-Agenten entscheidet. 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. 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 Service Desk Manager und dem Datenbankmanagementsystem (DBMS). Datenbank-Agenten halten am CA Service Desk Manager-Datenbankschema fest und übersetzen den SQL-Code in das vom DBMS benötigte Formular (zum Beispiel, Oracle).
- **Web-Engine:** CA Service Desk Manager-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. Auf dem Primärserver muss eine Web-Engine für den WSP vorhanden sein, damit der WSP-Schemadesigner Schema-Dateien erstellen kann. Web-Engines sind der eigentliche Client des Objektmanagers für den Webbrowser eines Benutzer-Clients. Web-Engines speichern HTML-Webformulare für verbundene Benutzer im Zwischenspeicher. 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 Service Desk Manager-Datenbank abgerufenen Zahlungsmetrik basiert.

CA Service Desk Manager 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 358).

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 Service Desk Manager-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.
Prozess Typ	X			System-KPI-Metriken können von den folgenden CA Service Desk Manager-Prozessen abgeleitet werden:

Feld	Sys.	S.Q.	SQL	Beschreibung
				■ domsrvr – Objektmanager ■ bpvirtddb – BOP Virtual-Datenbankserver ■ db_agents – Datenbank-Agenten ■ webengine – Der CA Service Desk Manager-Webservice Weitere Informationen zu diesen Prozessen finden Sie unter System-KPIs (siehe Seite 779).
System Name	X			Der interne Name des System-KPIs. Nicht editierbar
Benutzer Kontext		X	X	(Optional) Gibt die Benutzer-ID eines CA Service Desk Manager-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 Service Desk Manager-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 Service Desk Manager-Version 6.0 und früher.
- Hinweis: Das Aktivieren dieser Funktion kann dazu führen, dass die CA Service Desk Manager-Leistung sinkt.

Weitere Informationen:

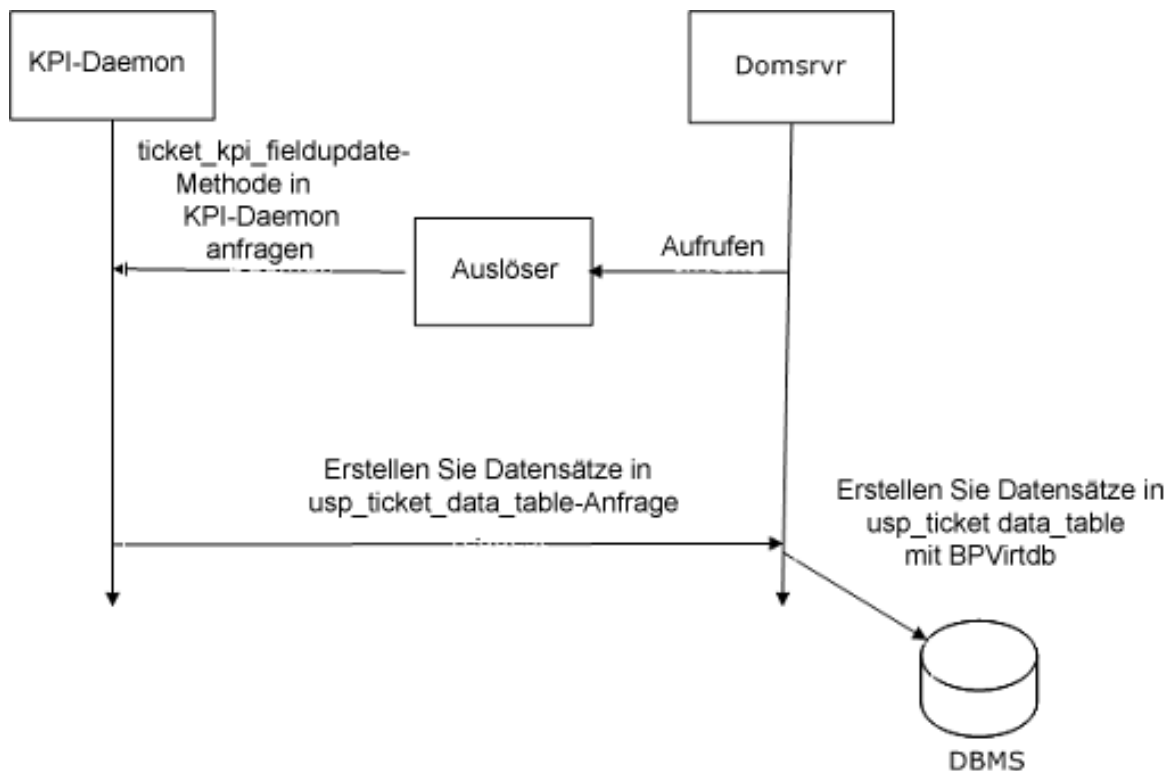
[Datei "NX.env"](#) (siehe Seite 788)

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 Service Desk Manager-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*.

Problembehandlung

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 Service Desk Manager 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 786).

Schreiben von CA Business Intelligence-Berichten

Sie können CA Business Intelligence-Berichte für CA Service Desk Manager schreiben.

Weitere Informationen:

[CA Service Desk Manager-ODBC-Treiber](#) (siehe Seite 790)

[Schreiben von SQL für BusinessObjects-Berichte](#) (siehe Seite 791)

[PDM-Funktionen](#) (siehe Seite 792)

[Attributaliasnamen](#) (siehe Seite 794)

[pdm_isql - interaktives SQL](#) (siehe Seite 795)

CA Service Desk Manager-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 Service Desk Manager verbunden.

Dies bietet verschiedene Vorteile:

- SELECT-Anweisungen, die von BusinessObjects-Berichten verwendet werden, referenzieren Objekte und Attribute mit Hilfe ihrer CA Service Desk Manager-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 Service Desk Manager-ODBC-Treiber ordnet Attribute wie "combo_name" und Objekte wie "cnt" ihren entsprechenden DBMS-Namen zu.
- Alle CA Service Desk Manager-Sicherheitseinstellungen, einschließlich derjenigen zu Datenpartition und Einschränkungen der Mandantenfähigkeit, werden automatisch auf Berichte angewendet. Alle Verbindungen zwischen BusinessObjects und CA Service Desk Manager sind einem CA Service Desk Manager-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 Service Desk Manager-Attributalias "vereinfacht" die CA Service Desk Manager-Datenbank. Attribut-Aliasnamen sind zusätzliche Attribute in CA Service Desk Manager-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 Service Desk Manager-ODBC-Treiber unterstützt Datumsliterale in Abfragen und überträgt automatisch Werte im internen CA Service Desk Manager-Datumsformat in ein standardmäßiges DBMS-Datum.

Wichtig! Der CA Service Desk Manager-ODBC-Treiber wird nur für BusinessObjects-Berichte unterstützt (Crystal und Web Intelligence). CA Service Desk Manager 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 Service Desk Manager-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 Service Desk Manager-Objektnamen und anstelle von DBMS-Spaltennamen werden CA Service Desk Manager-Attributnamen verwendet.
- Ein CA Service Desk Manager-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 794).

- DERIVED-Attribute von CA Service Desk Manager (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 Service Desk Manager-interne Datumsformat (Anzahl der Sekunden ab 1. Januar 1970, Mitternacht).

PDM-Funktionen

Zur Erleichterung der Arbeit mit speziellen CA Service Desk Manager-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.
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

PDM-Funktionen	Beschreibung
	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. Beachten Sie, dass das Argument erforderlich ist.
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.
PdmToday()	PdmToday ([timeAdj [, day [, month [, year]]]]) Gibt das aktuelle Datum ab dem 01.01.70 in Sekunden zurück. Diese Funktion kann an einer beliebigen Stelle in der Abfrage verwendet werden. Die folgenden Argumente passen das zurückgegebene Datum an: timeAdj ■ -1 => Zeit auf Beginn des Tages einstellen (0:00:00; ■ +1 => Zeit auf Ende des Tages einstellen (23:59:59) Tag ■ negative => Datum um die angegebene Anzahl von Tagen korrigieren ■ positive => Tag auf angegebenen Absolutwert einstellen (oder auf letzten Tag des Monats, je nachdem, welcher Wert niedriger ist) month ■ negative => Datum um die angegebene Anzahl von Monaten

PDM-Funktionen	Beschreibung
	korrigieren ■ positive => Monat auf angegebenen Absolutwert einstellen (oder auf "Dezember (12)", je nachdem, welcher Wert niedriger ist) year ■ negative => Datum um die angegebene Anzahl von Jahren korrigieren ■ positive => Jahr auf angegebenen 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 Service Desk Manager-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 Service Desk Manager r12.5 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 Service Desk Manager-ODBC-Treiber erstellt automatisch Verknüpfungen nach Bedarf für den Zugriff auf die Tabellen, die von Attributaliasnamen referenziert werden. Ein Benutzer in der CA Service Desk Manager-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 Service Desk Manager" > "Codes" > "Attribut-Aliasnamen".

pdm_isql - interaktives SQL

Zusammen mit CA Service Desk Manager 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 Service Desk Manager-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 Service Desk Manager-Anmeldeinformationen stehen und der Hostname der Hostname eines CA Service Desk Manager-Servers mit einer Web-Engine ist.)
4. Geben Sie SQL SELECT-Anweisungen ein, gefolgt von einem Semikolon.

Kapitel 18: Generieren von Berichten in USDK

Dieses Kapitel enthält folgende Themen:

[Berichte erzeugen](#) (siehe Seite 797)

[Datenbankansichten](#) (siehe Seite 797)

[Einrichten von Berichtsmethoden](#) (siehe Seite 801)

[Berichtsformatierung](#) (siehe Seite 801)

[Ändern der Sortierreihenfolge der Spalten](#) (siehe Seite 802)

[Zusammengefasste Berichte und Detailberichte](#) (siehe Seite 802)

[Analyseberichte](#) (siehe Seite 803)

Berichte erzeugen

CA Service Desk Manager 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 Service Desk Manager-Berichten finden Sie in der *Online-Hilfe* unter "Erzeugen von Berichten". Neben der Verwendung der in CA Service Desk Manager integrierten Berichtsfunktionen können Sie benutzerdefinierte Berichte auf der Basis der Tabellen und Ansichten in Ihrer CA Service Desk Manager-Datenbank generieren. Weitere Informationen zu benutzerdefinierten Berichten finden Sie im *Implementierungshandbuch*.

Datenbankansichten

Die CA Service Desk Manager-Datenbank ist ein Repository für die Daten, die Sie für den Betrieb Ihres Service Desks eingeben und nutzen. CA Service Desk Manager bietet mehrere Datenbankansichten und ermöglicht Ihnen die Erstellung benutzerdefinierter Berichte der Datenbank.

Diese Ansichten unterteilen sich in zwei Arten:

- grundlegende Ansichten
- erweiterte Ansichten

Weitere Informationen:

[Beschreibungen der Felder in Ansichten](#) (siehe Seite 985)

Grundlegende Ansichten

Die grundlegenden Ansichten basieren auf den Tabellen von CA Service Desk Manager. 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

Name anzeigen	Beschreibung
View_Request_to_Act_Log	alle Anfragen mit ihren Aktivitätsprotokollen (diese Ansicht ist ein Verbindung von "View_Request" und "View_Act_Log")
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 ein 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)

Name anzeigen	Beschreibung
View_Issue_to_Issue_WF	Issues und ihre Workflow-Aufgaben (dies muss nicht alle Issues einschließen, insbesondere, wenn ihnen keine Workflow-Aufgaben zugewiesen sind)
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 Service Desk Manager.

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 Service Desk Manager-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 363)

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,p)// 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,p)// 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,p)// 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 Service Desk Manager-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 Service Desk Manager 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 Service Desk Manager 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 Anfragen und Issues](#) (siehe Seite 803)

[Generieren von Berichten zu Anfragebereichen und Issue-Kategorien](#) (siehe Seite 804)

[Erstellen von Berichten zur Priorität von Anforderungsbereichen und zur Priorität von Issue-Kategorien](#) (siehe Seite 804)

Generieren von Berichten zu Anfragen 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 Anfragen oder Issues über die Web-Schnittstelle:

1. Wählen Sie 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 Anfragebereichen 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 Anfragebereich oder Issue-Kategorie sortiert.

So generieren Sie Berichte zu Anfragebereichen oder Issue-Kategorien über die Web-Schnittstelle:

1. Wählen Sie 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 Anforderungsbereich oder Problemanfragenkategorie sortiert.

So generieren Sie Berichte zur Priorität von Anforderungsbereichen oder zur Priorität von Problemanfragenkategorien über die Web-Schnittstelle:

1. Wählen Sie 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 19: Verwalten von Knowledge

Dieses Kapitel enthält folgende Themen:

[Knowledge-Management](#) (siehe Seite 805)
[Suchen von Prozeduren für das Knowledge Management](#) (siehe Seite 806)
[Knowledge und Mandantenfähigkeit](#) (siehe Seite 806)
[So richten Sie eine Knowledge Base ein:](#) (siehe Seite 807)
[So verwenden Sie Dokumente in der Knowledge Base:](#) (siehe Seite 810)
[Knowledge-Dateien](#) (siehe Seite 817)
[Knowledge-Suche](#) (siehe Seite 818)
[Foren](#) (siehe Seite 818)
[Knowledge-Baumstrukturdokumente](#) (siehe Seite 818)
[Knowledge-Dokument-Ablaufplan](#) (siehe Seite 819)
[Zugreifen auf Export/Import](#) (siehe Seite 830)
[Webservices](#) (siehe Seite 845)

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 199)

Suchen von Prozeduren für das Knowledge Management

Mit CA Service Desk Manager 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 Service Desk Manager an.
Die Hauptseite von CA Service Desk Manager 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, PCHowTo 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 ausführen, 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 Benutzer ihre zugewiesenen Aufgaben durch Ändern ihrer Dokumente entsprechend der ihnen zugewiesenen Rollen durchführen.

Alle Benutzer 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. Benutzer 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 Service Desk Manager. 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 Benutzern 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 Benutzer 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** — Benutzer 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 Überprüfen 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 Endbenutzer 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 Benutzer das Dokument geöffnet hat.

Knowledge-Einreichung in CA Service Desk Manager

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 Service Desk Manager 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 Service Desk Manager 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 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 Benutzer zugewiesen wird, eröffnen die Standard-Datenpartitionseinschränkungen dem Benutzer 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 810)

[Dokument-Attribute](#) (siehe Seite 813)

[Dokumentberechtigungen](#) (siehe Seite 813)

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 Überprüfen und erneuten Veröffentlichen ersetzt wird. Die Notwendigkeit, die Veröffentlichung des Dokuments zuerst rückgängig zu machen, wird dadurch umgangen.

Benutzer 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 Benutzer 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 Service Desk Manager-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 Service Desk Manager-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 Service Desk Manager-Datenbank. Diese Regeln werden in bestimmten Zeitintervallen auf CA Service Desk Manager-Objekte angewendet.

Knowledge-Dateien

Eine *Knowledge-Datei* ist eine durchsuchbare Textdatei (.pdf, .zip, .xls, .exe, .html, .img, .msg, .ppt, .rtf, .txt, .avi, .doc und .xml), die mit einer Kategorie verknüpft ist und mit anderen Kategorien verwandt sein kann.

Knowledge-Dateien sind flexibel und ermöglichen die schnelle Nutzung von Knowledge einer externen Ressource, ohne dass die Informationen in einem strukturierten Knowledge-Dokument zusammengeführt werden müssen. Zum Beispiel kann ein Analyst Knowledge von einem Lieferanten verwenden, das erläutert, wie ein Drucker repariert wird und dieses Knowledge als Knowledge-Datei in einer Knowledge-Kategorie mit dem Namen "Drucker" speichern.

Eine Knowledge-Datei bietet Benutzern viele Möglichkeiten. Beispielsweise können sie eine Datei ersetzen, in ein Knowledge-Dokument umwandeln und an einen anderen Speicherort laden. Es können sowohl traditionelle als auch erweiterte Suchoptionen verwendet werden, um in einer Datei nach Knowledge zu suchen.

