

CA Service Desk Manager

Implementierungshandbuch

Version 12.9.00



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

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

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

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

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

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

Diese Dokumentation wurde von CA hergestellt.

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

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

CA Technologies-Produktreferenzen

Diese Dokumentation verweist auf die folgenden CA Technologies-Marken und -Produkte:

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

Technischer Support – Kontaktinformationen

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

Inhalt

Kapitel 1: Einführung 15

Überblick	15
Zielgruppe	15
Liste der Standardanwender von CA SDM	16
Serverkomponenten	17

Kapitel 2: Aktualisieren 27

So planen Sie CA SDM-Upgrades.....	27
Hinweise zur Datenbank	29
Hinweise zu Knowledge Management.....	32
DocType-Validierung.....	33
Übernehmen von Anpassungen.....	33
Hinweise zur LREL-Migration	38
Hinweise zum Statusübergang.....	40
Aktualisieren der E-Mail.....	40
Funktionsweise der Migrationskonsole	43
Protokolldatei der Migration	44
Manuelles Starten des Migrationsprozesses	44
Aktualisieren von CA CMDB von einer Vorgängerversion.....	45
Migration zu CA SDM r12.9 unter einem Linux/UNIX-64-Bit-Betriebssystem	47
Migration zu CA SDM r12.9 unter einem Windows-64-Bit-Betriebssystem	48
Beispiel: Migrieren von einer nicht unterstützten Windows-Umgebung	48
Beispiel: Migrieren von einer nicht unterstützten Windows-Umgebung	49
Support-Automatisierung-Datenmigration	50
Migrieren von Support-Automatisierung-Datenbanken	50
Konvertieren von Bereichen zu Mandanten	51
Exportieren von CA Support-Automatisierung-Daten	52
Importieren von Support-Automatisierung-Daten	54
Konfigurieren des Support-Automatisierung-Rollenzugriffs nach der Migration	54
Migrieren eines benutzerdefinierten CA Business Intelligence-Universums	55
Erstellen einer Sicherungskopie von einem benutzerdefinierten Universum	55
Installieren eines CA Business Intelligence-Universums	56
Aktualisieren einer Universe-Verbindung.....	56
Konfiguration nach der Aktualisierung.....	57
Inaktive Server, die keine primären oder sekundären Server sind	57
Vorhandene Kunden mit EEM 8.4-Server unterstützen.....	57

Aktualisieren von CA Workflow und CA EEM.....	57
Vorherige Serverkonfiguration beibehalten	59
Integration von CA SDM und CA IT PAM aktivieren	59
Löschen des Cache von Web-Engine und Browser	60
Konfigurieren des Web-Director und der Server	60
LREL nach der Migration	60
Bearbeiten von Zugriffstypen.....	64
Aktivieren der Prioritätsberechnung.....	64
Hinzufügen des Felds "Incident-Priorität" zu Incidents	65
Hinzufügen des Felds "Dringlichkeit" zu Mitarbeiter-Tickets.....	66
Festlegen von Ticket-Werten für Self-Service-Benutzer	67
Aktivieren von Statusübergängen	70
Aktivieren von Übergangstypen.....	71
Anpassen der Bereiche für funktionalen Zugriff	72
Die Datei SITEMODS.JS.....	74
Anpassen von Zugriffstypen.....	74
Anpassen von Datenpartitionseinstellungen	75
Ändern von Helpsets nach der Aktualisierung der Rollen.....	76
Standardeinstellungen für Einschränkungen	76
Starten der IIS-Web-Schnittstelle (CAisd)	77
Ändern von angepassten HTML-Formularen	78
Aktualisieren von Knowledge Management von Version r11.2.....	78
So aktualisieren Sie Knowledge Management von CA SDM r12.x	81

Kapitel 3: Planung 85

Standardports und empfohlene Ports für CA SDM	85
So planen Sie für erweiterte Verfügbarkeit.....	88
CA SDM-Architektur für erweiterte Verfügbarkeit	89
Entscheidung zur Konfiguration für erweiterte Verfügbarkeit	91
Überlegungen zur Konfiguration für erweiterte Verfügbarkeit	91
Planen der CA MDB-Installation	99
Hinweise zu CA MDB	100
Planen der CA SDM-Installation	102
Hinweise zu CA SDM	105
Planen der Installation von CA NSM	116
Planen der Installation von CA EEM und CA Workflow	116
Hinweise zu CA EEM.....	118
Hinweise zu CA Workflow	118
Planen der Integration von CA Process Automation	123
Sicherheitsempfehlungen	124
Einrichten von SSL-Kommunikation mit CA Process Automation	125

Installationsplanung für CA Business Intelligence	128
Hinweise zu Berichten	130
Best Practices bei der Berichtserstellung	134
Implementierungsstrategien	134
Aktivieren der Windows-Authentifizierung in Firefox	135

Kapitel 4: Wird installiert 137

Implementieren der Software	137
So konfigurieren Sie CA SDM-Server	138
Konfigurieren des Primärservers	140
Hinzufügen eines Servers	140
Konfigurieren der Sekundärserver	142
Konfigurieren des Hintergrundservers	142
Konfigurieren der Standby-Server oder Anwendungsserver	143
Überprüfen der Serverdetails	145
So führen Sie eine Konvertierung von der konventionellen Konfiguration in eine Konfiguration für erweiterte Verfügbarkeit durch	146
Deaktivieren aller Sekundärserver	147
Konfigurieren des Hintergrundservers	148
Ändern des Sekundärservertyps	148
Konfigurieren der Standby-Server und Anwendungsserver	149
Überprüfen der Serverdetails	150
So führen Sie eine Konvertierung von der Konfiguration für erweiterte Verfügbarkeit in eine konventionelle Konfiguration durch	152
Überprüfen der Voraussetzungen	153
Deaktivieren aller Anwendungsserver und Standby-Server	153
Konfigurieren des Primärservers	154
Überprüfen der Serverdetails	154
Konfigurieren der Sekundärserver	155
Überprüfen der Serverdetails	155
So installieren Sie CA MDB	156
MDB-Installationen	157
Suchen nach Informationen zur Produktintegration und Kompatibilität	157
Installieren unter SQL Server (Windows)	158
Installieren auf Oracle (Windows)	160
Installieren in der Oracle-Umgebung (Linux/UNIX)	163
Installieren einer Remote-MDB unter HP-UX	164
So installieren Sie CA SDM	165
Variablen der Oracle-Umgebung	166
Installieren unter SQL Server (Windows)	166
Installieren auf Oracle (Windows)	168
Installieren in der Oracle-Umgebung (Linux/UNIX)	173

Visualizer-Konfiguration	174
Konfigurieren von Visualizer auf einem Sekundärserver	175
Konfiguration von Support-Automatisierung-Komponenten	176
So installieren Sie Web Screen Painter	181
So installieren und konfigurieren Sie die CA SDM- und CA NSM-Integration	182
Überprüfen der Hinweise zur Integration	184
Installieren der CA NSM-Integrationskomponente	185
CA SDM-Event Converter	188
Überprüfen der Hinweise zur Post-Integration	189
Überprüfen der CA NSM-Integration	190
Fehlerbehebung bei der CA NSM-Integration	216
Verwenden der CA NSM-Integration	222
So installieren Sie CA EEM	230
Installieren von CA EEM (Windows)	230
Konfigurieren des CA EEM-SDK im FIPS-Compliance-Modus	232
Installieren von CA EEM (UNIX)	232
So installieren Sie CA Workflow	233
Installieren von CA Workflow (Windows)	234
Installieren von CA Workflow (UNIX)	234
Installieren des Standalone-Clients CA Workflow IDE	235
Deinstallieren des CA Workflow IDE-Clients (Windows und Linux)	237
So installieren Sie CA Business Intelligence für CA SDM	237
Planen der CA Business Intelligence-Installation	238
Installieren von CA Business Intelligence	239
Überprüfen der CA Business Intelligence-Installation	240
Überprüfen der Installation	241
Das Installationsprotokoll	242

Kapitel 5: Konfigurieren 243

Produktkonfiguration	243
Konfigurieren der CA SDM-Komponenten	244
Einrichten des CA CMDB-Auditprotokolls	246
Integrieren von CA Cohesion ACM in CA CMDB	246
Konfigurieren von CA CMDB Visualizer unter AIX	246
Modifizieren von Drittanbieter-Skripten für CA CMDB-Kompatibilität	247
Umschalten des Zielservers für CA CMDB-Berichte	247
Konfigurieren der Webschnittstelle	248
Hinzufügen von Web-Engines oder Web-Directors	249
Konfigurieren der Web-Schnittstelle	252
Starten der Web-Schnittstelle	252
So implementieren Sie CA Business Intelligence für CA SDM	253

Überprüfen der Voraussetzungen.....	255
Konfigurieren von CA Business Intelligence	255
Überprüfen der Berichte	273
So konfigurieren Sie integrierte Windows-Authentifizierung für CA SDM.....	274
Überprüfen der Voraussetzungen.....	275
Konfigurieren von IIS für IWA.....	276
Konfigurieren von CA SDM für IWA	277
Testen von IWA	278
Ausführen der Automatisierungsrichtlinien	278
Ausführen der Knowledge-Berichtskarte	279
Knowledge Management-Beispieldatenimport	280
Konfiguration der Such-Engine.....	281
"pdm_k_reindex" — Dienstprogramm zur Knowledge-Neuindizierung.....	281
Neue Tags für die Konfiguration eines Domservers für die Crawler-Oberfläche	283
So konfigurieren Sie CA Workflow:	283
Starten und Anhalten von CA Workflow	284
Einrichten der automatischen Anmeldung (Externe Authentifizierung).....	288
Konfigurieren der Worklist und des Workflow-Managers für die automatische Anmeldung	289
Konfigurieren der Workflow-Entwicklungsumgebung für die automatische Anmeldung	290
CA Workflow-Optionen	291
Konfigurieren des Problem Management-Beispiel-Workflows	292
Konfigurieren des Beispiel-Workflows "PC-Auftrag"	294
Beispiel einer Change-Management-Prozessdefinition	295
Konfigurieren der Workflow-Integration in CA Process Automation.....	299
Überprüfen der Installationen von CA Process Automation und CA SDM.....	300
Konfigurieren von CA Process Automation Workflow-Optionen.....	300
CA Process Automation-Anwenderverwaltung.....	304
Unterstützen von Single Sign-On von CA SDM bei CA Process Automation mithilfe CA EEM	305
Einrichten der automatischen Anmeldung (CA MDB-Authentifizierung)	307
Konfigurieren des "Single Point of Entry"	308
Implementieren der Mandantenfähigkeit	309
Mehrere Mandanten.....	311
Implementieren der Mandantenfähigkeit	316
Aktivieren von Multi-Tenancy	329
Exportieren und Importieren von Mandantendaten	338
Dienstprogramme für mehrere Mandanten	341
So aktivieren Sie Auto-Failover	350

Kapitel 6: Anpassung **353**

Kapitel 7: Anpassung – Übersicht **355**

So verschieben Sie das Authentifizierungsmodul zu einem externen Server	356
Überprüfen der Voraussetzungen.....	358
Konfigurieren von CA SDM für die Verwendung der externen Authentifizierung	359
So starten Sie die CA SDM-Server neu	360
Überprüfen der Authentifizierung	363
Anpassen der Benachrichtigungsmethode	364
Benachrichtigungsprozess.....	364
Variablen der Benachrichtigungsmethode	365
Erstellen einer angepassten Benachrichtigungsmethode.....	370
Anpassen von Abfragen und Meldungen	373
Scoreboard-Abfragen	374
ITIL-spezifische Abfragen	381
Anpassen der Meldung für Aktivitätsbenachrichtigungen.....	381
Anpassen der Webschnittstelle.....	388
So passen Sie das Schema mithilfe von Web Screen Painter an	389
So passen Sie eine Web-Schnittstelle von Web Screen Painter an.....	408