Alle Dateien werden im Knowledge-Datei-Repository gespeichert, wobei der Administrator dafür sorgt, dass Benutzer schnell und sicher auf die Dateien zugreifen können.

Hinweis: Informationen zum Hinzufügen von Knowledge-Dateien an ein Repository finden Sie unter "Anhangsbibliothek" in der *Online-Hilfe*.

Knowledge-Suche

Knowledge-Management bietet Benutzern 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.

Knowledge-Baumstruktur

Stellt eine Reihe von Fragen, um den Benutzer zu möglichen Lösungen zu führen. Die zur Auswahl stehenden Antworten führen den Benutzer zu einer Lösung, die am relevantesten erscheint.

Lesezeichen

Bietet Zugriff auf häufig angesehene Dokumente, die in einer Lesezeichenliste enthalten sind.

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 Skripterstellung- 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 Schlüsselereignisse im Knowledge Management-Lifecycle bereit. Die folgenden Ereignisse 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 678) 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 Benutzer in einer Installation für mehrere Mandanten angezeigt.

Ereignistyp

Filtert die Suche nach den folgenden Ereignistypen:

- 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 Ereignisse 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 Service Desk Manager-Listenseite an.

Hinweis: Klicken Sie auf das Symbol "Weitere", um das Feld "Weitere Suchargumente" anzuzeigen. Dieses Feld ist nur für Fachleute gedacht, die mit SQL und Majic umgehen und bestimmte Suchargumente angeben können, die nicht in den standardmäßigen Suchfilterfeldern 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-Ereignisse haben nur ein Datum (keine Uhrzeit) und werden nach Ereignistyp gruppiert. Sie ähneln somit Changes, die für jeden Zeitraum und Change-Typ gruppiert werden.
- Ereignistypen 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 Service Desk Manager-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 Benutzer 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 Benutzer eine Ansicht mit einem oder mehr Tagen außerhalb des Datenauswahlbereichs des Suchfilters auswählt. Bei der Festlegung des Werts auf 0 muss der Benutzer 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 Service Desk Manager 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 Service Desk Manager nur die erste maxGroups-1 an und ersetzt die letzte durch einen "...nn zusätzliche Changes"-Hyperlink, über den der Benutzer 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 Ereignissen 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 Service Desk Manager-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)	runde 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-CIs 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 Service Desk Manager zeigt Attribute in der Zusammenfassungen-, 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 Monatansicht führt alle Elemente in einer Gruppe in ein einzelnes Ereignis zusammen. Ansichten mit Ausnahme der Monatansicht 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

bicolor=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 "#FF000" 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 Ereignisse im Ablaufplan. Ändern Sie diese Funktion, wenn Sie neue Gruppenobjekte anzeigen möchten. Die vordefinierten Gruppenobjekte werden standardmäßig angezeigt.

CA Service Desk Manager ruft "setSchedEvents()" je einmal für jedes Objekt (Change oder Knowledge-Dokument) auf, das über den Suchfilter des Ablaufplans ausgewählt wurde. Die Funktion erstellt Ereignisse für das Objekt durch Aufrufen einer zweiten Funktion, schedEvent(), und deren Übergabe an die Gruppen-ID, das Startdatum und Enddatum des Ereignisses.

Die Funktion kann eine beliebige Anzahl von Ereignissen (einschließlich Null) für ein Objekt erstellen. Die Standardfunktion "setSchedEvents()" für den Change-Kalender ("list_chgsched.html") erstellt je ein Ereignis 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 Ereignis 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 importiert werden können.

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 Benutzer bei CA Service Desk Manager angemeldet ist. Die Rolle des Standard-Befehlszeilendienstprogramms wird auf dem Zugriffstyp für den Benutzer gesetzt.

So exportieren/importieren Sie Knowledge:

Mit Export-/Importvorlagen können Sie Export-/Importtransaktionen definieren.

Um Knowledge zu exportieren oder zu importieren, führen Sie die folgenden Schritte aus:

1. Führen Sie eine der folgenden Aufgaben 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 auf der Seite "Vorlage – Detail" auf "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 842)
3. Importieren Sie Knowledge-Daten aus dem Paket, indem Sie eine der folgenden Aktionen ausführen:
 - Kopieren Sie das Knowledge-Paket in eine Ziel-CA Service Desk Manager-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 843)

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 834)

Exportieren von Transaktionen

Sie können Transaktionen nach Paket, Vorlage und Status sortieren. Alle KEIT-Transaktionen werden in den folgenden Protokolldateien aufgezeichnet:

stdlog

Zeichnet CA Service Desk Manager-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>" auswählen, ist das Objekt öffentlich.

Die Seite "Transaktionen exportieren" enthält die folgenden Felder:

Paket

Gibt den Namen des Exportpakets an.

Ausführen nach

Zeigt den Benutzer 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>" auswählen, ist das Objekt öffentlich.

Die Seite enthält die folgenden Felder:

Paket

Gibt den Namen des Importpakets an.

Ausführen nach

Zeigt den Benutzer 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 839)

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

Sie können Paketverzeichnisse definieren, indem Sie die Option *keit_path* unter "Optionsmanager" > "Knowledge" bearbeiten. Pakete werden in den folgenden Standardverzeichnissen gespeichert:

- Pakete exportieren
KEIT_PATH\export
- Pakete importieren
KEIT_PATH\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 "Verwaltung".
Die Administrationskonsole 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 Service Desk Manager 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 mehrere Mandanten installiert haben, wählen Sie den entsprechenden Mandanten aus der Dropdown-Liste 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 837)
- [Exportfilter](#) (siehe Seite 838)
- [Importeinstellungen](#) (siehe Seite 839)

Klicken Sie auf "Speichern".

Die Vorlage wird erstellt.

Siehe auch:

[Exportieren von Transaktionen](#) (siehe Seite 832)

[Importieren von Transaktionen](#) (siehe Seite 833)

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 Zielsystem überschreiben.

Dokumente überschreiben, die nicht den Status "Veröffentlicht" aufweisen

Ermöglicht, dass importierte Dokumente nicht-veröffentlichte Dokumente auf dem Zielsystem 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.

Autor

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 837)
- [Exportfilter](#) (siehe Seite 838)
- [Importeinstellungen](#) (siehe Seite 839)

5. Klicken Sie auf "Speichern".

Ihre Änderungen werden gespeichert.

Weitere Informationen:

[Importieren von Transaktionen](#) (siehe Seite 833)

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 Zielsystem:

`$NX_ROOT/site/attachments/default`

Mit diesem Hilfsprogramm haben Sie die folgenden Möglichkeiten:

- Erstellen Sie die Konfigurationsdatei auf der Grundlage der entsprechenden Knowledge-Exportvorlage.
- Exportieren 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_ATTMTNT).

Die Dateien werden von einer Remote-Repository in den lokalen Paketordner kopiert.

So rufen Sie das Hilfsprogramm 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 Ereignissen. 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 Zielservers, gemäß den Einstellungen in der Konfigurationsdatei eines Pakets.

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 r12.5.

Die Daten, die früher mit dem Hilfsprogramm "pdm_ket" verknüpft wurden, erhalten den tatsächlichen UUID- oder ID-Wert des Zielservers. 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 Benutzer-ID (für Kontakte) oder der verknüpfte Name (für Felder wie Asset) mit einer geeigneten UUID des Zielservers 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 Hilfsprogramm 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 Standardbenutzer an.

-v

(Optional) Aktiviert eine umfassende Protokollierung (bop_logging) von programmspezifischen Ereignissen. Diese Option wird in der Regel zum Beheben von internen Problemen verwendet.

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 Schritte 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 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 Webservices finden Sie im *Implementierungshandbuch*.

Kapitel 20: Verwalten von Knowledge-Management

Dieses Kapitel enthält folgende Themen:

[Knowledge-Verwaltung](#) (siehe Seite 847)
[Suchen von Prozeduren für die Knowledge-Administration](#) (siehe Seite 848)
[Rollen und Funktionen von Knowledge-Management](#) (siehe Seite 848)
[So verwalten Sie Rollenberechtigungen und die Dokumentsichtbarkeit:](#) (siehe Seite 862)
[Aktionsinhalte](#) (siehe Seite 862)
[Genehmigungsvorgang für Dokumente](#) (siehe Seite 868)
[Automatisierungsrichtlinien](#) (siehe Seite 876)
[Knowledge-Dokumentsteuerung](#) (siehe Seite 881)
[Knowledge-Kategorien](#) (siehe Seite 898)
[Berichte und Indikatoren](#) (siehe Seite 909)
[Suchen](#) (siehe Seite 911)
[Optionen zur Integration von CA Service Desk Manager](#) (siehe Seite 935)
[Lösungsumfrage](#) (siehe Seite 944)
[Knowledge-Management-Systemeinstellungen](#) (siehe Seite 947)

Knowledge-Verwaltung

Sie können Verwaltungseinstellungen für Knowledge-Management konfigurieren. Sie können [Self-Service-Knowledge-Optionen](#) (siehe Seite 851) konfigurieren, um den Anforderungen der Benutzer 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, die dazu beitragen, dass die Funktionen und die Verwendung von Knowledge-Management vereinheitlicht werden.

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 Service Desk Manager 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 Service Desk Manager an.
Die Hauptseite von CA Service Desk Manager 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" und dann auf "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 Benutzer 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 Benutzerrollen:

- **Kunde:** Ein externer Endbenutzer, der grundlegende Self-Service-Aufgaben ausführt.
- **Mitarbeiter:** Ein interner Endbenutzer, der grundlegende Self-Service-Aufgaben ausführt.
- **Knowledge-Analyst:** Ein Benutzer, der für einen oder mehrere Schritte innerhalb des Knowledge Managements verantwortlich ist. Dieser Benutzer 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 Kategoriestructur, 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 Service Desk Manager- und Knowledge-Management-Produkten hat. Diese Rolle kommt für gewöhnlich dann zur Anwendung, wenn CA Service Desk Manager implementiert wird und sicher gestellt werden muss, dass alle Benutzer und Rollen richtig eingerichtet werden. Sie kommt auch dann zu 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 Service Desk Manager-Umgebung ist eine bestimmte Zugriffsebene zugeordnet. Diese Ebenen helfen dabei, die Aufgaben zu definieren, die jede Rolle erfüllt.

Siehe auch:

[Knowledge-Management-Benutzeroberflächen](#) (siehe Seite 850)

[Konfiguration und Verwaltungsfunktionen von Knowledge-Management](#) (siehe Seite 850)

[Optionen für Self-Service-Knowledge](#) (siehe Seite 851)

[Dokumente und Benutzer](#) (siehe Seite 857)

[So verwalten Sie Rollenberechtigungen und die Dokumentsichtbarkeit:](#) (siehe Seite 862)

Knowledge-Management-Benutzeroberflächen

Die folgenden Benutzeroberflächen helfen Ihnen, Knowledge zu verwalten:

- **Self-Service** - In der Self-Service-Schnittstelle können Kunden und Mitarbeiter, die CA Service Desk Manager 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 Service Desk Manager-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 Service Desk Manager 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 Service Desk Manager-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.
- Wenn CA Service Desk Manager konfiguriert wird, um die Knowledge-Management-Suchmaschine zu verwenden, können Sie optional auf die FAST-Suchmaschine umschalten (wenn diese installiert wird). Die FAST-Suchmaschine stellt zusätzliche Suchfunktionen zur Verfügung, mit denen Sie u. a. über Websites oder Dateisysteme nach Knowledge-Lösungen suchen können.
- Erstellen Sie "empfohlene Dokumente", die in der Self-Service-Schnittstelle angezeigt werden, wenn Benutzer nach Knowledge-Lösungen suchen.
- Suchen von Tickets mit der Funktion "Ähnliche suchen". Die FAST ESP-Suchmaschine ist hierfür erforderlich.
- 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 Service Desk Manager, einschließlich Feldzuordnung und Suchkonfiguration für Anfragen und Issues.

Optionen für Self-Service-Knowledge

Kunden und Mitarbeiter, die CA Service Desk Manager 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. 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 Benutzer 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:

Zusammenfassung

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 Vorfall
- Neuer Incident auf Grundlage dieses Dokuments
- Druckbare Version

Weitere Informationen:

[Erstellen von Kommentartypen](#) (siehe Seite 883)

[Konfigurieren von Self-Service-Richtlinien](#) (siehe Seite 943)

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 Service Desk Manager-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 930).

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 Problenumgehung
 - 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 Benutzer

In der Schnittstelle "Knowledge-Dokumente", die über den Knoten "Knowledge-Dokumente" im USDK>-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.

Dokument-Posteingang

Der Knowledge-Dokument-Posteingang (und der Gruppen-Posteingang) im CA Service Desk Manager-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 Benutzers. 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 Service Desk Manager-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 Benutzer zugewiesen wird, eröffnen die Standard-Datenpartitionseinschränkungen dem Benutzer 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.

Knowledge-Dateien

Eine *Knowledge-Datei* ist eine durchsuchbare Textdatei (.pdf, .zip, .xls, .exe, .html, .img, .msg, .ppt, .rtf, .txt, .avi, .doc und .xml), die mit einer Kategorie verknüpft ist und mit anderen Kategorien verwandt sein kann.

Knowledge-Dateien sind flexibel und ermöglichen die schnelle Nutzung von Knowledge einer externen Ressource, ohne dass die Informationen in einem strukturierten Knowledge-Dokument zusammengeführt werden müssen. Zum Beispiel kann ein Analyst Knowledge von einem Lieferanten verwenden, das erläutert, wie ein Drucker repariert wird und dieses Knowledge als Knowledge-Datei in einer Knowledge-Kategorie mit dem Namen "Drucker" speichern.

Eine Knowledge-Datei bietet Benutzern viele Möglichkeiten. Beispielsweise können sie eine Datei ersetzen, in ein Knowledge-Dokument umwandeln und an einen anderen Speicherort laden. Es können sowohl traditionelle als auch erweiterte Suchoptionen verwendet werden, um in einer Datei nach Knowledge zu suchen.

Alle Dateien werden im Knowledge-Datei-Repository gespeichert, wobei der Administrator dafür sorgt, dass Benutzer schnell und sicher auf die Dateien zugreifen können.

Hinweis: Informationen zum Hinzufügen von Knowledge-Dateien an ein Repository finden Sie unter "Anhangsbibliothek" in der *Online-Hilfe*.

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 "Anhänge".
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 Repositories den Namen der Datei auszuwählen, die angehängt werden soll.

Der Name wird auf der Registerkarte "Anhänge" angezeigt.

Hinweis: Wenn Sie ein Knowledge-Dokument mit einem oder mehreren Anhängen kopieren, werden nur Dateien mit dem Dokument kopiert, die aus der Liste "Repositories" in der Bibliothek hochgeladen und angehängt wurden. Dateianhänge, die aus anderen Speicherorten hochgeladen wurden, werden nicht mit dem Dokument kopiert.

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 Service Desk Manager 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 Benutzer 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 Endbenutzer 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 Benutzer 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 864)

[Erstellen von Aktionsinhalten \(Aktions-URL\)](#) (siehe Seite 865)

[Erstellen von Aktionsinhalt \(interner HTML\)](#) (siehe Seite 866)

[Bearbeiten von Aktionsinhalten](#) (siehe Seite 866)

[Suchen nach Aktionsinhalten](#) (siehe Seite 867)

Anzeigen von Aktionsinhalten

Sie können die Details der Live-URLs anzeigen, mit denen Sie Aktionen für Endbenutzer 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 Aktionseinhalten (Aktionen-URL)

Sie können Aktionseinhalte für Knowledge-Dokumente erstellen. Diese Aktionen-URLs können eine Live-Website starten, die für alle Benutzer Ihres Systems zugänglich ist. Sie können auch Aktionen-URLs mit automatischen Aufgaben auf Ihrem Server verknüpfen und diese Skripts in Ihre Knowledge-Dokumente, Strukturdokumente, Dokumentvorlagen und Knowledge-Foren einbetten.