Kapitel 8: Ändern einer Datenrasterliste auf einem Listenformular **427**

HTML-Vorlagen (HTMPL-Formular).....	433
HTMPL-Tags	438
Servervariablen	462
Unterstützte Servervorgänge.....	469
Erweiterte Anpassung	477

Kapitel 9: Anpassung der Event-Protokoll-Datenspeicherung **509**

Anpassen von CA Business Intelligence-Berichten.....	511
Infrastruktur von CA Business Intelligence	512
Entwicklungsumgebung	513
Rahmen	515
Schemaänderungen an der Infrastruktur.....	518
Berichts- und Ordnerstrukturen.....	521
Übernehmen von neuen Crystal Reports in CA Business Intelligence	526
Übernehmen vorhandener Access-Berichte in CA Business Intelligence	527
Verschieben aus der Entwicklung in die Produktion.....	528
Anpassen von Legacy-Berichten.....	529
Benutzerdefinierte Berichtslayouts	530
Erstellen von Berichten	538

Berichtsvorlagenreferenz	539
Anpassen von Crystal Reports.....	555

Kapitel 10: Füllen von CA CMDB **557**

Füllen der Datenbank	557
Füllen der Datenbank durch GRLoader	557
Importieren von Daten mit GRLoader	558
Familien- und Klassenzuweisungen.....	558
Laden von CA APM-Daten	559

Kapitel 11: Benutzen des MDR Launcher **561**

Der MDR Launcher	562
MDR-Terminologie	563
MDR-Zuordnung.....	564
Starten von MDR	564
CMDBf Viewer	565
Definieren eines MDR für CA CMDB	565
MDR URL-Definitionen	569
MDR-Start-URL.....	570
Parameter für die URL-Ersetzungen.....	572
Zusammenschlüsse unter Verwendung von GRLoader	574
Föderieren eines CI	574
Definieren von mehreren MDRs für ein CI mit GRLoader	575
Zuordnen zwischen MDR-CIs und CA CMDB-CIs	576
Konfigurieren von MDRs für CMDBf Viewer	578
Starten der MDR-Webbrowser-Schnittstelle	578
Integration von CA Cohesion.....	579

Kapitel 12: Verwalten von Webservices **581**

Verwalten von Webservices	581
CA SDM-Komponenten	582
Tipps für SOAP-Webservices-Clients	582
Java-Clients	583
Konfiguration der SOAP Webservices	585
Erneute Bereitstellung der Webservices.....	586
Sicherheit von Webservices	587
Fehlerbehandlung in SOAP.....	589
Sperrfehler	590
Zeitüberschreitungen.....	591
Fehlercodes	591

Installation von Webservices	593
Aktivieren der Entwicklungszeit	593
Externe Spezifikationen	594
Benutzerzugriffsauthentifizierung	594
Benutzername/Kennwort-Authentifizierung	594
PKI-Authentifizierung (Public Key Infrastructure)	596
Sitzung und Autorisierung	601
Zugriffssteuerung und -verwaltung	602
Objekte	613
Systemaktualisierungen und Zwischenspeicherung	614
Kategorien und Eigenschaften	615
XML-Objektrückgaben	616
ITIL Methodology	618
Erstellen von Incidents oder Problemen	618
Abfragen zu Incidents oder Problemen	619
Anhängen eines Incident an ein Problem	620
Anhängen eines Problems an einen Change	620
Konfigurationselemente	620
Verwenden der Webservices	621
Anmeldungen	621
Durchführen allgemeiner Aufgaben	621
REST und SOAP	625
REST Sicherheit	626
Webserviceoptionen	628

Kapitel 13: Integration mit anderen Produkten 631

CA Workflow-Integration	631
CA Workflow-Komponenten	632
CA Workflow-Zugriff	635
CA Portal-Integration	637
Überprüfen des Zugriffs auf die Web-Schnittstelle von CA SDM	637
Installieren und Starten von CA Portal	637
Konfigurieren von CA SDM für die Verwendung von SSL mit CA Portal	639
Integration von Mainframe-Produkten	643
Laden von CA SDM-Ergänzungsdaten	644
CA-Produkte, die gegenwärtig CAISDI nutzen	644
CA-Produkte, bei denen die Nutzung von CAISDI geplant ist	645
Integration von CA Business Service Insight	646
Anzeigen von CA BSI-Informationen in CA SDM	648

Kapitel 14: Beispiele-Verzeichnis **653**

Inhalt des Beispiele-Verzeichnisses.....	653
Ändern des Meldungskatalogs.....	653
call_mgt.....	654
Daten.....	655
macro_lock.....	655
Mehrere Mandanten.....	655
pdmconf.....	655
Berichterstellung.....	656
sdk.....	656
Ansichten	657

Kapitel 15: Laden von ergänzendem Inhalten **659**

sd_content.dat	659

Kapitel 1: Einführung

Dieses Kapitel enthält folgende Themen:

[Überblick](#) (siehe Seite 15)

[Zielgruppe](#) (siehe Seite 15)

[Liste der Standardanwender von CA SDM](#) (siehe Seite 16)

[Serverkomponenten](#) (siehe Seite 17)

Überblick

Dieses Handbuch bietet Ihnen Informationen, die Sie für eine erfolgreiche CA SDM-Implementierung in Ihrem Unternehmen benötigen. Dazu gehören auch Anleitungen zu folgenden Vorgängen:

- Neuinstallationen und Aktualisierungen planen und vorbereiten
- Alle erforderlichen Produktkomponenten installieren und aktualisieren
- Produktkomponenten konfigurieren
- In andere CA-Produkte integrieren

Hinweis: In diesem Handbuch wird *nicht* die Integration in alle CA Technologies-Produkte beschrieben. Ausführliche Informationen zur Integration von weiteren Produkten in CA SDM, die in diesem Handbuch nicht enthalten sind, finden Sie im *CA Unicenter Service Desk Green Book zur Integration* unter <http://ca.com/support>.

Hinweis: Die aktuellste Version der Versionshinweise mit den jeweils gültigen Systembedingungen und der optionalen Readme-Datei (sofern verfügbar) finden Sie unter <http://ca.com/support>.

Zielgruppe

Dieses Handbuch richtet sich an alle, die wissen möchten, wie CA SDM installiert, aktualisiert und konfiguriert wird. Die folgenden Anwender können bei der Durchführung ihrer Aufgaben auf die Informationen in diesem Handbuch zurückgreifen:

- *Systemadministratoren* und *Administratoren* können mit den Informationen in diesem Handbuch in Kombination mit ihren Betriebssystemkenntnissen das Produkt zum ersten Mal installieren, mit neuen Versionen aktualisieren und gemäß den Implementierungsanforderungen konfigurieren.

- *Systemintegratoren* dienen die Informationen in diesem Handbuch in Verbindung mit ihren CA Technologies-Produktkenntnissen, um CA SDM erfolgreich in andere CA Technologies-Produkte zu integrieren.

Hinweis: In diesem Handbuch wird *nicht* die Integration in alle CA Technologies-Produkte beschrieben. Ausführliche Informationen zur Integration von weiteren Produkten in CA SDM, die in diesem Handbuch nicht enthalten sind, finden Sie im *CA Unicenter Service Desk Green Book zur Integration* unter <http://ca.com/support>.

- *Anwender* können bei Bedarf aufgrund der Informationen in diesem Handbuch das Produkt und die Komponenten installieren.

Um die Informationen in diesem Handbuch nutzen zu können, sind folgende Voraussetzungen erforderlich:

- Kenntnisse über die Betriebssysteme Windows und/oder UNIX, je nach Ihrer aktuellen Produktionsumgebung.
- Die Fähigkeit, grundlegende administrative Aufgaben für Ihr Betriebssystem zu erfüllen.
- Möglicherweise müssen Sie abhängig von Ihrer Arbeitsumwelt auch mit Großrechnern, mobilen Geräten, und Serverinstallationen vertraut sein.

Hinweis: In diesem Handbuch werden Sie immer wieder Referenzen zu NX_ROOT finden. Die Referenzen betreffen die Umgebungsvariable, die den Installationspfad von CA SDM enthält. Die Variable NX_ROOT wird in der Konfigurationsdatei NX.env festgelegt, die zur Definition von Umgebungsvariablen für CA SDM verwendet wird.

Beispiel zur NX_ROOT-Definition

@NX_ROOT=C:\Programme\CA\Service Desk Manager

Liste der Standardanwender von CA SDM

In der folgenden Liste sind die Standardanwenderinformationen für typische CA SDM-Implementierungen aufgeführt:

OS	Produkt	Standardanwender name	Betriebssyst emebene?	Art der Erstellung
Windows	CA SDM	ServiceDesk	Ja	Automatisch
	CA EEM	EiamAdmin		Standardkennwort: EiamAdmin
	CA MDB SQL Server	ServiceDesk	Nein	Während der Konfiguration in der MDB erstellt

OS	Produkt	Standardanwender name	Betriebssyst emebene?	Art der Erstellung
	CA MDB Oracle	mdbadmin	Nein	Während der Konfiguration in der MDB erstellt
UNIX	CA SDM	svcdesk	Ja	Manuell erstellt
	CA MDB Oracle	mdbadmin	Nein	Während der Konfiguration in der MDB erstellt
Linux	CA SDM	svcdesk	Ja	Manuell erstellt
	CA MDB Oracle	mdbadmin	Nein	Während der Konfiguration in der MDB erstellt

Serverkomponenten

CA SDM enthält Komponenten, die abhängig von der CA SDM-Konfiguration zusammen funktionieren und auf verschiedenen Servern ausgeführt werden. Vor der Implementierung sollten Sie die grundlegenden Merkmale der folgenden Komponenten kennen:

Daemon-Manager (pdm_d_mgr)

Startet Prozess-Sätze gemäß der Definition in der Startdatei "pdm_startup". Standardmäßig versucht der Daemon Manager bis zu 10 Mal, eine fehlgeschlagene Komponente zu starten. Um den Status aller CA SDM-Komponenten zu prüfen, verwenden Sie das Hilfsprogramm "pdm_status". Das Hilfsprogramm "pdm_d_refresh" weist den Daemon Manager an, einen neuen Zyklus von 10 Versuchen zu starten, um alle Prozesse zu starten, die zuvor als fehlgeschlagen markiert wurden.

Der Daemon-Manager wird auf allen CA SDM-Servern ausgeführt.

Message Dispatcher (sslump_nxd)

Agiert als gemeinsamer Bus oder gemeinsames System für die Meldungsübermittlung. Komponenten, die miteinander kommunizieren müssen, melden sich zuerst beim Message Dispatcher an. Wenn eine Komponente eine Meldung sendet, liefert der Message Dispatcher diese an diejenigen Komponenten, die sich für den Erhalt dieser Art von Meldung registriert haben. Wenn zwei Komponenten soviel kommunizieren, dass es ineffizient wäre, die Meldungen über den Message Dispatcher zu senden, erstellen sie einen direkten schnellen Kanal zwischen sich. Mit Hilfe des Hilfsprogramms *s/stat* können Sie eine Liste der registrierten Komponenten anzeigen.