So erstellen Sie Aktionseinhalte (Aktionen-URLs)

1. Wählen Sie auf der Registerkarte "Administration" die Option "Knowledge" > "Aktionseinhalte" aus.

Die Seite "Aktionseinhalte - Liste" wird angezeigt.

2. Klicken Sie auf "Neu erstellen".

Die Seite "Neuen Aktionseinhalt erstellen" wird angezeigt.

3. Füllen Sie die Felder aus. The following fields require explanation:

Code

Gibt eine eindeutige Kennung für diesen Aktionseinhalt an.

Internes HTML verwenden

[Erstellt eine interne Verknüpfung](#) (siehe Seite 866) in der Anwendung, die dynamisch Informationen, wie Benutzernamen und Sitzungs-ID, von Knowledge-Dokumenten an Drittanbieteranwendungen weitergibt. Wählen Sie diese Option nicht aus.

Aktionen-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 Aktionseinhalt 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 Benutzerattribute, wie den Benutzernamen, in die Zielanwendung (z. B. <http://www.ca.com?USERNAME=BBB>). Benutzerattribute 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 die folgenden Felder 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 Benutzer diese Aktionsinhalts-Verknüpfung innerhalb eines Knowledge-Dokuments anklickt, werden Benutzerattribute (z. B. der Benutzername) 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 "Aktionseinhalt - Details" wird angezeigt.
3. Klicken Sie auf "Bearbeiten".
Die Seite "Aktionseinhalt aktualisieren" wird angezeigt.
4. Bearbeiten Sie die Felder nach Bedarf.
5. Klicken Sie auf "Speichern".
Der Aktionseinhalt 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 "Aktionseinhalte - 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 Aktionseinhaltselements an.

Status

Zeigt an, ob dieses Element aktiv oder inaktiv ist.

Code

Gibt eine eindeutige Kennung für diesen Aktionseinhalt 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 Service Desk Manager 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 Benutzer in der Dokumentberechtigung zu berücksichtigen, die dem Dokument später im Genehmigungsvorgang zugeteilt werden könnten. Benutzer jener Gruppe haben nicht unbedingt die Berechtigung, das Dokument anzusehen. Wenn das Dokument einem bestimmten Benutzer zugewiesen wird, eröffnen die Standard-Datenpartitionseinschränkungen dem Benutzer 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: Benutzer 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 Benutzern 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 Benutzern bearbeitet werden, die über volle Berechtigung verfügen.

Legt fest, dass jeder dafür schreibberechtigte Benutzer 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 Benutzern mit voller Berechtigung bearbeitet werden.

Legt fest, dass ein Benutzer mit allen Berechtigungen veröffentlichte Dokumente bearbeiten kann.

Benutzer mit allen Berechtigungen können die Attribute des veröffentlichten Dokuments ändern.

Legt fest, dass alle für das Dokument schreibberechtigte Benutzer 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 Benutzer die Veröffentlichung eines Dokuments rückgängig machen muss, bevor er es bearbeitet.

Klicken Sie auf "Speichern".

Der Genehmigungsvorgang wird definiert.

Erstellen einer Genehmigungsprozessvorlage

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. The following fields require explanation:

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 872).

Klicken Sie auf "Speichern".

Die Vorlage für den Genehmigungsvorgang wird erstellt.

Weitere Informationen:

[Hinzufügen von alternativen Zuständigen zu einer Aufgabe](#) (siehe Seite 872)

[Bearbeiten von Vorlagen für den Genehmigungsvorgang](#) (siehe Seite 873)

[Suchen nach Vorlagen für den Genehmigungsvorgang](#) (siehe Seite 873)

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>" auswählen, 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 Service Desk Manager zu verwenden. Klicken Sie dazu auf der Listenseite auf die Schaltfläche "Exportieren".

Definitionen für den Dokumentstatus

Sie können benutzerdefinierte Dokumentstati hinzufügen und löschen sowie die Namen und Beschreibungen von vordefinierten Dokumentstati ändern.

Weitere Informationen:

[Erstellen eines neuen Dokumentstatus](#) (siehe Seite 874)

[Suchen nach dem Dokumentstatus](#) (siehe Seite 875)

[Bearbeiten des Dokumentstatus](#) (siehe Seite 875)

Erstellen eines neuen Dokumentstatus

Sie können in Ihrem CA Service Desk Manager-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 Service Desk Manager 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 Endbenutzer, die nach Lösungen suchen, Probleme schneller lösen. Sie können Problem eigenständig lösen, was einen Nutzen für Organisation darstellt.

Automatisierte Richtlinien arbeiten mit der Funktion "Ereignisse und Makros".

Weitere Informationen:

[Anzeigen von Automatisierungsrichtlinien](#) (siehe Seite 876)

[Einrichten von Automatisierungsrichtlinien](#) (siehe Seite 878)

[Erstellen von Automatisierungsrichtlinien](#) (siehe Seite 878)

[Bearbeiten von Automatisierungsrichtlinien](#) (siehe Seite 879)

[Planen von Automatisierungsrichtlinien](#) (siehe Seite 880)

[Anzeigen von Berichten zu Lebenszyklusrichtlinien für Dokumente](#) (siehe Seite 880)

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>" auswählen, 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 Bedingungsereignis der gespeicherten Abfrage auf dem CA Service Desk Manager-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 Dokumentenbearbeiter 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 Service Desk Manager zu verwenden. Klicken Sie dazu auf der Listenseite auf die Schaltfläche "Exportieren".

Weitere Informationen:

[Anzeigen von Berichten zu Lebenszyklusrichtlinien für Dokumente](#) (siehe Seite 880)

[Planen von Automatisierungsrichtlinien](#) (siehe Seite 880)

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 Server 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 Benutzer Dokumente während ihres Lebenszyklus anzeigen und durchsuchen können.
3. Auf der Seite "Automatisierungsrichtlinien - Liste" können Sie die Standardrichtlinien bearbeiten oder eigene Richtlinien definieren.

Hinweis: Wenn ein Dokument zur Bearbeitung geöffnet ist, dann wird auf der Registerkarte "Attribute" standardmäßig ein Kontrollkästchen angezeigt, bei dessen Aktivierung alle Lebenszyklusrichtlinien ignoriert (oder übersprungen) werden. 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 Service Desk Manager 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 Service Desk Manager 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>" auswählen, 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 Richtliniennamen und Aktionsinhalt an.

Attribute

Zeigt die Eigenschaften des Dokuments an, auf die sich die zugewiesenen Richtlinien auswirken.

Knowledge-Dokumentsteuerung

Wenn Benutzer ein Knowledge-Dokument öffnen, können sie Kommentare hinzufügen, Knowledge absenden und ihre Knowledge-Strukturdokumente ansehen. Sie können auch den Inhalt und die Form von Dokumenten durch das Auswählen einer Vorlage näher bestimmen.

So können Administratoren kontrollieren, wie Benutzer mit Dokumenten interagieren:

- Definieren Sie die [Kommentartypen](#) (siehe Seite 882), die in Knowledge-Dokumenten und Dropdown-Listen in der Endbenutzerschnittstelle erscheinen.
- Geben Sie Dokumenteneinstellungen (siehe Seite 948) an, die sich auf Kommentare, das Absenden von Knowledge und auf das Ansehen von Dokumenten beziehen.
- Erstellen Sie [Dokumentvorlagen](#) (siehe Seite 887), die den Inhalt und die Form von Dokumenten bestimmen.
- [Exportieren](#) (siehe Seite 831) (oder importieren) Sie Knowledge-Inhalte aus anderen Ressourcen oder Systemen.
- Verwalten Sie die Möglichkeiten zur [Versionskontrolle](#) (siehe Seite 815) von Dokumenten.
- Verwalten Sie die [Planung für Knowledge-Dokumente](#) (siehe Seite 819).

Siehe auch

[Kommentartypen](#) (siehe Seite 882)

[Dokumentvorlagen](#) (siehe Seite 887)

[Erstellen von Verknüpfungen für Knowledge-Dokumente](#) (siehe Seite 895)

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>" auswählen, 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 Benutzeransicht anzeigen

Zeigt den Kommentar in verschiedenen Listenansichten auf der Benutzeroberfläche an.

Nachverfolgung erforderlich

Gibt an, ob der Benutzer auf diesen Kommentar reagieren muss.

Zeit bis Abschluss (Tage)

Legt fest, wie viele Tage der Benutzer 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

Löscht den Suchfilter.

Neu erstellen:

Erstellt einen Kommentartyp.

Hinweis: Sie können Ergebnislisten nach Excel exportieren, um sie außerhalb von CA Service Desk Manager 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. The following fields require explanation:

Zeit bis Abschluss (Tage)

Legt fest, wie viele Tage der Benutzer diesen Kommentartyp nachverfolgen muss.

In Benutzeransicht anzeigen

Zeigt den Kommentar in verschiedenen Listenansichten auf der Benutzeroberfläche an.

Nachverfolgung erforderlich

Gibt an, ob der Benutzer 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 Service Desk Manager 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 Benutzer 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 Benutzer 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 Benutzer Kommentare für das Dokument absenden können. Die Benutzer 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 Benutzer Kommentare für das Dokument absenden können. Die Benutzer können keine Kommentare anzeigen, die mit dem geöffneten Dokument bereits verknüpft sind.
- **Weder Absenden noch Anzeigen von Kommentaren zulassen** - Verweigert Benutzern die Möglichkeit, Kommentare abzusenden oder anzusehen. Das Kommentarfeld wird in einem geöffneten Dokument nicht angezeigt.

Knowledge absenden

Legt das Repository für vom Benutzer abgesendeten Dokumente. Die Liste wird automatisch mit den Namen der Repositories ausgefüllt, die im Bereich "Anhangsbibliothek" definiert wurden.

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 Benutzer 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 Service Desk Manager aktualisiert oder erstellt wurden. Wenn Sie Dokumente von CA Service Desk Manager 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 Benutzern 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 894), 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: Schnellbearbeitung

Die Standardvorlagen werden verwendet, wenn Sie Knowledge-Dokumente und Knowledge-Strukturdokumente 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: Schnellobarbeitung

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.

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>" auswählen, 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 Service Desk Manager 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 "Verwaltung".
Die Seite "Administration" wird angezeigt.
2. Klicken Sie auf "Knowledge" > "Dokumente" > "Dokumentvorlagen".
Die "Dokumentvorlagen-Liste" wird angezeigt.
3. Führen Sie *einen* der folgenden Schritte 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 Service Desk Manager 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 Benutzeransicht 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 901) 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 früheren Berechtigungen für diese Kategorie gelöscht werden.

Allen Benutzern Schreibberechtigung erteilen

Gibt an, dass alle Benutzer Schreibzugriff auf die Kategorie haben. Schreibzugriff bedeutet, dass Sie diese Kategorie bearbeiten oder löschen können.

Hinweis: Das Kontrollkästchen "Allen Benutzern Leseberechtigung erteilen" wird automatisch aktiviert, wenn Sie das Kontrollkästchen "Allen Benutzern Schreibberechtigung erteilen" aktivieren.

Allen Benutzern Leseberechtigung erteilen

Gibt an, dass alle Benutzer Lesezugriff auf die Kategorie haben. Leseberechtigung bedeutet, dass Sie die Kategorie anzeigen, jedoch nicht bearbeiten oder löschen können. Benutzer mit Administratorrechten können einen Ordner bearbeiten, selbst wenn die ihnen zugeordnete Gruppe dies nicht kann. Gehört ein Benutzer 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 Benutzer Schreibzugriff).

Hinweis: Das Kontrollkästchen "Allen Benutzern Leseberechtigung erteilen" wird automatisch aktiviert, wenn Sie das Kontrollkästchen "Allen Benutzern 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 901)

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 Benutzer 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.

Anfrage-/Incident-/Problembereich

Bezeichnet einen Anfrage-/Incident-/Problembereich, den Ihr Administrator definiert, um einen Zuständigkeitsbereich zu bezeichnen. Klicken Sie auf das Suchsymbol, um aus den verfügbaren Bereichen auszuwählen.

Problemanfragenkategorie

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 901) 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 906) "Allen Benutzern Schreibberechtigungen erteilen" und "Allen Benutzern 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 im Kontextmenü "Kategorie einfügen".

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 Benutzern 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 Benutzern Schreibberechtigung erteilen

Gibt an, dass alle Benutzer Schreibzugriff auf die Kategorie haben. Schreibzugriff bedeutet, dass Sie diese Kategorie bearbeiten oder löschen können.

Hinweis: Das Kontrollkästchen "Allen Benutzern Leseberechtigung erteilen" wird automatisch aktiviert, wenn Sie das Kontrollkästchen "Allen Benutzern Schreibberechtigung erteilen" aktivieren.

Allen Benutzern Leseberechtigung erteilen

Gibt an, dass alle Benutzer Lesezugriff auf die Kategorie haben. Leseberechtigung bedeutet, dass Sie die Kategorie anzeigen, jedoch nicht bearbeiten oder löschen können. Benutzer mit Administratorrechten können einen Ordner bearbeiten, selbst wenn die ihnen zugeordnete Gruppe dies nicht kann. Gehört ein Benutzer 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 Benutzer Schreibzugriff).

Hinweis: Das Kontrollkästchen "Allen Benutzern Leseberechtigung erteilen" wird automatisch aktiviert, wenn Sie das Kontrollkästchen "Allen Benutzern 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 Benutzern 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 909)

[Webbasierte Berichte](#) (siehe Seite 911)

[Rollenbasierte Berichts-Webformulare](#) (siehe Seite 911)

Knowledge-Berichtskarte

Die Knowledge-Berichtskarte zeigt Informationen über den Wissensbeitrag jedes Endbenutzers 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 Endbenutzern 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 Service Desk Manager-Installation auf dem BusinessObjects-Berichterstellungs-Server bereitgestellt.

Sie werden entweder mit BusinessObjects Web Intelligence oder Crystal Reports entwickelt. Autorisierte Benutzer können Berichte auf der CA Service Desk Manager-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 Benutzern die empfohlenen Dokumente in der Liste ganz oben anzuzeigen.

Hinweis: Für ein Dokument können andere Berechtigungen vorhanden sein als für die damit verknüpften Anlagen.

- Schalten Sie auf die SCHNELLE Suchmaschine um (falls installiert).

Siehe auch:

[KT-Such-Engine](#) (siehe Seite 912)

[FAST ESP-Suche](#) (siehe Seite 925)

[Empfohlene Dokumente](#) (siehe Seite 929)

[Einrichten von Standard-Sucheinstellungen](#) (siehe Seite 933)

KT-Such-Engine

Nachdem Sie CA Service Desk Manager 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 912)

Verwenden der Knowledge-Management-Suche

Nachdem Sie CA Service Desk Manager 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 Benutzerrollen festlegen. Standardmäßig sind Knowledge-Dokumente für alle Benutzerrollen zugänglich.

Wenn CA Service Desk Manager für FAST ESP-Suche konfiguriert wird, können Sie auf die Standardsuch-Engine in "Optionsmanager" umschalten.

So verwenden Sie die Knowledge-Management-Suche:

1. Klicken Sie auf die Registerkarte "Verwaltung".
Die Administrationskonsole wird angezeigt.
2. Klicken Sie auf "Optionsmanager" > "Such-Engine".
Die Liste der Optionen wird angezeigt.
3. Klicken sie auf "ebr_version".
Die Seite "Optionen aktualisieren" 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".

Hinweis: Weitere Informationen über die Installation und Konfiguration von FAST ESP finden Sie im *Implementierungshandbuch*.

Siehe auch:

[Füllwörter, Synonyme und Sonderbegriffe](#) (siehe Seite 914)
[Erstellen von Füllwörtern](#) (siehe Seite 915)
[Bearbeiten von Füllwörtern](#) (siehe Seite 916)
[Anzeigen von Füllwörtern](#) (siehe Seite 916)
[Erstellen von Sonderbegriffen](#) (siehe Seite 917)
[Bearbeiten von Sonderbegriffen](#) (siehe Seite 918)
[Anzeigen von Sonderbegriffen](#) (siehe Seite 918)
[Erstellen von Synonymen](#) (siehe Seite 919)
[Anzeigen von Synonymen](#) (siehe Seite 920)
[Bearbeiten von Synonymen](#) (siehe Seite 920)
[Einstellungen für Suchsyntax](#) (siehe Seite 921)

Füllwörter, Synonyme und Sonderbegriffe

Hinweis: Füllwörter, Synonyme, und Sonderbegriffe sind nur in Verbindung mit der Standardsuch-Engine verfügbar. Die optionale FAST ESP Such-Engine verwaltet über einen internen Erkennungsmechanismus Füllwörter, Synonyme und Sonderbegriffe. Informationen zur Implementierung finden Sie in der Dokumentation zu FAST ESP.

Sie können Wörter (Synonyme, Füllwörter, und besondere Termini) festlegen, die sich auf Freitext- und Schlüsselwortsuchen in CA Service Desk Manager auswirken. Das Hinzufügen oder Entfernen der folgenden Begriffe hat eine drastische Auswirkung auf die Suchergebnisse, die dem Benutzer 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 Benutzer 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 "Füllwörter - Listenseite" 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 "Füllwörter - Listenseite". 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 einer "Füllwörter - Listenseite" 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 "Füllwörter - Listenseite".

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.

Anzeigen von Füllwörtern

Sie können die Zusammenfassung für jedes Füllwort auf der "Füllwörter - Listenseite" 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 "Füllwörter - Listenseite" 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 "Füllwörter - Listenseite" können Sie die folgenden Aufgaben ausführen:

- [Erstellen von Füllwörtern](#) (siehe Seite 915)
- [Bearbeiten von Füllwörtern](#) (siehe Seite 916)

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 "Sonderbegriffe - Listenseite" 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/die Sie als Sonderbegriff definieren möchten.
4. Klicken Sie auf "Speichern".

Das Fenster "Sonderbegriff erstellen" wird geschlossen und die "Sonderbegriff - Detailseite" 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 "Sonderbegriffe - Listenseite".

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 erstellen" wird geschlossen und die "Sonderbegriff - Detailseite" geöffnet, so dass Sie das Wort oder die Wortfolge überprüfen können, das bzw. die Sie hinzugefügt haben. Der neue Sonderbegriff erscheint auf der "Sonderbegriffe - Listenseite".

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 "Sonderbegriffe - Listenseite" 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 "Füllwort" keine Eingaben vorgenommen haben, werden alle systemdefinierten Füllwörter angezeigt.

Auf der "Füllwörter - Listenseite" können Sie die folgenden Aufgaben ausführen:

- [Erstellen von Sonderbegriffen](#) (siehe Seite 917)
- [Bearbeiten von Sonderbegriffen](#) (siehe Seite 918)

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" > "Sonderbegriffe".
Die "Synonyme - Listenseite" 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 "Sonderbegriff erstellen" wird geschlossen und die "Sonderbegriff - Detailseite" geöffnet, so dass Sie das Wort oder die Wortfolge überprüfen können, das bzw. die Sie hinzugefügt haben. Das neue Synonym erscheint auf der "Synonyme - Listenseite".

Anzeigen von Synonymen

Sie können für jeden Sonderbegriff eine Zusammenfassung anzeigen.

Um Synonyme anzusehen, wählen Sie auf der Registerkarte "Administration" die folgenden Optionen aus: "Knowledge" > "Suche" > "KT-Such-Engine" > "Synonyme".

Die "Synonyme - Listenseite" 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 "Füllwörter - Listenseite" können Sie die folgenden Aufgaben ausführen:

- [Erstellen von Synonymen](#) (siehe Seite 919)
- [Bearbeiten von Synonymen](#) (siehe Seite 920)

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 "Sonderbegriff" 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 "Sonderbegriff - Detailseite" geöffnet, so dass Sie das Wort oder die Wortfolge überprüfen können, das bzw. die Sie hinzugefügt haben. Der neue Sonderbegriff erscheint auf der "Sonderbegriffe - Listenseite".

Einstellungen für Suchsyntax

Hinweis: Die Funktion "Einstellungen für Suchsyntax" ist nur mit der STANDARD-KT-Suchmaschine verfügbar.

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 Benutzer die Knowledge Base, vergleicht die Software die Schlüsselwörter aus der Abfrage des Benutzers 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.

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 Benutzer die Knowledge Base, vergleicht die Software die Schlüsselwörter aus der Abfrage des Benutzers mit den Schlüsselwörtern, die durch die Knowledge Base analysiert wurden, und generiert dann eine Ergebnisliste.

Hinweis: FAST ESP verfügt über einen eigenen internen Optimierungsmechanismus, um relevante Ergebnisse anzuzeigen. Deshalb erscheinen die Einstellungen für die Suchsyntax (mit Ausnahme von "Gültiger Zeichenbereich") nicht in der Knowledge-Management-Administrationsschnittstelle, wenn die optionale FAST ESP Such-Engine installiert und konfiguriert ist.

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 Service Desk Manager-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 925) verstehen, damit Sie die Erwartungen der Benutzer 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-záéíóúñ
Französisch	a-zàâçèêëîïôû
Brasilianisches Portugiesisch	a-zãäãçéêíóü
Italienisch	a-zàèéìîù
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.

Nein

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.

Nein

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.

Nein

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 921) 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.

Hinweis: FAST ESP ist eine optionale Such-Engine, die Multibyte-Zeichen (MBCS) unterstützt und mit der Sie diese Einschränkungen umgehen können. Weitere Informationen zum Einrichten der FAST ESP-Such-Engine finden Sie im *Implementierungshandbuch*.

FAST ESP-Suche

Die FAST ESP-Suchmaschine ist eine neue optionale Suchmaschine, die Analysten und Knowledge-Managern die Suche in den folgenden Knowledge-Quellen ermöglicht:

- Knowledge-Dokumente mit mehreren Anhängen
- Analysten-Foren
- Knowledge-Dateien (.pdf, .zip, .xls, .exe, .html, .img, .msg, .ppt, .rtf, .txt, .avi, .doc und .xml)

- Freier Textinhalt (unstrukturiertes Knowledge) in Bezug auf ein Problem oder eine Lösung
- Service Desk-Issues, Incidents, Anfragen, Probleme und Änderungsaufträge
- Websites oder Dateisysteme. Die Suchmaschine katalogisiert und indiziert die Inhalte externer Repositories.

Für die Standardkonfiguration gelten die folgenden Einschränkungen:

- FAST kann nur zwei Suchabfragen pro Sekunde bearbeiten.
Hinweis: Informationen zur Erweiterung dieser Funktion erhalten Sie von CA Services.
- Die maximale Anzahl der Dokumente, die in der Knowledge Base indiziert werden kann, beträgt zwei Millionen.
- Für ein Dokument können andere Berechtigungen vorhanden sein als für die damit verknüpften Anhänge.

Standardmäßig wird CA Service Desk Manager nicht für die Verwendung von FAST ESP konfiguriert. Wenn Sie die FAST ESP-Suchmaschine installiert haben, können Sie sie als Standardsuchmaschine für Knowledge-Management-Suchvorgänge auswählen. Standardeinstellungen für die Suchmaschine sind im Optionsmanager definiert.

Hinweis: Weitere Informationen über die Installation und Konfiguration von FAST ESP finden Sie im *Implementierungshandbuch*.

Verwenden der FAST-Such-Engine

Wenn CA Service Desk Manager konfiguriert wird, um die Standardsuch-Engine zu verwenden, können Sie die FAST-Such-Engine aktivieren, vorausgesetzt sie ist installiert. Die FAST-Such-Engine sorgt für zusätzliche Suchfunktionen, mit denen Benutzer u. a. über Websites oder Dateisysteme nach Knowledge-Lösungen suchen können.

Führen Sie diese Schritte auf dem primären oder sekundären Server von CA Service Desk Manager durch.

Hinweis: Weitere Informationen über die Installation und Konfiguration von FAST ESP finden Sie im *Implementierungshandbuch*.

So verwenden Sie die FAST-Such-Engine:

1. Klicken Sie auf die Registerkarte "Verwaltung".
Die Administrationskonsole wird angezeigt.
2. Klicken Sie in der Baumstruktur auf der linken Seite auf "Optionsmanager" > "Such-Engine".
Die Liste der Optionen wird angezeigt.
3. Geben Sie die folgenden Einstellungen an:

ebr_version

Gibt die FAST-Such-Engine an.

ebr_search_engine_baseport

Gibt den Basisport des dedizierten Servers an, auf dem die FAST ESP-Such-Engine installiert ist. Berücksichtigen Sie beim Festlegen des Basisports Folgendes:

- Stellen Sie sicher, dass die Portnummer, die Sie hier eingeben, mit dem Basisport übereinstimmt, den Sie während der FAST ESP-Installation angegeben haben (Standardport ist 13000).
- FAST ESP verwendet den Basisport, um statische Ports zu berechnen.
- Auf jedem Host sollten zwischen dem FAST ESP-Basisport und der FAST ESP-Installation mindestens 4000 Ports liegen, da FAST ESP die statischen Ports relativ zum Basisport festlegt (also zur Portnummer der Administrationsschnittstelle, falls diese gleich 16000 ist).
- Vergewissern Sie sich, dass im Portbereich keine Konflikte mit anderen vom Server verwendeten Produkten oder Diensten auftreten.
- Ports mit Nummern unter 1024 können Sie nicht verwenden.
- Da der Lizenzserver stets die Portnummer 27000 verwendet, wird empfohlen, *keinen* Basisport im Nummernbereich zwischen 23000 und 27000 zu verwenden.

Wichtig! Alle Hosts benötigen uneingeschränkten Netzwerkzugriff im gesamten Portnummernbereich (z. B. Ports 13000 bis 16999).

ebr_search_engine_host

Gibt den vollständig qualifizierten Domänenname oder die IP-Adresse (empfohlen) des dedizierten Servers an, auf dem die FAST ESP-Such-Engine installiert ist.

4. Klicken Sie auf "Speichern" und dann auf "Aktualisieren".

Die Seite "Optionen - Detail" wird gemäß Ihrer Auswahl aktualisiert.

5. Klicken Sie auf "Fenster schließen".
6. Halten Sie den Dienst namens CA Service Desk Manager Server an, und starten Sie ihn erneut.
7. Führen Sie den Befehl *pdm_k_reindex* (siehe Seite 1067) *index factory:all* aus, um Knowledge-Dokumente und Tickets in FAST ESP zu indizieren.

Wichtig! Wenn Sie die FAST ESP-Dienste aus irgendwelchen Gründen anhalten und erneut starten, *müssen* Sie auch den Indizierungsdaemon (*bpeid_nxd*) anhalten und neu starten. FAST ESP *muss* zum Starten des Daemons ausgeführt werden. Andernfalls kommt es in *stdlog* und beim Erstellen von oder Suchen nach Knowledge-Dokumenten zu Fehlern.

Weitere Informationen:

["pdm k_reindex" — Dienstprogramm zur Knowledge-Neuindizierung](#) (siehe Seite 1067)

[Verwenden von pdm k_reindex](#) (siehe Seite 1069)

[Verwenden von "pdm k_reindex" mit FAST ESP](#) (siehe Seite 1070)

Suchvorgänge 'Ähnliche suchen'

Sie können nach ähnlichen Tickets auf der Registerkarte 'Knowledge' für Tickets suchen, einschließlich Issues, Anfragen, Incidents, Problemen und Änderungsaufträgen. "Ähnliche suchen" ist nur aktiviert, wenn Sie FAST ESP installieren. Mit dieser Funktionalität können Sie nach ähnlichen Tickets suchen, indem Sie die Ticket-Zusammenfassung und Beschreibung als eine Suchanfrage verwenden. Nach ähnlichen Tickets zu suchen, hilft Ihnen dabei, die Anzahl von Tickets in Ihrer Unterstützungsumgebung zu verringern.

Wichtig! Wenn Sie 'Ähnliche suchen' verwenden möchten, müssen Sie [pdm k_reindex](#) (siehe Seite 1070) ausführen, um die Dokumente zu synchronisieren. Sie müssen außerdem alle CA Service Desk Manager-Objekte, wie z. B. Verbindungsaufrufe, Änderungsanforderungen, Änderungsaufträge und so weiter, neu indizieren.

Verwenden der Suche "Ähnliche finden" für Tickets

Sie können auf der Registerkarte "Knowledge" eines Tickets nach ähnlichen Tickets suchen, wie beispielsweise einem Incident. "Ähnliche suchen" ist nur aktiviert, wenn Sie FAST ESP installieren. Sie suchen nach ähnlichen Tickets, um zu vermeiden, dass redundante Tickets in Ihrer Support-Umgebung erstellt werden.

So finden Sie ähnliche Tickets

1. Öffnen Sie ein Ticket, z. B. einen Incident.
Die Seite "Incident - Detail" wird angezeigt.
2. Klicken Sie auf der Registerkarte "Knowledge" auf "Ähnliche suchen".
Eine Liste ähnlicher Tickets wird angezeigt, die auf der aktuellen Ticket-Zusammenfassung und Ticket-Beschreibung basiert.

Empfohlene Dokumente

Hinweis: CA Service Desk Manager-Benutzer 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 Benutzer 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 930)

[Bearbeiten von Bedingungen für empfohlene Dokumente](#) (siehe Seite 931)

[Anzeigen von empfohlenen Dokumenten](#) (siehe Seite 932)

[Suchen empfohlener Dokumente](#) (siehe Seite 932)

Erstellen von empfohlenen Dokumenten

Administratoren können empfohlene Dokumente erstellen, die Benutzer 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".

Die Liste "Empfohlene Dokumente" 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 931) 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.

Keywords

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 Benutzer 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 930)
- [Bearbeiten von Bedingungen für empfohlene Dokumente](#) (siehe Seite 931)
- [Suchen von "Empfohlenen Dokumenten"](#) (siehe Seite 932)

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>" auswählen, 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 Wunsch 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 Benutzer über das Suchfeld nach Knowledge suchen.

Hinweis: Diese Suchoptionen werden von persönlichen Sucheinstellungen überschrieben, die von Benutzern 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
- Zusammenfassung
- Problem
- Lösung
- Anhänge

Sucheinstellungen für alle Quellen

Spezifiziert ob Suchen alle Wissensquellen einschließen können. Beispiel: Knowledge-Kategorien und Anfragebereiche.

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, Anfrage).

- 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 Service Desk Manager

Die folgenden Konfigurationsoptionen sind für die CA Service Desk Manager-Integration verfügbar:

Feldzuordnung

Gibt an, welche CA Service Desk Manager-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.

Anfrage/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 935)

[Definieren der Issue-Suchkonfiguration](#) (siehe Seite 938)

[Definieren der Suchkonfiguration für Anfragen/Incidents/Probleme](#) (siehe Seite 939)

[Knowledge-Vorschläge](#) (siehe Seite 940)

[Definieren von Issue-Kategorien](#) (siehe Seite 941)

[Definieren von Anfrage-/Incident-/Problembereichen](#) (siehe Seite 942)

[Konfigurieren von Self-Service-Richtlinien](#) (siehe Seite 943)

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 -Anfragen 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 -Anfragen 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 Benutzer die von Knowledge-Management erstellten Service Desk-Issues oder -Anfragen manuell ausfüllen.

Standard: Dieses Kontrollkästchen ist aktiviert.

Service Desk

Bezeichnet die Felder in Issues oder Anfragen, 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 das Issue oder die Anfrage 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 das Issue oder die Anfrage 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 einer Anfrage 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 einer Anfrage ausgefüllt werden soll.
- **Standard:** Problem.

Leere Service Desk-Felder ausfüllen

Legt fest, welche leeren Felder in einem Service Desk-Issue oder einer -Anfrage 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 "Anfragebereich" in Service Desk entsprechen, sind aktiviert.

Service Desk-Werte überschreiben

Legt fest, welche Felder in einem Service Desk-Issue oder einer -Anfrage 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 Service Desk Manager-Integration" > "Issue – Suchkonfiguration" aus.