Der "Message Dispatcher" wird abhängig von Ihrer CA SDM-Konfiguration auf folgenden Servern ausgeführt:

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

Database Agent (platform_agent)

Führt SQL-Abfragen in der Datenbank durch. Datenbank-Agenten nutzen das logische Schema von CA SDM und übersetzen das SQL auf dieser Ebene in physisches Datenbankplattform-SQL.

Hinweis: Der Datenbank-Agent erkennt die momentane Unterbrechung sowie fehlgeschlagene Abfragen und versucht die Verbindung wiederherzustellen und mit der Datenbank zu kommunizieren. Dies ist nur für kurze Ausfälle gedacht, z. B. für einen kurzen Netzausfall und eine vorübergehende Unterbrechung. Nicht gedacht ist dieses Verfahren für längere Ausfälle, z. B. für das Herunterfahren eines Datenbankdienstes zu Wartungszwecken usw. Der Agent wiederholt den Versuch, die Verbindung wieder aufzubauen, nur eine definierte Anzahl von Versuchen (der Standardwert beträgt 3 Mal) und nur für einen kurzen Zeitraum von einigen Minuten. Wenn der Ausfall länger als einige Minuten dauert, beendet der Agent den Versuch, die Verbindung wiederherzustellen, und CA SDM muss, wenn die Datenbank wieder zur Verfügung steht, neu gestartet werden.

Der "Database Agent" wird abhängig von Ihrer CA SDM-Konfiguration auf folgenden Servern ausgeführt:

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

Agent Provider (platform_prov_nxd)

Startet oder beendet den Datenbank-Agenten. Standardmäßig werden mehrere Agenten ausgeführt. Wenn mehr Agenten erforderlich sind, um die Anzahl der Datenbankabfragen zu bearbeiten, werden sie vom Agent Provider gestartet. Wenn das System nicht mehr so viele Datenbank-Agenten erfordert, beendet der Agent Provider die überflüssigen Datenbank-Agenten.

Der "Agent Provider" wird abhängig von Ihrer CA SDM-Konfiguration auf folgenden Servern ausgeführt:

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

Virtual Database (bpvirtddb_srvr)

Aktiviert den Betrieb mehrerer Objektmanager. Alle Objekt-Manager, die auf primären oder sekundären Servern ausgeführt werden, sind mit der virtuellen Datenbank verknüpft, die deren Zugriff auf die Datenbank-Agenten regelt. Zum Beispiel hilft die virtuelle Datenbank beim Abrufen eines neuen Bereichs von Ticketreferenznummern sicherzustellen, dass nur ein Objekt-Manager auf einmal auf die Tabelle zugreift, die die Referenznummern enthält. Die virtuelle Datenbank sorgt auch für das Zwischenspeichern der Datenbankinformationen für die Objektmanager.

Der "Virtual Database" wird abhängig von Ihrer CA SDM-Konfiguration auf folgenden Servern ausgeführt:

- Konventionell: Primärserver.
- Erweiterte Verfügbarkeit: Alle Server

Continuous Archive and Purge (arcpur_srvr)

Führt Ihre Archivierungs- und Lösungsregeln gemäß der Konfiguration durch den CA SDM-Administrator aus.

"Continuous Archive and Purge" wird abhängig von Ihrer CA SDM-Konfiguration auf folgenden Servern ausgeführt:

- Konventionell: Primärserver.
- Erweiterte Verfügbarkeit: Hintergrundserver

Database Monitor (dbmonitor_nxd)

Überwacht Änderungen an gemeinsamen Tabellen in der CA MDB, z. B. *ca_contact*.

Der "Database Monitor" wird abhängig von Ihrer CA SDM-Konfiguration auf folgenden Servern ausgeführt:

- Konventionell: Primärserver.
- Erweiterte Verfügbarkeit: Hintergrundserver

Mail Daemon (pdm_mail_nxd)

Sendet ausgehende E-Mail-Benachrichtigungen.

Der "Mail Daemon" wird abhängig von Ihrer CA SDM-Konfiguration auf folgenden Servern ausgeführt:

- Konventionell: Primärserver
- Erweiterte Verfügbarkeit: Alle Server.

Mail Eater (pdm_maileater_nxd)

Empfängt eingehende E-Mail für die Ticketerstellung und Updates.

Der Daemon "Mail Eater" wird abhängig von Ihrer CA SDM-Konfiguration auf folgenden Servern ausgeführt:

- Konventionell: Primärserver
- Erweiterte Verfügbarkeit: Hintergrundserver

Notification Manager (bpnotify_nxd)

Verwaltet Benachrichtigungen in einer Windows-Umgebung. Der "Notification Manager" wird abhängig von Ihrer CA SDM-Konfiguration auf folgenden Servern ausgeführt:

- Konventionell: Primärserver.
- Erweiterte Verfügbarkeit: Anwendungsserver, Hintergrundserver und Standby-Server.

Spell Checker (lexagent_nxd)

Führt die Rechtschreibprüfung entsprechend der Anforderungen der Clients durch. Der "Spell Checker" wird auf allen CA SDM-Servern ausgeführt.

Text API Daemon (pdm_text_nxd)

Erstellt und aktualisiert Tickets von externen Schnittstellen, z. B. Befehlszeile und E-Mail. Der "Text API Daemon" wird auf allen CA SDM-Servern ausgeführt.

Timed Event (animator_nxd)

Führt die Verzögerungszeiten der Ereignisse aus. In einer Implementierung mit vielen Servicetypen oder Verträgen kann es sein, dass die Timed Event-Maschine viele aktive Ereignisse verfolgen muss. In dieser Lage sollten Sie den Objektmanager des primären Servers ausschließlich der Timed Event-Maschine zuordnen. Sie können andere Objektmanager auf dem primären oder dem sekundären Server nach Bedarf für den Produktzugriff konfigurieren.

Der Daemon "Timed Event" wird abhängig von Ihrer CA SDM-Konfiguration auf folgenden Servern ausgeführt:

- Konventionell: Primärserver
- Erweiterte Verfügbarkeit: Hintergrundserver

Time-To-Violation (ttv_nxd)

Berechnet die voraussichtlichen Verletzungszeiten für Servicetypen. Der Daemon "Time-To-Violation" wird abhängig von Ihrer CA SDM-Konfiguration auf folgenden Servern ausgeführt:

- Konventionell: Primärserver
- Erweiterte Verfügbarkeit: Hintergrundserver

Proctor-Daemon (pdm_proctor_nxd)

(Nur Windows) Bewirkt den Start und den Neustart von CA SDM-Komponenten gemäß den Anweisungen des Daemon Managers auf primären und sekundären Servern. Wenn Sie einen sekundären Server installieren, ist der Prozess *pdm_proctor_nxd* als CA SDM-Remote-Daemon-Überwachungsservice installiert. Wenn der primäre Server startet, weist der Daemon Manager den Remote-Daemon-Proctor an, eine Verbindung zum Message Dispatcher herzustellen. Anschließend weist der Daemon Manager den Remote-Daemon-Proctor an, Komponenten auf dem sekundären Server gemäß der Definition durch die Prozess-Sätze in der Startdatei "*pdm_startup*" zu starten. Der "Proctor-Daemon" wird auf allen CA SDM-Servern in der Konfiguration für erweiterte Verfügbarkeit ausgeführt.

Objektmanager (domsrvr)

Agiert als Serverprozess von CA SDM. Wenn Sie einen primären Server installieren, sind standardmäßig zwei Objektmanager installiert: einer für Verbindungen zum Produkt, und einer, der ausschließlich dem Web Screen Painter zugeordnet ist. Dies ermöglicht Ihnen, Ihre Änderungen zu prüfen, ohne die Produktionsumgebung zu beeinträchtigen. Wenn Sie einen sekundären Server installieren, können Sie zusätzliche Objektmanager konfigurieren.

Es muss immer einen Standardobjektmanager geben, der auf dem primären Server ausgeführt wird, mit dem sich Clients wie z. B. die Timed Event-Maschine verbinden können.

Der Objektmanager sorgt auch für das Zwischenspeichern verschiedener Datensätze und Tabellen für Clients. Wenn Sie *pdm_userload* verwenden, um diese Datensätze zu ändern, können Sie auch das Hilfsprogramm *pdm_cache_refresh* verwenden, um den Objektmanager für den Abruf der neuen Daten einzusetzen. Der Objektmanager wird auf allen CA SDM-Servern in der Konfiguration für erweiterte Verfügbarkeit ausgeführt.

Method Engine (spel_srvr)

Bewirkt die Ausführung von SPEL-Code, Ereignissen, Makros usw. für einen Objektmanager. Es wird empfohlen, jeden Objektmanager mit seiner eigenen Methodenengine auszuführen.

Die "Method Engine" wird auf allen CA SDM-Servern ausgeführt.

Login Server (boplgln)

Verwaltet authentifizierte Anwendersitzungen.

Der "Login Server" wird abhängig von Ihrer CA SDM-Konfiguration auf folgenden Servern ausgeführt:

- Konventionell: Primärserver
- Erweiterte Verfügbarkeit: Alle Server

LDAP Virtual Database (ldap_virtddb)

Schnittstellen mit einem LDAP-Verzeichnis. Die "LDAP Virtual Database" wird abhängig von Ihrer CA SDM-Konfiguration auf folgenden Servern ausgeführt:

- Konventionell: Primärserver oder Sekundärserver
- Erweiterte Verfügbarkeit: Hintergrundserver oder Anwendungsserver

Knowledge Management-Such-Daemon (bpebr_nxd)

Führt Suchvorgänge in der Knowledge Base durch. Beim Start von CA SDM bewirkt der Daemon bpebr_nxd das Zwischenspeichern von Knowledge-Dokumentdaten aus der Datenbank in seinem Speicher. Bei einer großen Dokumentenbasis können dadurch Speicherprobleme auftreten. Für den Daemon "bpebr_nxd" gelten die folgenden Größenbedingungen:

Knowledge Management-Suche

- 100.000 Dokumente
- Speichergröße = 332.000 KB

Der "Knowledge Management Daemon" wird abhängig von Ihrer CA SDM-Konfiguration auf folgenden Servern ausgeführt:

- Konventionell: Primärserver oder Sekundärserver
- Erweiterte Verfügbarkeit: Hintergrundserver

Knowledge Management/Keyword Indexing Daemon (bpeid_nxd)

Indiziert die Knowledge Base.

Der "Keyword Index Daemon" wird abhängig von Ihrer CA SDM-Konfiguration auf folgenden Servern ausgeführt:

- Konventionell: Primärserver oder Sekundärserver
- Erweiterte Verfügbarkeit: Hintergrundserver

Knowledge Management-Daemon für FAQ-Einstufungen (bu_daemon)

Berechnet FAQ-Bewertungen für Knowledge Management. Wird abhängig von der CA SDM-Konfiguration auf folgenden Servern ausgeführt:

- Konventionell: Primärserver oder Sekundärserver
- Erweiterte Verfügbarkeit: Hintergrundserver

Knowledge Report Card Daemon (krc_daemon)

Führt Berechnungen für die Funktion Knowledge Management-Knowledge-Berichtskarte (KRC) durch. Mit dieser Funktion können Analysten und Manager, verschiedene Matrizenansichten ihrer Knowledge-Beiträge anzeigen und Feedback dazu abgeben, welche Dokumente am effektivsten sind. Die angezeigten Informationen können auf verschiedene Weise genutzt werden, um die Abläufe beim Erstellen von Knowledge-Dokumenten zu verbessern und somit den Kunden bestmöglich zu unterstützen.