Die Seite "Integration von CA Service Desk Manager" wird angezeigt.

2. Wählen Sie die Felder aus, die für Suchvorgänge in der Knowledge Base verfügbar sein sollen.

- Zusammenfassung
- Beschreibung
- Konfigurationselement
- 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 Anfragen/Incidents/Probleme

Sie können die Felder in Anfragen, 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 einer Anfrage, einem Incident oder einem Problem, die für Knowledge Base-Suchläufe verwendet werden sollen:

1. Wählen Sie auf der Registerkarte "Administration" die Option "Knowledge" > "CA Service Desk Manager-Integration" > "Anfrage/Incident/Problem – Suchkonfiguration" aus.
Die Seite "Integration von CA Service Desk Manager" wird angezeigt.
2. Wählen Sie die Felder aus, die für Suchvorgänge in der Knowledge Base verfügbar sein sollen.

- Zusammenfassung
- Beschreibung
- Konfigurationselement
- Relevanz
- Impact
- Urgency
- Priorität
- Anforderungsbereich
- 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 einer Anfrage, einem Incident oder einem 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 Benutzer 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 Anfragebereiche 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 Anfragebereiche an, für die den Mitarbeitern und Kunden auf der Self-Service-Benutzeroberfläche Knowledge entweder vorgeschlagen oder nicht vorgeschlagen wird. Der Self-Service-Benutzer darf die Anfragebereiche nicht bearbeiten, denn sie sind schreibgeschützt.

3. Klicken Sie auf *eine* der folgenden Schaltflächen:

Hinzufügen

Fügt der Liste den markierten Anfragebereich hinzu.

Entfernen

Entfernt den markierten Anfragebereich aus der Liste.

Alle entfernen

Entfernt alle Anfragebereiche aus der Liste.

Speichern

Speichert die Informationen zu den Anfragebereichen in der Knowledge Base.

Issue-Kategorien werden definiert.

Definieren von Anfrage-/Incident-/Problembereichen

Sie können Anfrage-, 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 Anfrage-/Incident-/Problembereiche:

1. Navigieren Sie auf der Registerkarte "Administration" zu "Knowledge" > "CA Service Desk Manager-Integration" > "Knowledge vorschlagen" > "Anfrage-/Incident-/Problembereiche".

Die Seite "Knowledge für Anfrage-/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 Anfrage-/Incident-/Problembereiche vorgeschlagen werden soll (außer für die Bereiche, die in der Liste der Anfragebereiche definiert sind).

Nicht vorgeschlagen

Wählen Sie diese Option aus, wenn *keine* Knowledge-Elemente für Anfrage-/Incident-/Problembereiche vorgeschlagen werden sollen (außer für die Bereiche, die in der Liste der Anfragebereiche definiert sind).

Für alle Anfrage/Incident-/Problembereiche außer den folgenden:

Zeigt die Liste der Anfragebereiche an, für die den Mitarbeitern und Kunden auf der Self-Service-Benutzeroberfläche Knowledge entweder vorgeschlagen oder nicht vorgeschlagen wird. Der Self-Service-Benutzer darf die Anfragebereiche nicht bearbeiten, denn sie sind schreibgeschützt.

3. Klicken Sie auf *eine* der folgenden Schaltflächen:

Hinzufügen

Fügt der Liste den markierten Anfragebereich hinzu.

Entfernen

Entfernt den markierten Anfragebereich aus der Liste.

Alle entfernen

Entfernt alle Anfragebereiche aus der Liste.

Speichern

Speichert die Informationen zu den Anfragebereichen in der Knowledge Base.

Die Anfrage/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 Benutzerszenarien auswirken.

So konfigurieren Sie Self-Service-Richtlinien:

1. Navigieren Sie auf der Registerkarte "Administration" zu "Knowledge" > "CA Service Desk Manager-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 Benutzerszenarien:

- Benutzer hat kein vorgeschlagenes Dokument geöffnet.
- Benutzer hat ein vorgeschlagenes Dokument geöffnet.
- Benutzer hat ein vorgeschlagenes Dokument als Lösung für sein Problem akzeptiert.
- Benutzer 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 945)

[Festlegen der Einstellungen für Lösungsumfragen](#) (siehe Seite 947)

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 Benutzern
- 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 Benutzer 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 folgende Felder wie gewünscht 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 Benutzern 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 948)

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.

So konfigurieren Sie die allgemeinen Einstellungen:

1. Markieren Sie im linken Fenster der Registerkarte "Administration" die Option "Administration" > "Knowledge" > "System" > "Allgemeine Einstellungen".

Das Fenster "Allgemeine Einstellungen" wird geöffnet.

2. Füllen Sie folgende Felder wie gewünscht aus:

Eröffnungsbildschirm für das Suchwerkzeug:

Legt 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 in den Feldern 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 Service Desk Manager-Startseite aufgeführt werden.

Standard: 10

Schließen Sie globale Daten ein

Zeigt Daten aller Mandanten in "Beste Lösungen" an.

Standard: Aktiviert

Benachrichtigungen beim Indizieren der Dokumente

Legt einen Benutzer fest, der E-Mail-Benachrichtigungen über den Status oder das Auftreten von Fehlern beim Indizieren von Dokumenten erhält. Die E-Mail-Adresse des Benutzers 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 Bevollmächtigten für den Erhalt von Benachrichtigungen festlegen. Damit E-Mail-Benachrichtigungen an diesen Bevollmächtigten gesendet werden, muss auf der Seite "Kontakt – Benachrichtigung" die E-Mail-Adresse des Bevollmächtigten angegeben werden.

Klicken Sie auf "OK".

Die allgemeinen Einstellungen werden konfiguriert.

Kapitel 21: Verwalten von Support-Automatisierung

Dieses Kapitel enthält folgende Themen:

[Automatisieren des Supports in Ihrer Umgebung](#) (siehe Seite 951)
[Verwalten von Support-Automatisierung-Analysten](#) (siehe Seite 954)
[Support-Automatisierung-Benutzerverwaltung](#) (siehe Seite 960)
[Support-Automatisierung-Aktivitätsbenachrichtigungsverwaltung](#) (siehe Seite 965)
[Support-Automatisierung-Seitenanpassungen](#) (siehe Seite 966)
[Support-Automatisierung-Systemeigenschaften](#) (siehe Seite 969)
[Support-Automatisierung-Warteschlangenverwaltung](#) (siehe Seite 969)
[Verwaltung von Ticket-Vorlagen](#) (siehe Seite 972)
[Administrationseinstellungen](#) (siehe Seite 972)
[Anpassen von Support-Automatisierung-Tools](#) (siehe Seite 975)
[Sitzungsprotokoll-Verwaltung](#) (siehe Seite 983)
[Support-Automatisierung-Berichte](#) (siehe Seite 984)

Automatisieren des Supports in Ihrer Umgebung

Sie können eine Supportstrategie implementieren, indem Sie Prozesse und Tools miteinander kombinieren. CA Service Desk Manager 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*.

Endbenutzer-Client

Der Endbenutzer-Client verbindet Endbenutzer mit Analysten in Live-Unterstützungssitzungen. Endbenutzer kommunizieren mit Analysten über Web-Chat. Wenn Sie jedoch die Tools in der Support-Automatisierung-Analystenschnittstelle verwenden müssen, startet CA Service Desk Manager den Client auf dem Endbenutzer-Computer.

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 Internetbenutzern und den Anwendungsservern bereitzustellen. Das Verwenden eines Socket-Proxy in diesem Szenario sorgt für eine Verarbeitungsverlagerung vom Primärserver.

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 Endbenutzern eingehen.
2. Der Socket-Proxy stellt für jede Verbindung eine Peer-Verbindung mit dem Primärserver auf dem konfigurierten internen Port her. Diese zwei Verbindungen werden Endbenutzerverbindung und Serververbindung genannt.
3. Die Endbenutzerverbindungen werden verschlüsselt, und der Socket-Proxy verschlüsselt/entschlüsselt alle Daten, die über die Endbenutzerverbindung 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 Primärserver weitergeleitet werden.
5. Der Primärserver entfernt den Verschlüsselungs- und Entschlüsselungsvorgang.
6. Der Socket-Proxy schließt die entsprechende Peer-Verbindung, sobald die Endbenutzer- oder Serververbindung getrennt wurde.

Verwalten von Support-Automatisierung-Analysten

Support-Automatisierung-Analysten überwachen und bewältigen in Live-Unterstützungssitzungen in Ihrer Umgebung mehrere Endbenutzeranfragen. Analysten verwenden Support-Automatisierung-Werkzeuge, um mit Endbenutzern zu interagieren und eine Live-Unterstützung bereitzustellen.

Analysten greifen auf die Schnittstelle von einem CA Service Desk Manager-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:

[Starten der Live-Unterstützung durch Analysten](#) (siehe Seite 955)

[Konfigurieren von Live-Unterstützung für Analysten](#) (siehe Seite 957)

[Verbinden von Endbenutzern mit Unterstützungssitzungen](#) (siehe Seite 958)

[Wie Analysten die Unterstützung für Endbenutzer automatisieren](#) (siehe Seite 959)

[Bereitstellen der Live-Unterstützung durch Analysten](#) (siehe Seite 959)

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 Service Desk Manager an und klicken auf die Registerkarte "Support-Automatisierung".
 - Sie öffnen ein CA Service Desk Manager-Ticket und klicken auf die Registerkarte "Support-Automatisierung".
2. CA Service Desk Manager fordert den Analysten auf, Java Runtime Environment (JRE) Version 1.6 oder später zu installieren, falls sie nicht bereits installiert ist.

CA Service Desk Manager 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 Endbenutzer den Web-Client startet. Weitere Informationen zur Tabelle "sa_login_session" finden Sie im *Technischen Referenzhandbuch* von CA Service Desk Manager.

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 Ihren 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 961) und [Support-Automatisierung-Zugriffsebenen](#) (siehe Seite 964) 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 969) für Ihre Live-Unterstützungsumgebung.

Sie erstellen Warteschlangen, um eingehende Live-Unterstützungsanfragen angemessen weiterzuleiten.

3. Definieren und verwalten Sie [Aktivitätsbenachrichtigungen](#) (siehe Seite 965) 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 982) 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 Service Desk Manager-Startseite Unterstützungssitzungen an oder wendet sich direkt, per Telefon oder E-Mail, an das Helpdesk. Der Support-Automatisierung-Analyst lädt den Endbenutzer vom CA Service Desk Manager-Ticket aus zu einer Sitzung ein.

1. Der Endbenutzer führt *einen* der folgenden Schritte aus:

- Der Endbenutzer fordert von der CA Service Desk Manager-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-Endbenutzer-Client startet, wird eine ausführbare Datei heruntergeladen, um das Programm zu auszuführen. Der Endbenutzer 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 Endbenutzers, 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
- Automatisierte Aufgaben 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 964)

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 Service Desk Manager 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 Service Desk Manager 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 Service Desk Manager-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-Benutzerverwaltung

System- und Mandantenadministratoren konfigurieren CA Service Desk Manager-Kontakte, Rollenberechtigungen, Zugriffs- und Datenschutzebenen, um Benutzerrechte zu definieren. Im Folgenden werden Benutzer 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 Benutzerkennwörter zurückzusetzen. Der Service Provider-Mandant legt die Berechtigungen fest.

Analyst

Definiert die Rechte für den Benutzer, der Endbenutzern Live-Unterstützung in Ihrer Unterstützungsumgebung bereitstellt.

Endbenutzer

Definiert die Rechte für Benutzer, die eine Live-Unterstützung durch Analysten in Ihrer Unterstützungsumgebung anfordern können, z. B. Angestellte und Kunden.

Konfigurieren von Rollenberechtigungen

Sie können CA Service Desk Manager-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 Endbenutzer-Zugriffsebenen in Ihrem System zu verwalten.

3. [Zuweisen](#) (siehe Seite 965) von Zugriffsebenen zu Rollen.

Sie weisen Endbenutzer-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 Service Desk Manager vorhandenen Genehmigungen. Sofern dies erlaubt ist, gestattet der Gastbenutzer anonymen Benutzern, sich in CA Service Desk Manager anzumelden. Sie können sich vom Server authentifizieren lassen, um Zugriff auf Folgendes zu bekommen:

- Live-Unterstützung
- Self-Service
- Editor für automatisierte Aufgaben
- Endbenutzer-Client

Konfigurieren von Support-Automatisierung für Gastbenutzer

Sie können Ihre Live-Unterstützungsumgebung so konfigurieren, dass Gastbenutzer darauf Zugriff haben. Um Gastbenutzer für bestimmte Mandanten zu konfigurieren oder sie für das gesamte System verfügbar zu machen, gehen Sie folgendermaßen vor:

1. Erstellen Sie einen Zugriffstyp, der [Webauthentifizierung](#) (siehe Seite 962) zulässt.

Wählen Sie den Validierungstyp "Geöffnet - Zugriff immer zulassen" aus.

2. [Weisen Sie](#) (siehe Seite 963) den Zugriffstyp einem Kontakt zu.

Sie können einen Gastkontakt für verschiedene Mandanten in Ihrer Umgebung erstellen.

3. Benachrichtigen Sie die entsprechenden Benutzer in Ihrer Umgebung über die anonyme Anmeldung unter Verwendung des folgenden URL-Formats:

`http://hostname?USRNAME=UserName`

Erstellen eines Zugriffstyps für Gastbenutzer

Sie können einen Zugriffstyp erstellen, mit dem sich Gastbenutzer ohne Authentifizierung bei CA Service Desk Manager anmelden können. Wenn Sie der Service Provider sind, können Sie für jeden Mandanten in Ihrer Umgebung einen Gast-Zugriffstyp anlegen.

So erstellen Sie einen neuen Gast-Zugriffstyp:

1. Klicken Sie auf "Sicherheits- und Rollenmanagement" > "Zugriffstypen".
Die Liste der Zugriffstypen wird angezeigt.
2. Klicken Sie auf "Neu erstellen".
Die Seite "Neuen Zugriffstyp erstellen" wird geöffnet.

3. Füllen Sie die entsprechenden Felder aus, z. B. "Symbol" und "Beschreibung".
4. Gehen Sie auf der Registerkarte "Webauthentifizierung" zur Dropdown-Liste "Validierungstypen", und wählen Sie die Option *Geöffnet - Zugriff immer zulassen*.
5. Speichern Sie den Zugriffstyp.
Der Zugriffstyp ist nun erstellt.
6. (Optional) Klicken Sie auf der "Zugriffstypen - Listenseite" mit der rechten Maustaste, um die Listenseite zu aktualisieren.
Der Gast-Zugriffstyp erscheint in der Liste.

Weisen Sie den Gast-Zugriffstyp einem Kontakt zu.

Nachdem Sie einen Zugriffstyp erstellt haben, der Webauthentifizierung verwendet, können Sie den Gast-Zugriffstyp einem Kontakt zuweisen, so dass der Kontakt sich bei CA Service Desk Manager anmelden kann. Nachdem Sie den Zugriffstyp zugewiesen haben, können Sie die entsprechenden Benutzer in Ihrer Umgebung über den Gastkontakt benachrichtigen.

So weisen Sie den Gast-Zugriffstyp zu:

1. Klicken Sie auf "Sicherheits- und Rollenmanagement" > "Kontakte".
Die Seite "Kontakt – Suche" wird angezeigt.
2. Klicken Sie auf "Neu erstellen".
Das Fenster "Neuen Kontakt erstellen" wird angezeigt.
Hinweis: Sie können einen Kontakt auch ändern.
3. Wählen Sie in der Dropdown-Liste "Kontakttyp" die Option "Gast".
4. (Optional) Verknüpfen des Kontakts mit einem Mandanten. Sie können den Kontakt auch öffentlich machen.
5. Speichern Sie den Kontakt.
Der Kontakt wird erstellt, und der Gast-Zugriffstyp wird mit dem Kontakt verknüpft.