Der "Knowledge Report Card Daemon" wird abhängig von Ihrer CA SDM-Konfiguration auf folgenden Servern ausgeführt:

- Konventionell: Primärserver oder Sekundärserver
- Erweiterte Verfügbarkeit: Hintergrundserver

Knowledge Management-Daemon (kt_daemon)

Verwaltet die Knowledge Base-Administration und die Knowledge Management-Logik. Dieser Daemon verwaltet auch Benachrichtigungen sowie den Dokumentgenehmigungsvorgang. Der "Knowledge Management Daemon" wird auf allen CA SDM-Servern ausgeführt.

Repository Daemon (rep_daemon)

Verwaltet die Anhang-Repositorys für CA SDM und den Knowledge Management/Daemon für die Schlüsselwortsuche. Der "Repository Daemon" wird abhängig von Ihrer CA SDM-Konfiguration auf folgenden Servern ausgeführt:

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

Version Control Daemon (pdm_ver_nxd)

Synchronisiert die Schemadateien zwischen einem primären und einem sekundären Server, um sicherzustellen, dass sie das gleiche Schema verwenden. Der "Version Control Daemon" wird abhängig von Ihrer CA SDM-Konfiguration auf folgenden Servern ausgeführt:

- Konventionell: Primärserver
- Erweiterte Verfügbarkeit: Hintergrundserver

Apache Tomcat Web Server (javaw)

Ermöglicht die Implementierung bestimmter Funktionen, unabhängig davon, ob Microsoft Internet Information Server (IIS) als Webserver für den Zugriff auf CA SDM verwendet wird. Zu diesen Funktionen gehören CA Workflow, Diagrammelemente, Anhänge und Webservices.

Der Apache Tomcat-Webserver kann mit dem Apache Tomcat-Controller (*pdm_tomcat_nxd*) verwaltet werden. "Apache Tomcat Web Server" wird auf allen CA SDM-Servern ausgeführt.

Web Engine (webengine)

Verbindet sich mit Webbrowsern durch Ausführen einer *pdmweb cgi* auf einem Microsoft IIS- oder Apache Tomcat-Webserver. Abhängig von Ihrer CA SDM-Konfiguration muss mindestens eine Web-Engine für WSP auf den folgenden Servern vorhanden sein.

Konventionell: Primärserver

Erweiterte Verfügbarkeit: Anwendungsserver, Standby-Server und Hintergrundserver

Dieser Vorgang stellt sicher, dass WSP-Schemadesigner Schemadateien schreiben können. Web-Engines sind der wahre Client eines Objektmanagers, über den ein Webbrowser auf das Produkt zugreift.

Web-Engines bewirken das Zwischenspeichern von .html-Webformularen für verbundene Anwender. Sie können den Cache-Speicher mit dem Hilfsprogramm *pdm_webcache* bearbeiten und mit dem Hilfsprogramm *pdm_webstat* Verbindungsstatistiken für den Webclient anzeigen. Die "Web-Engine" wird auf allen CA SDM-Servern ausgeführt.

RF Broker (pdm_rfbroker_nxd)

(Nur bei der Konfiguration für erweiterte Verfügbarkeit anwendbar). Verwalten Sie die Rollen der Server, und steuern Sie sie über die Konfiguration. Dieser Daemon wird auf allen Servern in der Konfiguration für erweiterte Verfügbarkeit ausgeführt. Er ist verantwortlich dafür, Informationen über Hintergrundserver und Standby-Server zu erfassen und die Informationen (wie z. B. Slump-ID, Knotenname, Servertyp) in der Klasse "ServerStatusMonitor" zu aktualisieren. Es werden Übertragungsmeldungen über Änderungen des Serverstatus und Requests zur Stilllegung empfangen, und es wird eine Anmeldung für "SLUMP_NODE_GONE"-Meldungen durchgeführt, die an "ServerStatusMonitor"-Objekte weitergeleitet werden, wenn der fehlgeschlagene Knoten der Hintergrundserver ist. Dieser Daemon kann nicht für die konventionelle Konfiguration angewendet werden.

Authentifizierung des angemeldeten Anwenders (bopauth_nxd)

Führt die Validierung der Anwenderkonten des Betriebssystems sowie Abfragen von Kontaktdatensätzen mit Hilfe des Felds "Systemanmeldung" durch, um einem Anwender einen Zugriffstyp zuzuordnen.

Wenn Ihr Geschäft CA SDM für andere Client-Geschäfte bereitstellt, können Sie den Anmeldeserver auf einem Sekundärserver an einem Client-Speicherort platzieren. Die externe Authentifizierung kann dann in den Zugriffstypen aktiviert werden. Dadurch wird die Erstellung von Anwenderkonten für Ihre Clients auf Ihren Geschäftssystemen vermieden. Wird abhängig von Ihrer CA SDM-Konfiguration auf folgenden Servern ausgeführt:

- Konventionell: Primärserver oder Sekundärserver (wenn konfiguriert)
- Erweiterte Verfügbarkeit: Hintergrundserver oder Anwendungsserver (wenn konfiguriert)

Intervallprotokollierung (pdm_intrvlog_nxd)

Erfasst die Debugging-Informationen für die Fehlerbehebung im System. Wird auf allen CA SDM-Servern ausgeführt.

QRY KPI Daemon (kpi_qry_daemon)

Führt SQL-Abfragen aus, um Leistungsschlüsselindikatoren in der Datenbank zu aktualisieren. "QRY KPI Daemon" wird abhängig von der CA SDM-Konfiguration auf folgenden Servern ausgeführt:

- Konventionell: Primärserver
- Erweiterte Verfügbarkeit: Hintergrundserver

SYS KPI Daemon (kpi_sys_daemon)

Erfasst Leistungsschlüsselindikatoren des Systemtyps, und schreibt in die Datenbank. "SYS KPI Daemon" wird abhängig von Ihrer CA SDM-Konfiguration auf folgenden Servern ausgeführt:

- Konventionell: Primärserver
- Erweiterte Verfügbarkeit: Alle Server.

Datenbank bestätigen (confirm_db)

Ein Hilfsprogramm, um den Datenbankzugriff zu überprüfen. Wird auf allen CA SDM-Servern ausgeführt.

Datenlexikon (ddictbuild)

Ein Hilfsprogramm, um das Datenlexikon zu erstellen. Wird auf allen CA SDM-Servern ausgeführt.

Set LogFile (pdm_logfile)

Ein Hilfsprogramm, um die maximale Größe der Protokolldatei anzuzeigen oder festzulegen. Wird auf allen CA SDM-Servern ausgeführt.

Report Manager (prrpt_nxd)

Ein Hilfsprogramm für PC-Berichterstellung. Wird auf allen CA SDM-Servern ausgeführt.

RPC Server (rpc_srvr)

Wird verwendet, um ausgehende SOAP-Webservice-Aufrufe zu verwenden. Wird auf allen CA SDM-Servern ausgeführt.

CA SA Tomcat (sa_tomcat)

"CA SA Tomcat" wird verwendet, um Support-Automatisierung auszuführen. Es wird auf einem beliebigen CA SDM-Server konfiguriert.

CAWF Tomcat (cawf_tomcat)

Die Tomcat-Instanz wird verwendet, um CA Workflow auszuführen. Sie kann auf einem beliebigen CA SDM-Server konfiguriert werden.

Visualizer-Tomcat (viz_tomcat)

Die Tomcat-Instanz wird verwendet, um "visualizer" auszuführen. Sie wird abhängig von der CA SDM-Konfiguration auf folgenden Servern konfiguriert:

- Konventionell: Alle Server
- Erweiterte Verfügbarkeit: Anwendungsserver

Event Manager (ehm_nxd)

Der "Event Manager" verwaltet Events aus CA NSM. Der "Event Manager" wird abhängig von Ihrer CA SDM-Konfiguration auf folgenden Servern ausgeführt:

- Konventionell: Primärserver
- Erweiterte Verfügbarkeit: Hintergrundserver

Knowledge ManagementIndexing Daemon (bpeid_nxd)

Ist verantwortlich für das Indizieren der Knowledge-Dokumente. Wird abhängig von der CA SDM-Konfiguration auf folgenden Servern ausgeführt:

- Konventionell: Primärserver
- Erweiterte Verfügbarkeit: Hintergrundserver

Registration Server (mdb_registration_nxd)

Ein Agent zur Abwicklung von MDB-Registrierungs-Requests. Der "Registration Server" wird abhängig von Ihrer CA SDM-Konfiguration auf folgenden Servern ausgeführt:

- Konventionell: Primärserver
- Erweiterte Verfügbarkeit: Alle Server

Kapitel 2: Aktualisieren

Dieses Kapitel enthält folgende Themen:

[So planen Sie CA SDM-Upgrades](#) (siehe Seite 27)

[Funktionsweise der Migrationskonsole](#) (siehe Seite 43)

[Aktualisieren von CA CMDB von einer Vorgängerversion](#) (siehe Seite 45)

[Migration zu CA SDM r12.9 unter einem Linux/UNIX-64-Bit-Betriebssystem](#) (siehe Seite 47)

[Migration zu CA SDM r12.9 unter einem Windows-64-Bit-Betriebssystem](#) (siehe Seite 48)

[Beispiel: Migrieren von einer nicht unterstützten Windows-Umgebung](#) (siehe Seite 48)

[Beispiel: Migrieren von einer nicht unterstützten Windows-Umgebung](#) (siehe Seite 49)

[Support-Automatisierung-Datenmigration](#) (siehe Seite 50)

[Migrieren eines benutzerdefinierten CA Business Intelligence-Universums](#) (siehe Seite 55)

[Konfiguration nach der Aktualisierung](#) (siehe Seite 57)

So planen Sie CA SDM-Upgrades

Verifizieren Sie die folgende Planungsrücksicht auf das CA SDM-Upgrade:

- CA SDM unterstützt Upgrades auf r12.9 von Version r11.2, r12.0, r12.1, r12.5, r12.6 und 12.7 für alle unterstützte Plattformen. Unter Windows können Sie ein Upgrade von r11.2, r12.0, r12.1, r12.5, r12.6, r12.7 direkt auf CA SDM r12.9 durchführen.
- Wenn Sie CA SDM unter Linux oder UNIX installiert haben, sind mehrere Schritte erforderlich, um das Upgrade von den Versionen vor r12.5 auf CA SDM r12.9 durchzuführen. Wenn Ihre Installation auf einer älteren Produktversion ausgeführt wird, wie z. B. r11.2, r12.0 und r12.1 unter Linux/UNIX, müssen Sie das automatisierte Upgrade-Skript für CA SDM r12.5 ausführen und CA SDM auf eine unterstützte Plattform und Datenbank verschieben, bevor das automatisierte Upgrade-Skript für <uskd> r12.9 ausgeführt wird. Wenn Sie über Anpassungen verfügen, dann müssen Sie sie nur einmal anwenden, nachdem Sie das letzte automatisierte Upgrade-Skript auf r12.9 durchgeführt haben.
- Wenn Sie über eine frühere Produktversion, wie Unicenter Service Desk r6.0 oder r11.1 verfügen, *müssen* Sie zuerst auf CA SDM r11.2 und anschließend auf CA SDM r12.9 aktualisieren.
- Hinweis: Wenn Sie zur Datei "NX.env" vor der Migration manuell Variablen hinzugefügt haben, fügen Sie die Variablen nach der Migration erneut manuell ein.