Verwalten der Support-Automatisierung-Zugriffsebenen

Sie können Support-Automatisierung-Zugriffsebenen verwalten und sie innerhalb Ihrer Unterstützungsumgebung verschiedenen CA Service Desk Manager-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.

Endbenutzer

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 Service Desk Manager-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 Endbenutzerwarteschlange abgelaufen ist. Das Ablaufen der Zeit wird von einem Ereignis-Bedingungsmakro von CA Service Desk Manager erkannt.

Endbenutzer zu einer Unterstützungssitzung einladen - Incident

Benachrichtigt den Endbenutzer, wenn ihn der Analyst zu einer Unterstützungssitzung über einen Incident oder eine Anfrage einlädt.

Endbenutzer 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 Endbenutzer entsprechend Ihren Geschäftsanforderungen konfigurieren. Über die folgenden Anpassungen können Sie kontrollieren, was dem Benutzer angezeigt wird, bevor die Unterstützungssitzung beginnt und nachdem die Sitzung beendet wird:

- Passen Sie die Kopf- und Fußzeile aller Seiten an, die dem Endbenutzer 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 Endbenutzer festlegen.

- Passen Sie die Seitenlayouts an, die Endbenutzern bei der Anmeldung und beim Warten auf die Teilnahme an Unterstützungssitzungen angezeigt werden.

Sie können die Seiten, durch die Ihre Endbenutzer geführt werden, den Anforderungen Ihres Unternehmens anpassen.

Hinweis: Weitere Informationen über das Konfigurieren von Support-Automatisierung-Seiten für Analysten und Endbenutzer finden Sie in der *Online-Hilfe*.

Branding-Verwaltung

Sie können die Kopfzeile und Fußzeile von Endbenutzer-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 Service Desk Manager r12.5 migriert. Sie sollten Branding-Anpassungen überprüfen, um sicherzustellen, dass sie dem Branding von CA Service Desk Manager 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 Service Desk Manager 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. Endbenutzer 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 Endbenutzers 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 Endbenutzer.

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 Endbenutzer sich bei "Live-Unterstützung" von CA Service Desk Manager anmelden, dann wird eine Standard-Startseite angezeigt. Auch wenn der Endbenutzer 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
- Endbenutzerseite 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 Service Desk Manager-Angestellte und -Kunden.
- Aktivieren oder deaktivieren Sie den Link für die Teilnahme an einer Sitzung von der Startseite für CA Service Desk Manager-Angestellte und -Kunden.
- Aktivieren oder deaktivieren Sie die Option, um einen CA Service Desk Manager-Incident zu erstellen, wenn die Verbindung zum Endbenutzer 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 Anfragen für Unterstützungssitzungen an den am besten geeigneten Analysten weiterzuleiten. Der Endbenutzer 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 Anfragen von Unterstützung 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 Anfragen von Endbenutzern automatisch, indem es Zuordnungen zwischen Warteschlangen und Incident-Bereichen herstellt. Wenn ein Bereich einer Warteschlange zugeordnet wird, wählt der Endbenutzer eine Kategorie aus und wird zu der entsprechenden Warteschlange weitergeleitet. FAST ESP-Suchfunktionen werden auf die Beschreibungen von Incidents oder Issue-Kategorien angewandt, um relevante Warteschlangen zu finden. Der Benutzer wird daraufhin an die Warteschlange weitergeleitet, die am besten auf seine Anfrage passt.

Wichtig! Diese Suchfunktionen stehen nur zur Verfügung, wenn FAST ESP installiert ist. Weitere Informationen über die Installation und Konfiguration von FAST ESP finden Sie im *Implementierungshandbuch*.

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 Endbenutzer 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

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 Server durch einen globalen Offen- oder Geschlossen-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 Service Desk Manager-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
- Endbenutzer-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*.

Routing-Server für Meldungen

Mithilfe von Routing-Servern für Meldungen (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 Datenschutzebenen können Sie festlegen, welche Aktionen für verschiedene Endbenutzer ausgeführt werden dürfen, um deren Privatsphäre zu schützen. Datenschutzebenen sind mit CA Service Desk Manager-Rollen verknüpft. Es sind drei Standardberechtigungen vorhanden: "Hoch", "Mittel" und "Niedrig". Sie können jedoch ggf. weitere definieren. Sie können die Datenschutzebenen, die für den Endbenutzer verfügbar sind, hinzufügen, aktualisieren und löschen.

Außerdem können Sie den Namen und die Beschreibung der betreffenden Datenschutzebenen 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 Endbenutzer in Ihrer Support-Umgebung. Sobald die Support-Automatisierung-Funktion geschlossen ist, können Endbenutzer nicht mehr darauf zugreifen. Sie können in nur einem Schritt schnell Änderungen an mehreren Schichten vornehmen.

Wichtig! Sie können Schichten sowohl Support-Automatisierungszeiten als auch einzelnen Warteschlangen für Live-Unterstützung zuweisen. Wenn Sie Support-Automatisierungszeiten und einzelnen Warteschlangen verschiedene Schichten zuweisen, kann dies für Analysten und Endbenutzer 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 Endbenutzer 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 Endbenutzer-Computer.
- Passen Sie die Disclaimer an, die Endbenutzern 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 977)

Konfigurieren von automatisierten Aufgaben

Sie installieren und konfigurieren den automatischen Aufgaben-Editor, um automatische Aufgaben zu verwalten, mit deren Hilfe Support-Automatisierung-Analysten Endbenutzer unterstützen. Der Endbenutzer 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 Endbenutzers. Sie erstellen automatische Self-Service-Aufgaben, die mit dem Endbenutzer interagieren und die Eingabe des Endbenutzers 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 Benutzern 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 Benutzernamen und das Kennwort eines Benutzers 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 Diestanbietermandanten, 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 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-Services*.

Verwalten automatischer 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 Service Desk Manager-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 heraufladen, 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 Service Desk Manager-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 Endbenutzern 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 Endbenutzerfrage.

URL-Voreinstellung

Identifiziert eine häufig verwendete URL, auf die der Endbenutzer zugreifen kann.

Sie können jede Chat-Voreinstellung lokalisieren. Die Chat-Voreinstellung wird mit der Endbenutzerlokalisierung synchronisiert, so dass der Endbenutzer 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 Endbenutzers ausführen, wenn der Endbenutzer gewöhnlich keine Zugriffsrechte für derartige Aktivitäten hat. Falls der aktuelle Endbenutzer 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 Endbenutzer Self-Service-Aufgaben startet, erscheint ein Disclaimer-Text, dem er zustimmen muss, bevor er fortfahren kann.

Sie können Disclaimer-Geschäftsobjekte 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 Service Desk Manager 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*.

Anhang A: Beschreibungen der Felder in Ansichten

Dieses Kapitel enthält folgende Themen:

[Beschreibungen der Felder in Ansichten](#) (siehe Seite 986)

[View Act Log](#) (siehe Seite 986)

[View Audit Assignee](#) (siehe Seite 988)

[View Audit Group](#) (siehe Seite 988)

[View Audit Priority](#) (siehe Seite 989)

[View Audit Status](#) (siehe Seite 990)

[View Change Act Log](#) (siehe Seite 990)

[View Change](#) (siehe Seite 992)

[View Change to Assets](#) (siehe Seite 997)

[View Change to Change Act Log](#) (siehe Seite 997)

[View Change to Change WF](#) (siehe Seite 999)

[View Change to Properties](#) (siehe Seite 1001)

[View Contact Full](#) (siehe Seite 1002)

[View Contact to Environment](#) (siehe Seite 1005)

[View Group](#) (siehe Seite 1006)

[View Group to Contact](#) (siehe Seite 1007)

[View Issue](#) (siehe Seite 1007)

[View Issue Act Log](#) (siehe Seite 1012)

[View Issue to Assets](#) (siehe Seite 1014)

[View Issue to Issue Act Log](#) (siehe Seite 1014)

[View Change to Request](#) (siehe Seite 1016)

[View Issue to Issue WF](#) (siehe Seite 1019)

[View Issue to Properties](#) (siehe Seite 1021)

[View Request](#) (siehe Seite 1022)

[View Request to Act Log](#) (siehe Seite 1028)

[View Request to Properties](#) (siehe Seite 1028)

Beschreibungen der Felder in Ansichten

Sie können die Felddeschreibungsinformationen in den grundlegenden und erweiterten Ansichten von CA Service Desk Manager 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 797)

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).

Feld	Anmerkungen
time_spent	issalg.time_spent: Dauer dieser Aktivität, als Gesamtzahl von Sekunden gespeichert. Zum Beispiel 80 = 1 Minute, 20 Sekunden.
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 Benutzer geändert werden kann.
action_desc	act_log.action_desc: Textbeschreibung einer automatisierten Aktion, die vom Benutzer 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 Benutzers.
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 Benutzern 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 "audobj_uniqueid" (Anfrage oder Change) geben.

Feld	Anmerkungen
audobj_uniqueid	audit_log.audobj_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 "audobj_uniqueid" (Anfrage oder Change) geben.

Feld	Anmerkungen
audobj_uniqueid	audit_log.audobj_uniqueid: Die eindeutige ID des Audit-Protokollobjekts, die die "chg.id" oder die "call_req.id" darstellt.

Feld	Anmerkungen
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 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 die Tabelle "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

Feld	Anmerkungen
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 Benutzer 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 Benutzer geändert werden kann.
action_desc	issalg.action_desc: Textbeschreibung einer automatisierten Aktion, die vom Benutzer 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 Benutzern angezeigt werden kann oder nur für die interne Verwendung bestimmt ist.
knowledge_session	chgalg.knowledge_session: Eine ID für eine bestimmte Sitzung eines bestimmten Benutzers.
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 Endbenutzers, 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.last_mod_by = 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.last_mod_by = 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.last_mod_by = 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
Kategorie	chg.category: Zeiger auf den Change-Kategoriecode, um die Kategorie abzurufen, in die diese Änderung fällt. chg.category = chgcat.code
Priorität	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 Endbenutzer (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 diese Anforderung 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 Benutzer 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 benutzerdefinierbar.
string2	Dieses Textfeld ist benutzerdefinierbar.
string3	Dieses Textfeld ist benutzerdefinierbar.

Feld	Anmerkungen
string4	Dieses Textfeld ist benutzerdefinierbar.
string5	Dieses Textfeld ist benutzerdefinierbar.
string6	Dieses Textfeld ist benutzerdefinierbar.
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 Endbenutzers (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 Endbenutzers (affected_end_user) oder die Rolle des Requestors angibt. chg.person_contacting = perscon.id
status_name	pri.sym: Beschreibung der Priorität aus Benutzersicht. chg.status = chgstat.code
priority_num	pri.sym: Beschreibung der Priorität aus Benutzersicht. chg.priority = pri.enum
category_name	chgcac.sym: Name der Change-Kategorie, der einem Benutzer angezeigt wird. chg.category = chgcac.code
organization_name	ca_organization.org_name: Name der Organisation aus Benutzersicht. issue.organization = ca_organization.organization_uuid
affected_end_user_lastname	ca_contact.last_name: Der Nachname des betroffenen Endbenutzers. chg.affected_end_user = ca_contact.contact_uuid
affected_end_user_firstname	ca_contact.first_name: Der Vorname des betroffenen Endbenutzers. chg.affected_end_user = ca_contact.contact_uuid

Feld	Anmerkungen
affected_end_user_middlename	ca_contact.middle_name: Der zweite Vorname des betroffenen Endbenutzers. chg.affected_end_user = ca_contact.contact_uuid
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 Benutzersicht issue.organization = 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.last_mod_by = ca_contact.contact_uuid
group_name	ca_contact.last_name: Der Name der Gruppe, die diesem Change zugewiesen ist. chg.last_mod_by = 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 aus Benutzersicht chg.impact = impact.enum
product_sym	product.sym: Produktbeschreibung, die Benutzern angezeigt wird. chg.product = product.id
type_of_contact_sym	toc.sym: Typ der Kontaktbeschreibung, die Benutzern angezeigt wird. chg.type_of_contact = toc.id
rpting_method_sym	repmeth.sym: Beschreibung der Berichtsmethode, die Benutzern angezeigt wird. chg.reporting_method = repmeth.id
person_contacting_sym	perscon.sym: Beschreibung der Kontakt aufnehmenden Person

Feld	Anmerkungen
	aus Benutzersicht. 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

Feld	Anmerkungen
	„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.
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 Benutzer ändern kann.
system_time	chgalg.system_time: Datum/Zeit der Datensatzerstellung (pdmtime).
analyst	chgalg.analyst: Ein UUID-Zeiger zur Kontakt-UIID, 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 Benutzer geändert werden kann.
action_desc	act_log.action_desc: Textbeschreibung einer automatisierten Aktion, die vom Benutzer 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 Benutzern angezeigt werden kann oder nur für die interne Verwendung bestimmt ist.
knowledge_session	chgalg.knowledge_session: Eine ID für eine bestimmte Sitzung eines bestimmten Benutzers.
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-UIID, 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 Benutzer 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 = tskty.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 Service Desk Manager angezeigt und ausgeführt werden soll (z. B. aufsteigend).
wf_status	wf.status: ID, die auf einen tskstat-Datensatz verweist, der den aktuellen Status dieser Workflow-Aufgabe angibt. wf.status = tskstat.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
creator	wf.creator: Binäre UUID, die auf einen Datensatz in der Tabelle "ca_contact" verweist. Gibt die Person an, die diese Workflow-Aufgabe

Feld	Anmerkungen
	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 Service Desk Manager 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 Benutzer 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
erforderlich	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 Benutzer bei der Eingabe eines sinnvollen Wertes in "prp.value" zu

Feld	Anmerkungen
	unterstützen.
prp_description	prp.description: Textfeld, das erklärt, welche Art von Wert in "prp.value" eingegeben werden sollte.
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 Dienstyp 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.

Feld	Anmerkung
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
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: Benutzer-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: Benutzer-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
department	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

Feld	Anmerkung
	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
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_identifier	ca_contact.alternate_identifier: 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 Benutzer-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

Feld	Anmerkung
	"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.
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 Diensttyp, 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 Kontakttable, die jedoch nur Gruppenkontakte aufführt. Die Kontakttyp-ID = 2308, die der Kontakttyp für Gruppen ist. Sie können diese Ansicht mit anderen CA Service Desk Manager-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_Group_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

Feld	Anmerkungen
	Problemanfrage zu beziehen.
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
Kategorie	issue.category: Zeiger auf den Problemanfragen-Kategoriecode; verweist auf die Kategorie, in die diese Problemanfrage fällt. issue.category = isscat.code
Priorität	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 Endbenutzer (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.
support_lev	issue.support_lev - Zeiger auf einen Service-Beschreibungsdatensatz,

Feld	Anmerkungen
	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 Benutzer als Kontrollkästchen angezeigt wird und der angibt, ob der Analyst am issue.call_back_date benachrichtigt werden soll.
string1	Dieses Textfeld ist benutzerdefinierbar.
string2	Dieses Textfeld ist benutzerdefinierbar.
string3	Dieses Textfeld ist benutzerdefinierbar.
string4	Dieses Textfeld ist benutzerdefinierbar.
string5	Dieses Textfeld ist benutzerdefinierbar.
string6	Dieses Textfeld ist benutzerdefinierbar.
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.
type_of_contact	issue.type_of_contact - Zeiger auf einen Datensatz in der Inhaltsverzeichnis-tabelle 'toc', der die allgemeine Kategorie des

Feld	Anmerkungen
	betroffenen Endbenutzers (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 Benutzersicht. issue.status = issstat.code
priority_num	pri.sym: Beschreibung der Priorität aus Benutzersicht. issue.priority = pri.enum
category_name	isscat.sym: Der Name der Issue-Kategorie, der einem Benutzer angezeigt wird. issue.category = isscat.code
organization_name	ca_organization.org_name: Name der Organisation, der Benutzern angezeigt wird. issue.organization = ca_organization.organization_uuid
affected_end_user_lastname	ca_contact.last_name: Der Nachname des betroffenen Endbenutzers. issue.affected_end_user = ca_contact.contact_uuid
affected_end_user_firstname	ca_contact.first_name: Der Vorname des betroffenen Endbenutzers. issue.affected_end_user = ca_contact.contact_uuid
affected_end_user_middlename	ca_contact.middle_name: Der zweite Vorname des betroffenen Endbenutzers. 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 Benutzern angezeigt wird. issue.impact = impact.enum
product_sym	product.sym: Produktbeschreibung, die Benutzern angezeigt wird. issue.product = product.id
type_of_contact_sym	toc.sym: Beschreibung des Kontakttyps, die Benutzern angezeigt wird. issue.type_of_contact = toc.id
rpting_method_sym	repmeth.sym: Beschreibung der Berichtsmethode, die Benutzern angezeigt wird. issue.reporting_method = repmeth.id
person_contacting_sym	perscon.sym: Beschreibung der Kontakt aufnehmenden Person, die Benutzern 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

Feld	Anmerkungen
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.
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 Benutzer geändert werden kann.
action_desc	issalg.action_desc: Textbeschreibung einer automatisierten Aktion, die vom Benutzer 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 Benutzern angezeigt werden kann oder nur für die interne Verwendung bestimmt ist.
knowledge_session	issalg.knowledge_session: Kennung für eine bestimmte Sitzung eines bestimmten Benutzers.
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.
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".

Feld	Anmerkungen
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.
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-UIID, 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 Benutzer geändert werden kann.
action_desc	issalg.action_desc: Textbeschreibung einer automatisierten Aktion, die vom Benutzer 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 Benutzern angezeigt werden kann oder nur für die interne Verwendung bestimmt ist.
knowledge_session	issalg.knowledge_session: Kennung für eine bestimmte Sitzung eines bestimmten Benutzers.
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-UIID, 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

Feld	Anmerkungen
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
customer	call_req.customer: Eindeutige binäre ID, die auf einen Datensatz in der Tabelle "ca_contact" verweist. Stellt den betroffenen Endbenutzer 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 Aufrufen 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 Benutzers) an. call_req.urgency = urgency.enum

Feld	Anmerkungen
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
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 Endbenutzer (affected_end_user) kontaktiert werden soll.
cr_call_back_flag	call_req.call_back_flag: Boolescher Indikator, der dem Benutzer 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 Meldungen 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.

Feld	Anmerkungen
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 Benutzer 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 = tshty.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 Service Desk Manager angezeigt und ausgeführt werden soll (z. B. aufsteigend).
wf_status	isswf.status: ID, die auf den Datensatz "tskstat" verweist. Gibt den

Feld	Anmerkungen
	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
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.

Feld	Anmerkungen
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.
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 Service Desk Manager angezeigt werden soll (z. B. aufsteigend).
label	issprp.label: Kurze Beschreibung zu dem Wert, der in das Feld

Feld	Anmerkungen
	"issprp.value" einzugeben ist.
value	issprp.value: Wert, der vom Benutzer 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
erforderlich	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 Benutzer bei der Eingabe eines sinnvollen Wertes in "issprp.value" zu unterstützen.
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 Service Desk Manager-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.

Feld	Anmerkungen
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).
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

Feld	Anmerkungen
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_uid
customer	call_req.customer: Eindeutige binäre ID, die auf einen Datensatz in der Tabelle "ca_contact" verweist. Stellt den betroffenen Endbenutzer für diese Anfrage dar. call_req.customer = ca_contact.contact_uid
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_uid.
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.
Kategorie	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
Priorität	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 Benutzers) an. call_req.urgency = urgency.enum

Feld	Anmerkungen
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.
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 Endbenutzer (affected_end_user) kontaktiert werden soll.
call_back_flag	call_req.call_back_flag: Boolescher Indikator, der dem Benutzer als Kontrollkästchen angezeigt wird und der angibt, ob der Analyst zum Datum "call_req.call_back_date" benachrichtigt werden soll.

Feld	Anmerkungen
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.
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

Feld	Anmerkungen
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 Endbenutzers an. call_req.customer = ca_contact.contact_uuid
customer_firstname	ca_contact.first_name: Gibt den tatsächlichen Vornamen des betroffenen Endbenutzers an. call_req.customer.ca_contact.contact_uuid
customer_middlename	ca_contact.middle_name: Gibt den tatsächlichen zweiten Vornamen des betroffenen Endbenutzers 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 Service Desk Manager 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.

Feld	Anmerkungen
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
erforderlich	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 B: LDAP-Ergebniscodes von RFC 2251

Dieses Kapitel enthält folgende Themen:

[LDAP-Rückgabecodes](#) (siehe Seite 1031)

[Rückgabecodes des LDAP-Servers](#) (siehe Seite 1031)

[Rückgabecodes des LDAP-Clients](#) (siehe Seite 1037)

[LDAP-spezifische RFC-Standards](#) (siehe Seite 1039)

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	Reserviert
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

Hex	Dezimal	Beschreibung
		Steuerelement nicht, oder das Steuerelement ist für die Art der Operation nicht zutreffend.
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.

Hex	Dezimal	Beschreibung
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
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:

Hex	Dezimal	Beschreibung
		■ 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.
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

Hex	Dezimal	Beschreibung
		aufgrund der Containment-Regeln unzulässig ist.
		Der relative eindeutige Name (RDN) für den Eintrag verwendet einen unzulässigen Attributtyp.
0x41	65	LDAP_OBJECT_CLASS_VIOLATION Zeigt an, dass die Hinzufügungs- 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 Hinzufügungs- oder Änderungsoperation versucht, einen Eintrag hinzuzufügen, der keinen Wert für ein erforderliches Attribut enthält. - Die Hinzufügungs- 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 Hinzufügungsoperation 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

Hex	Dezimal	Beschreibung
		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.
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 <code>ldap_bind</code> oder <code>ldap_bind_s</code> mit einer

Hex	Dezimal	Beschreibung
		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.
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.

Hex	Dezimal	Beschreibung
		Gewöhnlich geschieht dies beim Verfolgen von Verweisungen.
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

RFC	Beschreibung
1823	LDAP-API
1959	Ein LDAP-URL-Format
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

RFC	Beschreibung
2739	Kalenderattribute für vCard und LDAP
2798	Definition der LDAP-Objektklasse „inetOrgPerson“
2820	Anforderungen für die Zugriffssteuerung für LDAP
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

Anhang C: Referenzbefehle

Dieser Anhang enthält ausführliche Informationen zu den Referenzbefehlen, die für CA Service Desk Manager verfügbar sind.

Dieses Kapitel enthält folgende Themen:

[bop_sinfo – Systeminformationen anzeigen](#) (siehe Seite 1045)
[dbmonitor_nxd – Daemon zur Überwachung von Datenbanken](#) (siehe Seite 1046)
[pdm_backup – Exportieren der Datenbank in eine ASCII-Datei](#) (siehe Seite 1048)
[pdm_cache_refresh – Aktualisieren der Datenbank](#) (siehe Seite 1049)
[pdm_configure – Öffnen des Konfigurationsfensters](#) (siehe Seite 1051)
[pdm_d_refresh – Starten fehlgeschlagener Daemons](#) (siehe Seite 1052)
[pdm_deref – Dereferenzieren von ASCII-Daten](#) (siehe Seite 1053)
[pdm_discimp – Importieren ermittelter Assets](#) (siehe Seite 1056)
[pdm_discupd – Asset-Aktualisierung ermittelt](#) (siehe Seite 1058)
[pdm_edit – Konfigurieren von Serverprozessen](#) (siehe Seite 1059)
[pdm_extract – Extrahieren von Daten aus der Datenbank](#) (siehe Seite 1061)
[pdm_halt – Beenden von Daemons oder Anhalten von Diensten](#) (siehe Seite 1064)
[pdm_init – Starten von Daemons](#) (siehe Seite 1065)
[pdm_key_refresh – Aktualisieren von im Cache gespeicherten Schlüsselinformationen](#) (siehe Seite 1066)
["pdm_lexutil" – CA Service Desk Manager-Lexika ändern](#) (siehe Seite 1066)
["pdm_k_reindex" – Dienstprogramm zur Knowledge-Neuindizierung](#) (siehe Seite 1067)
[pdm_listconn – Auflisten der aktiven Verbindungen](#) (siehe Seite 1074)
[pdm_load – Hinzufügen, Aktualisieren und Löschen von Datenbank-Datensätzen](#) (siehe Seite 1076)
[pdm_logfile – Ändern der Cutover-Größe von STDLog](#) (siehe Seite 1078)
[pdm_proctor_init – Starten von Proctor auf sekundären Servern](#) (siehe Seite 1079)
[pdm_replace – Ersetzen einer Datenbanktabelle](#) (siehe Seite 1079)
[pdm_restore – Wiederherstellen einer Datenbank](#) (siehe Seite 1081)
[pdm_status – Anzeigen des Status von Daemons oder Prozessen](#) (siehe Seite 1083)
[pdm_task – Einstellen der Umgebungsvariablen](#) (siehe Seite 1083)
[pdm_text_cmd – Befehlszeilenschnittstelle für Text-API](#) (siehe Seite 1084)
[pdm_uconv – Konvertiert den lokalen Zeichensatz in UTF-8](#) (siehe Seite 1087)
[pdm_userload – Hinzufügen, Aktualisieren und Löschen von Datenbank-Datensätzen](#) (siehe Seite 1090)
[pdm_webstat – Zurückgeben von Webnutzungsstatistiken](#) (siehe Seite 1093)
[report – Generieren von Berichten](#) (siehe Seite 1097)
[rpt_srv – Generieren von Berichten](#) (siehe Seite 1098)
[uniconv – Starten des UNIX CA NSM-Event Converter-Daemons](#) (siehe Seite 1100)

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

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 Service Desk Manager die Cache-Speicherung solcher Datenbanktabellen zu erlauben, die aktualisiert werden sollen, wenn Änderungen außerhalb von CA Service Desk Manager gemacht werden.

Die Hauptfunktion von "dbmonitor_nxd" besteht darin, CHANGE-Benachrichtigungen für Änderungen in den angegebenen Tabellen zu generieren, die nicht durch CA Service Desk Manager 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 Service Desk Manager-Prozesse zur Folge und beeinträchtigt die Leistung von CA Service Desk Manager erheblich.

Um dieser Leistungsbeeinträchtigung von CA Service Desk Manager entgegenzuwirken, wurde dbmonitor_nxd für diesen Release des Produkts aktualisiert. Die Überwachung unterstützt eine Befehlszeilenschnittstelle, die es dem Benutzer 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 Benutzer 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 Service Desk Manager-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-Benutzer 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 Service Desk Manager an und schreibt dann eine oder mehrere Tabellen von einer CA Service Desk Manager-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 Service Desk Manager-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 Service Desk Manager installiert haben.
- Wenn keine Tabelle angegeben ist, wird die gesamte CA Service Desk Manager-Datenbank exportiert, einschließlich Fenstergruppen und Menüregistrierungsdateien.

Einschränkung

pdm_backup kann nicht ausgeführt werden, während CA Service Desk Manager aktiv ist.

Wichtig! Bei UNIX muss der LIBPATH vor der Ausführung mehrerer CA Service Desk Manager-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 1081)

pdm_cache_refresh – Aktualisieren der Datenbank

pdm_cache_refresh bewirkt, dass CA Service Desk Manager-Daemons oder -Prozesse Daten verwenden, die mit pdm_userload oder anderen Datenbankdienstprogrammen, einschließlich CA Service Desk Manager-fremden Datenbank-Tools, in die Datenbank geladen wurden.

Die meisten Daemons und ausführbaren Dateien von CA Service Desk Manager 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 Service Desk Manager 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 Service Desk Manager-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 Service Desk Manager. 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 Service Desk Manager-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 Service Desk Manager-Konfigurationsfenster enthält. In diesem Fenster können Sie die CA Service Desk Manager-Konfiguration nach der Installation von CA Service Desk Manager festlegen oder die CA Service Desk Manager-Konfiguration ändern, nachdem CA Service Desk Manager läuft. Aus folgenden Gründen könnte es notwendig sein, die Konfiguration von CA Service Desk Manager zu ändern:

- Änderung des Datenbanktyps oder -servers
- Neuladen der Standarddaten
- Ändern der Kennwörter für CA Service Desk Manager-Systemkonten
- Wiederherstellen der Schemadateien zur Integration von Änderungen
- Neukonfigurieren als primärer Server oder sekundärer Server

Syntax

Dieser Befehl hat das folgende Format:

```
pdm_configure
```

Restrictions

pdm_configure kann auf einem CA Service Desk Manager-Server (primärer oder sekundärer Server) oder auf einem CA Service Desk Manager-Linux-Client ausgeführt werden. Zur Ausführung von "pdm_configure" müssen Sie der privilegierte Benutzer oder der Root sein.

pdm_d_refresh – Starten fehlgeschlagener Daemons

Das Befehlszeilenhilfsprogramm "pdm_d_refresh" wird hauptsächlich für Remote-Daemon-Konfigurationen verwendet. Das Programm fordert den Daemon-Manager dazu auf, Daemons zu starten die bereits zehnmal nicht gestartet werden konnten und die der Daemon-Manager als "nicht ausführbar" gekennzeichnet hat. Dies wird oft beim Starten des Primärservers verursacht, wenn folgendes auftritt:

- Einer oder mehrere der sekundären Server sind noch nicht gestartet worden.
- Ein sekundärer Server wird gestoppt, während der Primärserver läuft.

Der Daemon-Manager versucht, Remote-Daemons zu starten. Wenn er den sekundären Server nicht kontaktieren kann, versucht er es zehn Mal und hält dann an. 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 Service Desk Manager-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</cs> 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 Service Desk Manager-Datenbank oder Tabellenkalkulation kompatibel sind. Es kann außerdem verwendet werden, um Berichte oder Ausgabedateien für eine Nicht-CA Service Desk Manager-Datenbank oder Tabellenkalkulation zu erstellen.

Wichtig! Verwenden Sie "pdm_deref</cs> nicht, wenn Sie mit SQL nicht vertraut sind. Die Verzeichnisse „export“ und „import“ in "\$NX_ROOT/samples</cs> (UNIX) oder "installation-directory\samples</cs> (Windows) enthalten ein Standardset von "specfiles</cs>, 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 Benutzerinformationen 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 Fortschrittsmeldungen der Protokolldatei aus.

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 Service Desk Manager-Installationsverzeichnisses 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 Eingabe vorzubereiten

Dieses Beispiel zeigt, wie Sie "pdm_deref" verwenden können, um Daten für die Eingabe 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 folgenden 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 1061)

pdm_discimp – Importieren ermittelter Assets

Batch-Registrierung ermittelter Nicht-CA Service Desk Manager-Anlagen. Dieses Dienstprogramm kann verwendet werden, um die MDB nach Anlagen zu durchsuchen, die von anderen Softwareprodukten registriert wurden und diese als CA Service Desk Manager-Anlagen zu registrieren, so dass sie in CA Service Desk Manager 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 Service Desk Manager-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 Service Desk Manager registriert zu werden.

Um die entsprechenden Datensätze für die Verarbeitung herauszufinden, werden aufgrund der Struktur der MDB und der CA Service Desk Manager-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 Service Desk Manager-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 Service Desk Manager-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 Service Desk Manager-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_edit – Konfigurieren von Serverprozessen

Mit *pdm_edit* bearbeiten Sie die Startvorlagendatei, *pdm_startup.tpl*, auf dem CA Service Desk Manager-Server. Einige Beispiele dafür, wann Sie die Startvorlagendatei bearbeiten müssen, sind die Definition von Objekt-Engine-Aliasnamen, die Einrichtung der Web-Engine für die Ausführung auf einem sekundären Server und die Einrichtung der Remote-Authentifizierung auf einem sekundären Server.

Für UNIX

UNIX-Benutzer müssen die Berechtigungen für die Datei "pdm_edit.pl" in „ausführbar“ ändern.