- CA SDM unterstützt nur ITIL. Wenn Sie von einem anderen als einem ITIL-System aktualisieren, wird durch die CA SDM r12.9-Installation auf eine ITIL-Umgebung aktualisiert.
- Wenn Sie eine kombinierte CA SDM r11.2- und CA CMDB r11.1-Installation verwenden, können Sie nicht direkt auf CA SDM r12.9 aktualisieren. Sie *müssen* zuerst CA CMDB auf r11.2 aktualisieren und dann die Aktualisierung r12.9 ausführen. Dadurch wird CA SDM r11.2 auf r12.5 und ebenso CA CMDB r11.2 auf r12.5 aktualisiert. CA CMDB r12.0 und r12.1 kann auch direkt auf CA SDM r12.9 aktualisiert werden.

Hinweis: Weitere Informationen über das Aktualisieren von einer früheren Version finden Sie im *Implementierungshandbuch zu CA SDM r11.2*. Aktualisierungspatches und Unterstützung erhalten Sie vom Technischen Support unter <http://ca.com/support>.

- Bevor Sie auf den aktuellen Release von CA SDM aktualisieren, sollten Sie sich über Folgendes im Klaren sein:
 - [Hinweise zur Datenbank](#) (siehe Seite 29)
 - [Übernehmen von Anpassungen](#) (siehe Seite 33)
 - [Hinweise zur LREL-Migration](#) (siehe Seite 38)
 - [Hinweise zum Statusübergang](#) (siehe Seite 40)
 - [Hinweise zu E-Mail-Optionen](#) (siehe Seite 40)
 - Auf Linux/UNIX-Plattformen muss das UTF-8-Gebietsschema installiert werden.
- Unter Linux/UNIX verwendet CA SDM das Skript smtp_mail für die Verarbeitung ausgehender E-Mail-Benachrichtigungen nicht mehr. Wenn Sie als Kunde smtp_mail verwenden und auf den aktuellen Release aktualisieren, muss Ihr Administrator die entsprechenden E-Mail-Optionen auf der Detailseite "Standardpostfach" konfigurieren, um die Funktion zur E-Mail-Benachrichtigung von CA SDM zu aktivieren.

Hinweise zur Datenbank

Bevor Sie ein Upgrade auf CA SDM r12.9 durchführen, berücksichtigen Sie folgende Informationen zur Datenbank:

- Erstellen Sie mit Hilfe Ihrer üblichen Datenbanksicherungsverfahren eine Sicherungskopie Ihrer vorhandenen Datenbank.
- (Anwendbar für alle Computer mit einem anderen Betriebssystem als Windows)
Wenn die früheren Versionen von CA SDM mit der Oracle 10gr2-Datenbank konfiguriert ist, sollten Sie Oracle 11gr2-Client installieren, bevor Sie ein Upgrade auf CA SDM r12.9 durchführen.

Wichtig! Bevor Sie ein Upgrade durchführen, ändern Sie den Oracle-Startseitenpfad in der Datei \$NXROOT/NX.env auf den Pfad des oracle11g-r2-Clients.

- Nach dem Upgrade sind alle webLicenseCt-KPI-Versionen (aktiv und inaktiv) nicht mehr verfügbar und alle verknüpften KPI-Daten sind ungültig. Diese Daten bleiben noch in der Tabelle "usp_kpi_data" erhalten, werden aber nicht mehr für Berichte abgerufen. Kunden können auch die OOTB-KPI-Regel, KPI-Daten (System) (standardmäßig inaktiv) ausführen, um die Daten zu entfernen.

Wichtig! Wir empfehlen Ihnen, die verfügbaren Daten in der Tabelle "usp_kpi_data" zu überprüfen, da bei der Ausführung dieser KPI-Regel auch andere erfasste System-KPI-Daten archiviert und/oder bereinigt werden.

Hinweis: Ein neuer KPI "webConcurrentTotalLicenseCt" wird in CA SDM r12.9 verwendet, um die Anzahl der einzelnen Anwender zu berechnen, die während dieses Intervalls bei CA SDM angemeldet sind. Weitere Informationen finden Sie im *Implementierungshandbuch*.

- Archivieren Sie mit Hilfe Ihrer üblichen Archivierungsverfahren das Installationsverzeichnis (\$NX_ROOT). Dadurch müssen weniger Daten übertragen werden und Sie sparen Speicherplatz.
- Führen Sie das passende Skript über eine Eingabeaufforderung aus, um etwaige doppelte Datensätze in Ihrer Datenbank zu identifizieren:

Hinweis: Führen Sie dieses Skript auf den sekundären Servern aus. Wenn Sie dieses Skript mithilfe von SQL Query Analyzer ausführen möchten, bearbeiten Sie das Skript "SQLCHECK.SQL" und entfernen Sie das Argument "EXIT", bevor Sie den Befehl ausführen.

- (Oracle) Führen Sie OracleCheckr12UniqueIndexes.sql aus, das sich im Verzeichnis "\Migrate" des Installationsdatenträgers befindet.
- (SQL Server) Öffnen Sie ein Eingabeaufforderungsfenster, und führen Sie "SQLCHECK.SQL" wie folgt aus:

```
cd $NX_ROOT\samples\views\SQLServer
```

Geben Sie folgenden Befehl ein:

```
Sqlcmd -E -e < SQLServer\SQLCHECK.SQL
```

Hinweis: Nach der Aktualisierung auf CA SDM r12.9 finden Sie diese Dateien unter "\$NX_ROOT/samples/views/SQLServer" oder unter \$NX_ROOT/samples/views/Oracle auf dem Server.

Wichtig! Diese Skripte identifizieren Ihre doppelten Datensätze. Löschen Sie identifizierte doppelte Datensätze, bevor Sie mit der Migration fortfahren.

- Unter Windows können Sie ein Upgrade direkt von r11.2, r12.0, r12.1, r12.5, r12.6 und r12.7 durchführen.
- Wenn CA SDM unter UNIX oder Linux installiert ist, können Sie ein Upgrade von r12.5, r12.6 und r12.7 durchführen.
- Wenn Ihre Installation eine frühere Version des Produkts, wie z. B. CA SDM r11.2, r12.0 oder r12.1 auf nicht unterstützten UNIX- bzw. Linux-Betriebssystemen und -Datenbanken, enthält, müssen Sie ein Upgrade auf CA SDM r12.5 durchführen. Verschieben Sie CA SDM anschließend in eine unterstützte Betriebsumgebung und Datenbank, bevor Sie das Upgrade durchführen.
- Aktualisieren Sie Ihr System CA SDM r11.2 auf eine unterstützte Datenbank (SQL Server und Oracle).

Hinweis: Weitere Informationen über unterstützte Datenbanken finden Sie in den *Versionshinweisen*.

- Aktualisieren Sie von Unicenter Service Desk r11.0 auf CA SDM r11.2, bevor Sie Ihre Daten zu einer unterstützten Datenbank migrieren.
- Windows-Sonderzeichen, wie z. B. einen langen Bindestrich in CA SDM oder Knowledge Management auf einem anderen als einem Windows-System, werden in der Datenbank nicht richtig gespeichert.
- **Ingres:** Konvertieren Sie Ihre Daten bei Verwendung einer Ingres-Datenbank vor der Aktualisierung in Oracle oder SQL Server.

Hinweis: Informationen über die Konvertierung finden Sie in der Datenbankdokumentation.

- **Oracle:** Bei Oracle wird die Groß-/Kleinschreibung im Index für die Registrierung der Configuration Items nicht beachtet. Überprüfen Sie vor der Migration zu Oracle, ob SQLPlus und Oracle DB unter Verwendung des Hostnamens kommunizieren können. Überprüfen Sie, wenn die Kommunikation fehlschlägt, ob Oracle mit Loopbackadapter konfiguriert ist.

Hinweis: Wenn Sie eine Migration in eine Umgebung mit Doppelbyte-Zeichen und Oracle-Datenbank durchführen, erhöhen Sie das Höchstlimit für geöffnete Cursors auf mindestens 500. Weitere Informationen finden Sie in der Oracle-Dokumentation zu ORA-01000 ("maximum open cursor exceeded").

- **SQL Server:** Wenn Sie SQL Server verwenden und ein Upgrade auf die aktuelle Version von CA SDM durchführen, muss die Standarddatenbank für die konfigurierte Datenbank-Anwender-ID "CA MDB" sein. Wenn die Standarddatenbank nicht CA MDB ist, schlägt die Migrationskonsole fehl, und es wird die folgende Meldung angezeigt:
"The acctyp_v2 table does not exist on the MDB"
- **Tomcat:** (Für Unicenter Service Desk r11.0, r11.1 oder CA SDM r11.2) Wenn Sie Tomcat für externe Authentifizierung konfiguriert haben, konfigurieren Sie Tomcat manuell für externe Authentifizierung neu, nachdem Sie ein Upgrade auf die aktuelle Produktversion durchgeführt haben.
- **Tabellenaktualisierungen:** Beachten Sie, dass folgende Tabellen während der Migration aktualisiert werden:
 - **Statustabellen:** Diese Tabellen werden auch mit dem entsprechenden Status aktualisiert, wenn die gleichen Codewerte in Ihrer Datenbank nicht vorhanden sind. Beispielsweise wird *Cr_Status* durch den Code *AEUR* (Wartet auf Antwort des Endanwenders) aktualisiert.
 - **Funktionsbereiche:** Für jede Rolle wird bei der Migration automatisch eine Zeile für jeden Datensatz *usp_functional_access* hinzugefügt. Die Migration legt die Zugriffsebene auf die gleiche Ebene für jeden Funktionsbereich von CA SDM r12.0 und r12.1 fest, den die Tabelle *usp_role* enthält. Neue Funktionsbereiche werden mit Hilfe eines Referenzfeldes zugeordnet.
- **Fremdschlüssel:** Berücksichtigen Sie die folgenden Informationen:
 - Fremdschlüssel (SRELs), die auf Tabellen verweisen, in denen der Primärschlüssel eine UUID ist, werden von Integer auf UUID (oder 16 Byte) umgestellt.
Hinweis: Informationen zum Festlegen von SREL-Attributen mit Fremdschlüsselwerten finden Sie im *technischen CA SDM-Referenzhandbuch*.
 - Denken Sie daran, dass Sie vor der Aktualisierung Fremdschlüsseleinschränkungen erneut erstellen müssen, wenn Sie diese zum Massenladen von Daten im vorherigen CA SDM-System verworfen haben. Die Skripte, die die Bedingungen entfernen, befinden sich an den folgenden Speicherorten:
 - Oracle
\$NX_ROOT/samples/views/Oracle/OracleDropConstraints.sql
 - SQL Server
\$NX_ROOT/samples/views/SQLServer/SQLDropConstraints.sql**Hinweis:** Wenden Sie die verworfenen Beschränkungen erneut an, indem Sie das Skript *OracleAddConstraints.sql* oder *SQLServer/SQLAddConstraints.sql* ausführen. Diese Skripte befinden sich im gleichen Verzeichnis wie die entfernten Bedingungen und enthalten in den genannten Dateien entsprechende Anweisungen.

- **MDB:** Die MDB stellt ein konsistentes Datenbankschema für verschiedene IT-Managementdaten zur Verfügung. Während der Entwicklung der MDB wurden Datenelemente von Ihrer bisherigen CA SDM-Umgebung in dieses Schema integriert. Die Größe der Datenelemente kann zunehmen und somit auch die Größe der gesamten Datenbank.