Syntax

Wechseln Sie in der CA Service Desk Manager-Server Installation in das Verzeichnis \$NX_ROOT/samples/pdmconf (UNIX) oder "*installation-directory*\samples\pdmconf" (Windows). Geben Sie dann zum Starten von "pdm_edit" den folgenden Befehl ein:

```
pdm_perl pdm_edit.pl
```

Hinweis: "pdm_edit" ist ein Perl-Skript, und es wird empfohlen, eine Version von Perl zu verwenden, die mit CA Service Desk Manager ausgeliefert wird (pdm_perl). Andere Versionen von Perl können aber auch funktionieren.

Verwendung

Wenn "pdm_edit" läuft, werden Sie zur Eingabe bestimmter Informationen aufgefordert, und der restliche Prozess ist menügesteuert. Um Informationen zur Verwendung zu erhalten, verwenden Sie die Menüoption „H“ für Hilfe. Sie können auch die Hilfe in der Datei "pdm_edit.README" einsehen, die Sie mit einem beliebigen Texteditor anzeigen können.

Ausgabe

Wenn Sie "pdm_edit</cs> beenden und Ihre Änderungen speichern, werden mehrere Dateien erstellt:

- "pdm_startup.rmt</cs> speichert Ihre neuen Konfigurationswerte.
- "alias_install.sh</cs> (UNIX) oder "alias_install.bat</cs> (Windows), wenn Sie Objekt-Engine-Aliasnamen definiert haben
- "pdm_startup.dat</cs> speichert Daten, die benötigt werden, wenn Sie "pdm_edit</cs> das nächste Mal aufrufen. Behalten Sie diese Datei im Arbeitsverzeichnis mit "pdm_edit.pl</cs> bei.

Damit Ihre Änderungen wirksam werden, gehen Sie wie folgt vor:

1. Erstellen Sie eine Sicherungskopie der Datei "pdm_startup.tpl", die sich im Verzeichnis "\$NX_ROOT/pdmconf</cs> (UNIX) oder "*installation-directory*\pdmconf</cs> (Windows) der CA Service Desk Manager Primärserverinstallation befindet, und ersetzen Sie sie durch die neu erstellte Datei "pdm_startup.rmt".

Note: Der berechtigte Nutzer muss die Datei "pdm_startup.tpl", die Sie aus der Datei "pdm_startup.rmt" erstellt haben, lesen können.

2. Wenn Sie Objekt-Engine-Aliasnamen definiert haben, führen Sie das Skript "alias_install</cs> aus, um den primären Server neu zu konfigurieren.
3. Führen Sie das Konfigurationsprogramm auf dem CA Service Desk Manager-Primärserver aus, ohne vorher Änderungen an der Datei vorzunehmen. Dadurch werden die neuen Konfigurationeneinstellungen beim Neustart des primären CA Service Desk Manager-Servers wirksam.
4. Setzen Sie im Bedarfsfall alle sekundären CA Service Desk Manager-Server in Gang, und starten Sie dann den Primärserver.

Wichtig! Bei UNIX muss der LIBPATH vor der Ausführung mehrerer CA Service Desk Manager-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:

[Starten des primären Servers](#) (siehe Seite 38)

[Starten von sekundären Servern](#) (siehe Seite 37)

pdm_extract – Extrahieren von Daten aus der Datenbank

Der Befehl `pdm_extract` extrahiert Daten aus den angegebenen Datenbanktabellen von CA Service Desk Manager oder die gesamte CA Service Desk Manager-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 Benutzerinformationen 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 Standard-Verhalten 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[.nnnnnn][[+|-][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 1053)
[pdm_replace – Ersetzen einer Datenbanktabelle](#) (siehe Seite 1079)
[pdm_userload – Hinzufügen, Aktualisieren und Löschen von Datenbank-Datensätzen](#) (siehe Seite 1090)
[rpt_srv – Generieren von Berichten](#) (siehe Seite 1098)

pdm_halt – Beenden von Daemons oder Anhalten von Diensten

pdm_halt beendet alle CA Service Desk Manager-Daemons (UNIX) oder den Systemserverdienst (Windows) ordnungsgemäß auf dem System, auf dem pdm_halt ausgeführt wird. Das Dienstprogramm "pdm_halt</cs>" 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. Geben Sie anschließend **pdm_halt -F** ein.

Syntax

Dieser Befehl hat das folgende Format:

```
pdm_halt [-F]
```

-F

So umgehen Sie das normale Verfahren für das Beenden eines Daemons oder eines Dienstes und beenden sowohl den Daemon als auch den Dienst. CA Service Desk Manager fordert Sie zur Bestätigung auf. Wenn Sie Daemons oder Dienste zwangsweise beenden, werden einige laufende Anwendungsprozesse unter Umständen nicht protokolliert.

Restrictions

pdm_halt kann auf einem CA Service Desk Manager-Server (primärer oder sekundärer Server) oder auf einem CA Service Desk Manager-UNIX-Client ausgeführt werden. Zur Ausführung von "pdm_halt" müssen Sie der privilegierte Benutzer sein.

pdm_init – Starten von Daemons

Gilt nur für UNIX

pdm_init startet alle automatischen Prozesse von CA Service Desk Manager 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
```

Restrictions

pdm_init kann auf einem CA Service Desk Manager-Server (primärer oder sekundärer Server) oder auf einem CA Service Desk Manager-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 Service Desk Manager 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 Service Desk Manager-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 Service Desk Manager-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 Service Desk Manager-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. Sie können dieses Dienstprogramm auch in einer [FAST ESP-Integration](#) (siehe Seite 1070) verwenden.

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.

Um das Dienstprogramm zur Knowledge-Reindizierung auszuführen, geben Sie den folgenden Befehl in der Eingabeaufforderung ein:

```
pdm_k_reindex
```

Zu diesem Befehl sind die folgenden Optionen verfügbar.

Schnittstelle:

-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 Tabelle „re-index“ nach Neuindizierung.

Hinweis: Parameter mit einem Bindestrich als Präfix, z. B. "-D", sollten anderen Parametern, die dieses Präfix nicht haben, vorausgehen.

Datei:reindex.txt

Dokumente werden im Hinblick auf die entsprechende Datei neu indiziert.

+i

Erstellt nur Indizes der neu indizierten Tabelle (entspricht der Suchtabelle nach der Neuindizierung). Alte Indizes werden vor der Neuindizierung entfernt.

+t

Tauscht nur die Namen der Tabellen "search" und "re-index" aus.

Hinweis: Das Präfix "+" kennzeichnet nur diesen Parameter.

sdtout

Definiert, wie häufig die Statistik im Befehlsfenster erscheint. Standardmäßig zeigt das Dienstprogramm zur Knowledge-Reindizierung jeweils nach 1000 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.

Wichtig! Bei UNIX muss der LIBPATH vor der Ausführung mehrerer CA Service Desk Manager-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.

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.

Sie können "pdm_k_reindex" mit oder ohne FAST ESP-Integration verwenden:

- [Verwenden von "pdm_k_reindex" ohne FAST ESP](#) (siehe Seite 1067)
- [Verwenden von "pdm_k_reindex" mit FAST ESP](#) (siehe Seite 1070)

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.

Hinweis: Bei der Integration mit FAST ESP wird das Dienstprogramm "pdm_k_reindex" nicht aufgerufen, weil Dokumente im Hintergrund indiziert sind.

Verwenden von "pdm_k_reindex" mit FAST ESP

Das Dienstprogramm "pdm_k_reindex" wird verwendet, um ausgewählte Dokument-Factories wie KD, cr, iss usw. neu zu indizieren, die Indizierung zu entfernen und zu synchronisieren (Neuindizierung und Entfernen der Indizierung). Das Dienstprogramm rufen Sie wie folgt auf:

```
pdm_k_reindex [operation] [factory] [mode]
```

operation

Die folgenden Vorgänge sind gültig:

-h

Zeigt Hilfe zum Dienstprogramm an.

index

(Standardwert) Führt eine Neuindizierung der Dokumente durch.

deindex

Entfernt die Dokumente aus dem Index.

sync

Ermöglicht Dokumente neu zu indizieren bzw. die Indizierung zu entfernen, um die Such-Engine nach Lösch- oder Wiederherstellungsvorgängen zu synchronisieren. Die folgenden Modi sind für den Synchronisierungsvorgang gültig:

- **Löschung**

Synchronisiert die Suchmaschine nach dem Löschen.

- **restore**

Synchronisiert die Suchmaschine nach dem Wiederherstellen.

status

Anzeige der Anzahl der noch zu verarbeitenden Dokumente

factory

Die folgenden Factorys sind gültig:

all

Legt alle Factorys fest.

KD

(Standardwert) Legt die KD-Factory fest.

cr

Legt die cr-Factory fest.

Iss

Legt die iss-Factory fest.

mode

Die folgenden Modi sind gültig:

Löschung

Synchronisiert die Suchmaschine nach dem Löschen.

restore

Synchronisiert die Suchmaschine nach dem Wiederherstellen.

Hinweis: Wenn keine Vorgangs- oder Factory-Argumente ausgewählt sind, wird die KD-Factory indiziert.

Beispiel: Parameter "index"

```
pdm_k_reindex [index] [factory:KD|cr|iss|all]
```

Beispiel: Parameter "de-index"

```
pdm_k_reindex deindex factory:KD|cr|iss|all [clearrange]
```

clearrange

(Optional) Indizierung von Dokumenten entfernen, die außerhalb des vordefinierten Factory-Bereichs liegen

Hinweis: Für den Parameter "deindex" ist ein Factory-Argument erforderlich.

Beispiel: Parameter "sync"

```
pdm_k_reindex sync[:purge|restore] factory:KD|cr|iss|all
```

Hinweis: Wenn Sie das Löschen oder Wiederherstellen von Modi unterdrücken, werden beide Modi aufgerufen. Für den Parameter "sync" ist ein Factory-Argument erforderlich.

Verschiedene Parameter

```
pdm_k_reindex -pm
```

Legt die Dokumentverknüpfungen und eingebetteten Bilder im Lösungsfeld fest.

```
pdm_k_reindex -ml
```

Legt die Dokumentverknüpfungen im Lösungsfeld fest und ordnet sie der Datenbank zu.

Hinweis: Weitere Informationen über das Hilfsprogramm "pdm_k_reindex" finden Sie im *Implementierungshandbuch*.

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

cproc 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
```

Dabei gilt:

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 Service Desk Manager-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 Service Desk Manager-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 Service Desk Manager 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 Service Desk Manager 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 Service Desk Manager-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 Service Desk Manager 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 Service Desk Manager-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_backup – Exportieren der Datenbank in eine ASCII-Datei](#) (siehe Seite 1048)

[pdm_replace – Ersetzen einer Datenbanktabelle](#) (siehe Seite 1079)

[pdm_restore – Wiederherstellen einer Datenbank](#) (siehe Seite 1081)

[pdm_userload – Hinzufügen, Aktualisieren und Löschen von Datenbank-Datensätzen](#) (siehe Seite 1090)

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.

Restrictions

Sie können pdm_load ausführen, während CA Service Desk Manager aktiv ist; die Leistung kann jedoch sehr beeinträchtigt werden. Führen Sie pdm_load am besten aus, wenn kein Benutzer CA Service Desk Manager verwendet.

Wichtig! Bei UNIX muss der LIBPATH vor der Ausführung mehrerer CA Service Desk Manager-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_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 Service Desk Manager-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</cs> akzeptiert eine Textdatei als Eingabe, die das gleiche Dateiformat hat, das von "pdm_userload</cs> 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.

Restrictions

- pdm_replace kann nur auf einem CA Service Desk Manager-Server ausgeführt werden.
- Nur der berechtigte Benutzer oder Root können "pdm_replace" ausführen.
- Führen Sie pdm_replace nicht aus, wenn Benutzer in CA Service Desk Manager 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 1061)

[pdm_userload – Hinzufügen, Aktualisieren und Löschen von Datenbank-Datensätzen](#) (siehe Seite 1090)

pdm_restore – Wiederherstellen einer Datenbank

pdm_restore hält CA Service Desk Manager an, löscht alle Datensätze aus einer CA Service Desk Manager-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 Service Desk Manager-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
```

Restrictions

pdm_restore kann nur auf einem CA Service Desk Manager-Server ausgeführt werden. Nur der berechtigte Benutzer oder Root können "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 Benutzer in CA Service Desk Manager 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" erstellt wurde.

Wichtig! Bei UNIX muss der LIBPATH vor der Ausführung mehrerer CA Service Desk Manager-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:

[Datenbankwiederherstellung](#) (siehe Seite 467)

[pdm_backup – Exportieren der Datenbank in eine ASCII-Datei](#) (siehe Seite 1048)

[pdm_userload – Hinzufügen, Aktualisieren und Löschen von Datenbank-Datensätzen](#) (siehe Seite 1090)

pdm_status – Anzeigen des Status von Daemons oder Prozessen

pdm_status zeigt den Status aller Daemons (UNIX) oder Prozesse (Windows) von CA Service Desk Manager 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 1097).

pdm_text_cmd – Befehlszeilenschnittstelle für Text-API

"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.

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
- Anforderung

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 Benutzerkennung.

-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". Weitere Informationen finden Sie unter [Verwenden der Text-API](#) (siehe Seite 489).

-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 Service Desk Manager-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.

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 Service Desk Manager oder von Daten aus Integrationen mit anderen CA-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 cnvtrs.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 Service Desk Manager-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 Service Desk Manager 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 Service Desk Manager 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 Service Desk Manager-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 Service Desk Manager 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 Service Desk Manager-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, NONNEWID)

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").

Restrictions

Sie können pdm_userload ausführen, während CA Service Desk Manager aktiv ist; die Leistung kann jedoch sehr beeinträchtigt werden. Führen Sie pdm_userload am besten aus, wenn kein Benutzer CA Service Desk Manager verwendet.

Weitere Informationen:

[pdm_backup – Exportieren der Datenbank in eine ASCII-Datei](#) (siehe Seite 1048)

[pdm_replace – Ersetzen einer Datenbanktabelle](#) (siehe Seite 1079)

[pdm_restore – Wiederherstellen einer Datenbank](#) (siehe Seite 1081)

pdm_webstat – Zurückgeben von Webnutzungsstatistiken

Verwenden Sie pdm_webstat, um Statistiken für CA Service Desk Manager-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
```

```
=====
Report 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
```

```
=====
Report 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 Service Desk Manager-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.

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".

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 Service Desk Manager 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']
```

Restrictions

"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.

Anhang D: Formulargruppen

Dieses Kapitel enthält folgende Themen:

[Formulargruppe "Kunden"](#) (siehe Seite 1101)

[Formulargruppe "Mitarbeiter"](#) (siehe Seite 1102)

[Formulargruppe "Analysten"](#) (siehe Seite 1104)

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

H

- 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.html

- [html_editor_insert_table.html](#)
- [html_editor_tabs.html](#)
- [html_editor_toolbar.html](#)

I

- [insert_iss_wf.html](#)
- [insert_wf.html](#)
- [in_relreq_tab.html](#)
- [isscat_auto_assignment_tab.html](#)
- [isscat_prptpl_tab.html](#)
- [isscat_wftpl_tab.html](#)
- [issue_status_change.html](#)
- [iss_accumulate.html](#)
- [iss_close_all_child.html](#)
- [iss_custfld_tab.html](#)
- [iss_expedite.html](#)
- [iss_lr.html](#)
- [iss_reliss_tab.html](#)
- [iss_resol_tab.html](#)

K

- [kd_action_forward.html](#)
- [kd_action_publish.html](#)
- [kd_action_reject.html](#)
- [kd_action_unpublish.html](#)
- [kd_action_unretire.html](#)
- [kd_attachments_tab.html](#)
- [kd_attributes_tab.html](#)
- [kd_categories_tab.html](#)
- [kd_content_tab.html](#)
- [kd_file_prop_tab.html](#)
- [kd_permissions_tab.html](#)
- [kd_qa_attributes_tab.html](#)
- [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
- saprobttyp_dh_tab.html
- saprobttyp_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