Hinweis: Wenn standardmäßige Datenelemente über die für die MDB definierte Spaltenbreite hinausgehen, kann der Aktualisierungsprozess Daten in diesen Elementen kürzen. Entsprechende Meldungen weisen Sie gegebenenfalls während der Aktualisierung auf das Abschneiden von Daten hin.

- **Verteiltes Setup:** Wir empfehlen, dass Sie ein Upgrade Ihrer Server abhängig von Ihrer CA SDM-Konfiguration in der folgenden Reihenfolge durchführen:
 - **Konventionell**
 - Primärserver
 - (Optional) Ein oder mehrere sekundäre Server
 - **Erweiterte Verfügbarkeit**
 - Hintergrundserver
 - Ein oder mehrere Standby-Server
 - Ein oder mehrere Anwendungsserver
 - **Remote-Datenbank-Setup:** Berücksichtigen Sie die folgenden Informationen:

Wir empfehlen, den Datenbankserver vor der Aktualisierung des Primärservers mit einer neuen MDB zu aktualisieren. Wenn es sich um einen Remote-Datenbankserver handelt, führen Sie zuerst die CA MDB-Installation auf dem Datenbankserver aus und aktualisieren diese anschließend.

 - Wenn Sie eine SQL Server-MDB-Datenbank verwenden, muss "sqlcmd" auf dem Client-Computer installiert sein, bevor Sie eine Verbindung zur Remote-MDB herstellen.

Hinweise zu Knowledge Management

Bevor Sie auf CA SDM r12.9 aktualisieren, sollten Sie die folgenden Knowledge Management-Informationen beachten:

- Kunden, die ein Upgrade von einer früheren Version von CA SDM durchführen, in der die Such-Engine "FAST ESP" verwendet wurde, *müssen* in die EBR-Such-Engine geändert werden. Die FAST ESP-Lizenz läuft im Mai 2013 ab. Um zur Such-Engine "EBR" zu wechseln, klicken Sie auf "Optionsmanager", "Such-Engine", und bearbeiten Sie "ebr_version", um die Such-Engine "KT" anzugeben.
- So führen Sie ein [Upgrade für Knowledge Management von CA SDM r11.2 durch](#) (siehe Seite 78).
- So führen Sie ein [Upgrade für Knowledge Management von CA SDM r12.x durch](#) (siehe Seite 81).

DocType-Validierung

In früheren Versionen von CA SDM wurde folgender DocType für HTML verwendet, der aus HTML-Formularen in der Eigenschaft "HtmlDocType" von "web.cfg" generiert wurde:

```
HtmlDocType <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
```

Die Eigenschaft "HtmlDocType" von "web.cfg" wird für CA SDM r12.9 folgendermaßen angezeigt:

```
HtmlDocType <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Frameset//EN"
"http://www.w3.org/TR/html4/frameset.dtd">
```

Diese Zeile beginnt normalerweise auf der ersten Liste einer Seite.

Hinweis: Nachdem Sie ein Upgrade auf CA SDM r12.9 durchgeführt haben, überprüfen Sie, ob der Eigenschaftswert "HtmlDocType" in Ihren angepassten Formularen geändert wurde. Sie können eine HTML-Datei aus dem Verzeichnis "\$NX_ROOT/bopcfg/www/wwwroot/html" mit einem Texteditor öffnen und den Wert "DocType" überprüfen.

Übernehmen von Anpassungen

Lesen Sie folgende Informationen über Ihr angepasstes Produkt durch, bevor Sie ein Upgrade auf die Version CA SDM r12.9 durchführen:

Hinweis: Wenn Sie die Migrationskonsole schließen, bevor die Aktualisierung abgeschlossen ist, dann wird der Prozess weiter im Hintergrund ausgeführt.

- **Anwenderspezifische Berichte:** Wenn Sie anhand von anwenderspezifischen Berichten auf Datenbanktabellen von früheren Versionen zugreifen, die in umbenannte Tabellen übertragen wurden, werden die Spaltennamen in r12.9 geändert.

Hinweis: Weitere Informationen über Tabellen finden Sie im technischen *CA SDM-Referenzhandbuch*.

- **Angepasste Formulare:** Bei einem Upgrade auf CA SDM r12.9 werden Anpassungen der Formulare der vorherigen CA SDM-Version beibehalten. Allerdings können Sie die CA SDM r12.9-Funktionalität auf den angepassten Formularen nicht anzeigen, nachdem Sie ein Upgrade durchgeführt haben.

- **Angepasste Admin-Struktur:** Wenn Sie die Admin-Struktur in Unicenter Service Desk r11.0 angepasst haben, werden diese Änderungen aufgrund von Änderungen an der Architektur nicht aktualisiert, um die rollenbasierte Anwenderschnittstelle zu unterstützen. Zu solchen Anpassungen an der Administrations-Baumstruktur zählen die Ergänzung von neuen Knoten, das Umbenennen vorhandener Knoten, die Änderung von Zugriffstypen und andere Datenveränderungen. Um die Anpassungen zu verwenden, gehen Sie folgendermaßen vor:
 1. Prüfen Sie vor der Aktualisierung die Admin-Struktur von Unicenter Service Desk r11.0, und notieren Sie sich sämtliche Anpassungen, die Sie nach der Aktualisierung verwenden möchten.
 2. Identifizieren Sie nach Abschluss der Anpassung die Rollen mit einer Admin-Struktur.
 3. Wenden Sie die Anpassungen auf die gewünschten rollenbasierten CA SDM r12.9-Admin-Strukturen an.
 4. Vergewissern Sie sich durch Tests, dass die gewünschte Funktionalität erhalten blieb.
- **Angepasste Formularschaltflächen:** Nach der Aktualisierung wird für Schaltflächen in angepassten Formularen unter "*site/mods/html*", bei denen der Codeteil "*msgtxt(n)*" nicht in Anführungsstriche gesetzt war, anstelle des Schaltflächennamens eine Fehlermeldung angezeigt.

Setzen Sie zum Beispiel im Formular *detail_cr.html* den Wert "*msgtxt(441)*" in Anführungszeichen, um den richtigen Schaltflächennamen anzuzeigen:

```
ImgBtnCreate("btnchg", "msgtext(441)", "detailSave('NEW_CHANGE')",  
true, 0, msgtext(440)); // Change erstellen und speichern
```
- **Übernehmen von Anpassungen:** Wenn Sie die Funktionen von CA SDM r12.9 benötigen und Ihre Anpassungen aus einer früheren Version übernehmen möchten, müssen Sie die Anpassungen an einem Basisformular von CA SDM r12.9, das über die r12.9-Funktionen verfügt, wiederholen.

Hinweis: Wenn Sie die Berichte "*acctypedtl.rpt*" und "*acctypesum.rpt*" angepasst haben, sind die Rückgabedaten in CA SDM r12.9 veraltet.
- **Benachrichtigungsregeln:** Wenn Sie die Standardaktivitätsbenachrichtigungen "Kontakt", "Objektkontakte" und "Kontakttypen" von der vorherigen CA SDM-Installation entfernt haben und diese Funktion übernehmen möchten, müssen Sie sich die Standardkontakte, die Sie vor der Migration entfernt haben, notieren. Nach der Aktualisierung auf die neue Version sollten Sie die Standardbenachrichtigungskontakte wieder entfernen.

- **Rollenbasierte Funktionen:** Die Aktualisierung kann zu Problemen mit rollenbasierten Funktionen führen. Lesen Sie sich folgende Informationen sorgfältig durch:
 - Wenn Sie eines der folgenden Formulare angepasst haben, werden diese von Web Screen Painter in CA SDM r12.9 als schreibgeschützt betrachtet. Sie sind jedoch auch in einer "xxx_site.html"-Version vorhanden, in der Sie anwenderspezifischen Code verwenden können:
 - ahdtop.html
 - menu_frames.html
 - reports.html
 - std_body.html
 - std_footer.html
 - std_head.html
 - styles.html
 - msg_cat.js
 - menu_frames_role.html
- **Angepasste HTML Dateien:** Beachten Sie folgende Informationen:
 - Alle angepassten HTML-Dateien behalten ihre standardmäßigen Einstellungen der Menüleiste bei, nachdem Sie ein Upgrade durchgeführt haben. Ein Pop-up-Fenster übernimmt die Menüleiste von der Registerkarte "Hauptseite" aufgrund einer rollenbasierten Benutzeroberfläche. Angepasste HTML-Dateien sind auf den angepassten Formularen der vorherigen Version nicht verfügbar, nachdem ein Upgrade durchgeführt wurde.
 - CA SDM r12.9 verwendet keine angepassten HTML-Dateien aus den vorherigen Versionen. Das Migrationsskript führt das Perl-Skript "\$NX_ROOT/bin/migrate_to_r12_9_web_check.pl" aus, das die Dateien mit der Erweiterung "incompatible_for_r2_9" anhängt. Öffnen Sie nach der Migration "\$NX_ROOT/site/web_check_files.txt" mit einem Texteditor, um die Liste der inkompatiblen Formulare für r12.9 anzuzeigen.
 - Wenn Sie die Datei "list_dblocks.html" in einer früheren Version von CA SDM angepasst haben, dann wird dieses Formular in CA SDM r12.9 nicht funktionieren. Wenn Sie die Admin-Struktur angepasst haben, um "list_dblocks.html" in anderen Teilen der Struktur anzuzeigen, dann wird die Anpassung nach der Migration nicht funktionieren. Ändern Sie das Formular manuell, um die neue URL und das Formular zu verwenden. Um diese Änderung abzuschließen, klicken Sie auf "Sicherheits- und Rollenmanagement", "Menüstrukturressourcen", und öffnen Sie "Aktuelle Sperrungen". Aktualisieren Sie die Ressourcen mit der folgenden CA SDM r12.9-Zeichenfolge:
`OP=SEARCH+FACTORY=record_lock+QBE.NN.lock_time=NULL`

- **Fremdschlüssel:** Wenn der Aktualisierungsprozess beim Versuch, Fremdschlüssel zurückzusetzen, Probleme mit der referenziellen Integrität erkennt, werden entsprechende Fehler in der Datei "migration.log" angezeigt. Der zugehörige Fremdschlüssel wird auf eine vordefinierte gültige Referenz gesetzt.
- **Server- und Web-Director-Konfiguration:** Wenn Ihre vorherige Installation konfiguriert wurde, um zusätzliche Server oder Web-Directors zu verwenden, dann müssen Sie zunächst die Konfiguration für die spezifischen Server erstellen und das CA SDM-Server-Konfigurationsprogramm (pdm_configure) ausführen. Weitere Informationen über das Erstellen der Konfigurationen finden Sie im Administrationshandbuch.
- **CA-Support-Automatisierung-Bereiche:** Wenn Sie Bereiche zu Mandanten migrieren möchten, müssen Sie diese Daten vor der Konfiguration und Aktivierung von Support-Automatisierung in CA SDM r12.9 konvertieren.

Umbenennen der angepassten HTML-Formulare

Wenn Sie HTML-Formulare in einer früheren Version von CA SDM angepasst haben, führen Sie ein Skript aus, um die Formulare umzubenennen, bevor Sie ein Upgrade auf CA SDM r12.9 durchführen. Sie führen dieses Skript auf allen CA SDM-Servern aus. Das Skript "migrate_to_r12_9_web_check.pl" benennt alle anwenderspezifischen Webformulare, Stylesheets, Java-Skripts, Images und Makros im site/mods-Verzeichnis um. Das Umbenennen dieser Dateien hilft Ihnen beim Identifizieren Ihrer angepassten Formulare.

Gehen Sie wie folgt vor:

1. Führen Sie `pdm_perl $NX_ROOT/bin/migrate_to_r12_9_web_check.pl` in einer Eingabeaufforderung aus.

Das Skript hängt die angepassten Formulare mit der Erweiterung *incompatible_for_r12_9* an.

2. Öffnen Sie "`$NX_ROOT/bin/migrate_to_r12_9_web_check.pl`" mit einem Texteditor.

Eine Liste der inkompatiblen Formulare für r12.9 wird angezeigt.

Hinweis: Anders als in früheren Versionen von CA SDM stellt das Skript keine Dateien aus Sicherungsordnern im legacy- oder site/mods-Verzeichnis wieder her.

Weitere Informationen:

[Übernehmen von Anpassungen](#) (siehe Seite 33)

Hinweise zur Benutzeroberflächen-Migration

Bevor Sie ein Upgrade auf CA SDM r12.9 durchführen, berücksichtigen Sie folgende Informationen zur Migration der Benutzeroberfläche:

- Bei der Migration werden Formulare automatisch gesichert. Wenn Sie in CA SDM r11.2, r12.0, r12.1 oder r12.5 benutzerdefinierte HTML-Formulare verwendet haben, *müssen* Sie diese nach dem Upgrade auf CA SDM r12.9 erneut anpassen.
- Nachdem Sie ein Upgrade durchgeführt haben, ändern Sie alle angepassten HTML-Formulare, die zuvor Steuerungen für Notizbücher enthielten, um die neuen Webmakros einzuschließen und korrekte Registerkartengruppennamen anzugeben. Ändern Sie in WSP die Anweisung <PDM_NOTEBOOK> in <PDM_MACRO name=startNotebook> und die Anweisung <PDM_TAB> in <PDM_MACRO name=TAB> um.

Weitere Informationen:

[Ändern einer Datenrasterliste auf einem Listenformular](#) (siehe Seite 427)

[Ändern von Notizbüchern auf einem Detailformular](#) (siehe Seite 429)

Weboption "copy_inactive"

Neue CA SDM r12.9-Installationen installieren die Weboption "copy_inactive" nicht im Optionsmanager, sodass Verknüpfungen zu inaktiven Objekten nicht kopiert werden. Wenn Sie ein Upgrade von CA SDM r12.5 oder r12.6 durchführen, werden Verknüpfungen zu inaktiven Objekten kopiert, da die Migration die Option installiert.

Beachten Sie folgende Informationen, wenn Sie die Option "copy_inactive" nicht installieren:

- CA SDM kopiert keine SRELs, die auf inaktive Objekte verweisen, außer wenn SREL erforderlich ist.

Zum Beispiel hat die Organisation "org1" eine inaktive Lokation. Wenn Sie "org1" kopieren, hat die neue Organisation keine Lokation. Wenn jedoch SREL erforderlich ist, dann ignoriert CA SDM diese Regel und kopiert die Lokation. Zum Beispiel ignoriert CA SDM die Regel, und Sie können ein CI mit einer inaktiven Klasse kopieren.
- CA SDM kopiert keine LREL-Beziehungen (many-to-many) zu inaktiven Objekten.

Zum Beispiel hat das CI mit dem Namen "CITest1" eine Beziehung zur inaktiven Organisation "org2". Wenn Sie "CITest1" kopieren, wird "org2" nicht mit dem neuen CI verbunden.

Wichtig! Diese Regeln gelten auch, wenn Sie ein Ticket kopieren, auch wenn Sie ein Ticket aus einer Vorlage erstellen. Unabhängig davon, ob Sie "copy_inactive" installiert haben, die Ausnahme für die Regel gilt für inaktive Bereiche und Kategorien, die nicht von vorhandenen Tickets kopiert oder aus Vorlagen aufgefüllt wurden.

Hinweise zur LREL-Migration

Eine *Listenbeziehung* ("LREL") stellt eine Zuordnung zwischen zwei Objekten dar. Eine "LREL" hat eine linksseitige ("lhs") und rechtsseitige ("rhs") Beziehung. Jede Seite der Beziehung ist ein Attribut des majic-Objekts, das die Datenbeziehung enthält.

In Vorgängerversionen des Produkts beschreiben .maj-LREL-Anweisungen und -Objekte n:m-Beziehungen zwischen DBMS-Daten. Von n:m-Beziehungen werden keine LREL-majic-Anweisungen mehr verwendet. Statt dessen werden beide Seiten der Beziehung in einzelnen Tabellenspeichern gespeichert. Objekte greifen auf die Beziehung mit einer standardmäßigen BREL-Anweisung zu. Zum Beispiel können Sie die Beziehung zwischen Changes und CIs in der neuen Tabelle "usp_lrel_asset_chgnr" und im entsprechenden "lrel_asset_chgnr"-Objekt überprüfen.

Aufgrund der LREL-Änderungen ist es nicht mehr erforderlich, Attributnamen in der Datenbank zu speichern. Die zwei Seiten der Beziehung sind Fremdschlüssel-Einzelbeziehungen (SREL), die sich leicht verknüpfen und indizieren lassen. Bei Bedarf kann die Beziehung zusätzliche relationale Attribute enthalten.

Während der Aktualisierung werden die folgenden Aktivitäten ausgeführt, während die LREL-Tabellendaten nach r12.9 migriert werden:

- Das System migriert Tabellen und Objekte mit LREL-Beziehungen automatisch in r12.9-Tabellen und Objekte.
- Neue Tabellen werden vom System im Format "*usp_lrel_lhsName_rhsName*" benannt.

Beispiel: Die Tabelle "*usp_lrel_asset_chgnr*" hat eine linksseitige Beziehung zu Assets und eine rechtsseitige Beziehung zu Changes.
- Das System benennt die entsprechenden Objekte unter Verwendung von "*lrel_lhsName_rhsName*".

Beispiel: Das Objekt "*lrel_asset_chgnr*" entspricht der Tabelle "*usp_lrel_asset_chgnr*".
- Aufgrund einer Datenbankbeschränkung werden einige Namen abgekürzt.
- Die Daten werden aus den alten Tabellen in die r12.9-Tabellen migriert, und der ganze CA SDM-Code wird geändert, um diese Tabellen zu verwenden.
- Das System verwendet die alten LREL-Datenbanktabellen wie "*bmlrel*" nicht mehr. Zu Verweiszwecken behalten die alten Tabellen jedoch die Daten bei.
- Eine rückwärtsgerichtetes Beziehungsattribut ("BREL") für das neue Objekt ersetzt das ursprüngliche LREL-Attribut in jeder zugehörigen majic-Objektdefinition.
- Wenn Sie eine unterstützte API wie die Webservice-Methode "*CreateLrelRelationship()*" verwenden, verhält sich der Code wie erwartet.
- Wenn Sie benutzerdefinierte LREL-Stilbeziehungen hinzugefügt haben, werden diese von CA SDM in r12.9-Tabellen migriert.
- Alle standortdefinierten Codes oder Berichte, die direkt auf die alten LREL-Tabellen zugreifen, arbeiten mit den alten Daten, weil das System diese Tabellen nicht mehr verwendet. Es wird empfohlen, den Code zu aktualisieren, damit die r12.9-Tabellen verwendet und der Code und die Berichte korrekt ausgeführt werden.

Wichtig! Wenn der Code direkt auf veraltete LREL-Objekte oder -Tabellen zugreift, gibt er nach der Migration Fehler zurück. Es wird empfohlen, den Code vor der Migration zu aktualisieren. Beispiel: Wenn Ihr Code majic-Anweisungen zum Festlegen der LREL-Beziehungen verwendet, sollten Sie die "*createLrelRelationships()*"-Methode verwenden, anstatt direkt eine Tabelle zu füllen.

Hinweis: Es wird empfohlen, standortdefinierten Code und Berichte zu überprüfen, die direkt auf die Datenbank zugreifen oder sich an die veralteten LREL-majic-Objekte wie "lrel2" richten, um sicherzustellen, dass sie korrekt funktionieren. Sie können den Code anhand einer unterstützten Schnittfläche wie Webservices aktualisieren. Aktualisieren Sie auch die erforderlichen Tabellennamen. Für Berichte können Sie auch die Abfragen mit den neuen DBMS-Tabellenverweisen aktualisieren.

Hinweise zum Statusübergang

Beachten Sie folgende Informationen, wenn Sie Statusübergänge verwenden möchten, nachdem Sie ein Upgrade von CA SDM r11.2, r12.1 und r12.1 auf CA SDM r12.9 durchgeführt haben:

- Statusübergänge sind inaktiv, wenn Sie auf r12.9 aktualisieren.

Hinweis: Alle angepassten Statuscodebeschreibungen auf Ticket-Formularen werden beim Aktualisierungsprozess beibehalten.

- Die Option "*Status_Policy_Violations*" wird installiert und ist nach der Aktualisierung automatisch für standardmäßiges Warnen festgelegt. Diese Einstellung lässt undefinierte Übergänge zu, protokolliert aber eine Warnung.
- Wenn Sie die Option für das Zulassen von undefinierten Übergängen festlegen, werden diese nicht protokolliert.

Hinweis: Weitere Informationen zur Option "*Status_Policy_Violations*" finden Sie in der *Online-Hilfe*.

Aktualisieren der E-Mail

CA SDM ersetzt die E-Mail-Optionen für eingehende E-Mails im Optionsmanager durch ein Postfach (Tabelle "*usp_mailbox*"), das die entsprechenden Optionen bereitstellt. Die E-Mail-Optionen für ausgehende E-Mails sind im Optionsmanager noch vorhanden. Bei der Aktualisierung verwendet CA SDM die vorhandenen E-Mail-Einstellungen zum Konfigurieren des Postfachs anstatt der Standard-Postfacheinstellungen von CA SDM r12.9. Mit Ausnahme von "EMAIL_ATTACHMENT_DIR" (diese Option wird nicht mehr benötigt) ist jede E-Mail-Option einer Option in der Tabelle "*usp_mailbox*" zugeordnet. Jede nicht festgelegte Option ist in der Tabelle auf Null gesetzt.

Hinweis: Informationen zum Aktivieren des Standardpostfachs und zur Verwendung der Postfachoptionen finden Sie im *Administrationshandbuch* und in der *Online-Hilfe*.

Die folgende Tabelle listet Optionen auf, die aus den E-Mail-Optionen entfernt wurden und die in der Tabelle "*usp_mailbox*" enthalten sind. Daneben gibt sie deren Beschriftung auf der Postfach-Detailseite an.

<E-Mail-Option	"usp_mailbox"-Option	Beschriftung in "Standardpostfach-Detail"
EMAIL_ALLOW_ANONYMOUS	allow_anonymous	AllowAnonymous

<E-Mail-Option	"usp_mailbox"-Option	Beschriftung in "Standardpostfach-Detail"
EMAIL_ATTACHMENT_DIR	N. rel.:	N. rel.: Hinweis: Da "EMAIL_ATTACHMENT_DIR" veraltet ist, müssen Sie das Anhangs-Repository manuell auswählen, falls diese Option festgelegt und "EMAIL_MAIL_ATTACHMENT_REPOSITORY" nicht festgelegt wurde.
EMAIL_ATTACHMENT_REPOSITORY	attmnt_repository	AttachmentRepository
EMAIL_FORCE_ATTACHMENT_SPLITOUT	split_out_attachment	ForceAttachmentSplitout
EMAIL_IS_ATTACHMENT	attach_email	AttachEntireEmail
EMAIL_SAVE_UNKNOWN_EMAILS	save_unknown_emails	SaveUnknownEmails
MAIL_EATER_IMAP_HOST_PORT	host_port	Port-Überschreibung
MAILEATER_CHECK_MAIL_INTERVAL	check_interval	CheckInterval
MAILEATER_HOST	host_name	Hostname
MAILEATER_LOGIN_PASSWORD	password	Kennwort
MAILEATER_LOGIN_USERID	userid	Benutzer-ID
MAILEATER_POP3_HOST_PORT	host_port	Port-Überschreibung
MAILEATER_SECURITY_LEVEL	security_lvl	Sicherheitsebene
MAILEATER_SERVER_TYPE	email_type	EmailType

Wichtig! Die Einstellung für das Anhangsverzeichnis ist in r12.9 veraltet. Daher *müssen* Sie ein Anhangs-Repository angeben, bevor Sie mit dem Abfragen der Postfächer fortfahren.

Hinweise zu Maileater.cfg

Informationen, die früher in der Datei "*maileater.cfg*" enthalten waren, sind der Tabelle "*usp_mailbox_rule*" in r12.9 zugeordnet. Berücksichtigen Sie die folgenden Informationen zur Zuordnung von "*maileater.cfg*" zu "*usp_mailbox_rule*":

- Das "-i" am Zeilenanfang gibt an, dass die Groß- und Kleinschreibung nicht berücksichtigt wird und steht für eine Zuordnung zum Feld "filter_ignore_case".

- Der Suchfilter "Subject: *..." gab früher einen regulären Ausdruck an, nach dem gefiltert wurde. Das Wort "Subject:" wurde entfernt und durch ein "^"-Symbol ersetzt, und der restliche Wert steht für eine Zuordnung zum Feld "*filter_string*". "Filter_type" wird auf den Typ "SubjectContains" festgelegt.
- "TEXT_API xxx" gibt das Objekt an, das für die Regel verarbeitet wird. Die Zeichenfolge "TEXT_API" wurde entfernt, und der Rest steht für eine Zuordnung zum Feld "*action_object*". Das Feld "*action_operation*" ist auf "Objekt erstellen/aktualisieren" festgelegt.
- Die Antwort an den Benutzer enthält in der Regel "PDM_MAIL...". Wenn Sie "PDM_MAIL" festgelegt haben, setzen Sie "reply_method" auf "1800" oder belassen Sie den Wert bei Null.
- Wenn der "-s"-Parameter festgelegt wird, entfernen Sie das Feld "subject" aus dem Text und legen Sie "*reply_subject*" mit diesem Wert fest.
- Die Funktionalität behält die Reihenfolge der Einträge bei. Für jede gültige Zeile wird eine Sequenznummer festgelegt, beginnend bei 100 und um 100 erhöht.

Die anderen Felder in "*usp_mailbox_rule*" werden folgendermaßen festgelegt:

Feld	Wert
mailbox	Standard
action_write_to_log	0
action_log_prefix	null
delete_flag	0
description	Von der Datei "pdm_maileater.cfg" migriert
reply_failure_html	<leer, um Standardaktion zu übernehmen>
reply_failure_text	<leer, um Standardaktion zu übernehmen>
reply_success_html	<leer, um Standardaktion zu übernehmen>
reply_success_text	<leer, um Standardaktion zu übernehmen>
text_api_defaults	null
text_api_ignore_incoming	null
action_subject_handling	null
last_mod_dt	null
last_mod_by	null
inclusion_list	"*"
email_address_per_hour	-1
exclusion_list	null

Feld	Wert
log_policy_violation	1

Funktionsweise der Migrationskonsole

Die Migrationskonsole führt Sie durch die Migrations- und Aktualisierungsprozesse für CA SDM. Die Konsole entdeckt automatisch eine existierende Installation wie CA SDM r11.2. Sie können die Aktualisierung vom Installationsdatenträger aus oder [manuell](#) (siehe Seite 44) starten.

Hinweis: Wenn Ihre angepassten Webformulare nicht mit CA SDM r12.9 kompatibel sind, zeigt die Migrationskonsole eine Meldung an, die darauf hinweist, dass diese Formulare in das Verzeichnis "site/mods/www/html" verschoben wurden. Weitere Informationen zu diesen Formularen finden Sie in der Datei "Web_Forms_Changed.txt" im Verzeichnis "site/mods/".

Wichtig! Die CA SDM-Migrationskonsole wandelt Bereiche nicht in Mandanten um. Wenn Sie Support-Automatisierung in einer Umgebung für mehrere Mandanten konfigurieren möchten, *müssen Sie* Bereiche von CA Support-Automatisierung r6.0 SR1 eFix5 [getrennt](#) (siehe Seite 51) zu CA SDM r12.9-Mandanten migrieren, bevor Sie Support-Automatisierung in CA SDM aktivieren.

Die Konsole führt die folgenden Aufgaben durch:

1. Es wird sichergestellt, dass Ihr Produkt CA SDM r11.2, r12.0, r12.1, r12.5, r12.6 oder r12.7 ist.
2. Konvertiert Kennwörter in ein FIPS 140-2-kompatibles Format.
3. Wendet MDB-Aktualisierungen an.
Wichtig! Die Version der Remote-MDB muss mindestens CA MDB r1.5 sein, ansonsten schlägt die Migration fehl.
4. Migriert LREL-Daten.
5. Konvertiert angepasste Dateien in UTF-8.

6. Konvertiert Zugriffstyp-Datensätze in Rollen- und Zugriffstyp-Datensätze von CA SDM r12.9.
7. Migriert und aktualisiert Anwenderanfragen zum Scoreboard für rollenbasierte Operationen.
8. Migriert und aktualisiert vorhandene Benachrichtigungen zur Verwendung von Benachrichtigungsregeln und Benachrichtigungsvorlagen.

Hinweis: Wenn Sie "Aktualisierung durchführen" auswählen und auf "Installieren" klicken, können Sie die Migration und die Aktualisierung nicht mehr rückgängig machen.
Hinweis: Wenn Sie die Migrationskonsole schließen, bevor die Aktualisierung abgeschlossen ist, wird der Prozess weiter im Hintergrund ausgeführt.

Weitere Informationen:

[So installieren Sie CA MDB](#) (siehe Seite 156)

[Produktkonfiguration](#) (siehe Seite 243)

[Support-Automatisierung-Datenmigration](#) (siehe Seite 50)

[Aktualisieren von CA CMDB von einer Vorgängerversion](#) (siehe Seite 45)

Protokolldatei der Migration

Sollten während der Migration oder Aktualisierung Probleme auftreten, finden Sie den gesamten Prozess im Migrationsprotokoll. Dieses Protokoll befindet sich im folgenden Verzeichnis:

`$NX_ROOT/log/pdm_migrationr12_9.log`

Manuelles Starten des Migrationsprozesses

Die Aktualisierung können Sie mit folgendem Befehl manuell starten:

■ **Windows**

`$NX_ROOT\bin\migrate_to_r12_9.vbs`

■ **Linux/UNIX**

`$NX_ROOT\bin\migrate_to_r12_9.sh`

Hinweis: Wenn die Migration fehlschlägt und einen Schemavalidierungsfehler anzeigt, führen Sie die Aktualisierung erneut mit dem zuvor genannten Befehl aus.

Aktualisieren von CA CMDB von einer Vorgängerversion

Sie können CA CMDB auf CA SDM r12.9 von einer Vorgängerversion wie r11.2, r12.0 und r12.1 aktualisieren. Wenn Sie die Migration abbrechen, *müssen* Sie das Skript ausführen, um die Migrationskonsole neu zu starten. Das Skript befindet sich im `"/bin"`-Verzeichnis des Produkts, z. B. `"C:/CMDB/bin"`. Wenn Sie z. B. die Migration unter Linux oder Unix abbrechen, führen Sie das Skript `"migration_to_r12.9.sh"` aus.

Hinweis: Wenn Sie von einer eigenständigen CA CMDB-Version aktualisieren, können Sie weiterhin die eigenständigen CA CMDB-Funktionen in CA SDM r12.9 verwenden. Wenn Sie von einer Umgebung mit CA CMDB und CA SDM oder von einer CA SDM-Umgebung ohne CA CMDB aktualisieren, wird bei der Aktualisierung die Vollversion von CA SDM r12.9 installiert.

CA CMDB wird folgendermaßen aktualisiert:

1. Starten Sie das CA SDM-Installationsprogramm vom Installationsdatenträger aus.

Das Installationsprogramm erkennt die Produktversion, z. B. CA CMDB r11.2.

Hinweis: Wenn Sie von einer kombinierten CA SDM- und CA CMDB-Installation aktualisieren, zeigt das Installationsprogramm die erkannte Umgebung als CA CMDB-Version anstelle einer CA SDM-Version an.

2. Klicken Sie auf "Weiter".

Eine Installationsmeldung weist darauf hin, dass CA SDM und Knowledge Management erst nach Abschluss der Migration verwendet werden dürfen.

3. Klicken Sie auf "Weiter".

Wenn Visualizer erkannt wird, werden Sie aufgefordert, das Programm manuell zu deinstallieren.

Wichtig! Nachdem Sie Visualizer deinstalliert haben, *müssen* Sie den Rechner und das CA SDM-Installationsprogramm neu starten.

4. Akzeptieren Sie die Bedingungen der Lizenzvereinbarung, und klicken Sie auf "Installieren".

Während der Installation werden Ihre Daten gesichert und Services geschlossen.

Hinweis: Die CA CMDB-Aktualisierung sichert *nicht* die Datenbank.

Nachdem die Installation abgeschlossen ist, wird auf der Migrationskonsole eine Warnung angezeigt, die Sie auffordert, Ihre Migrationsdokumentation zu überprüfen.

5. Klicken Sie auf "Migrieren".

Die Migrationskonsole lädt Systemdaten, aktualisiert Ihre MDB und führt Services zurück.

Hinweis: Während des Prozesses kann das Migrationsprotokoll aktiv angezeigt werden.

6. Die Konsole überprüft Tabellen, verarbeitet Daten, sichert Daten und aktualisiert Ihr Produkt auf r12.9.

Die CA SDM-Konfiguration wird angezeigt.

7. (Optional) Konfigurieren Sie nur CMDB.

Wenn Sie von einer eigenständigen CA CMDB-Umgebung aktualisieren, wird im Formular "Allgemeine Einstellungen" das Kontrollkästchen "Nur CMDB konfigurieren" angezeigt.

Wichtig! Wenn Sie von einer CA CMDB-Standalone-Version nach CA SDM migrieren, erscheint während der Konfiguration ein Kontrollkästchen mit der Option "Nur CMDB konfigurieren". Wenn Sie das Kontrollkästchen "Nur CMDB konfigurieren" deaktivieren und Sie auf "Weiter" klicken, können Sie CA CMDB nicht noch einmal konfigurieren. Auch wenn Sie auf "Zurück" klicken, ist das Kontrollkästchen "Nur CMDB konfigurieren" nicht mehr verfügbar. Eine Meldung im Konfigurationsdialog warnt Sie davor. Wenn Sie die Konfiguration vor der Fertigstellung abbrechen und sie dann wiederholen, ist das Kontrollkästchen "Nur CMDB konfigurieren" verfügbar.

Über das Kontrollkästchen "Nur CMDB konfigurieren" steuern Sie den Wert der CA SDM-Umgebungsvariable NX_CMDB. Die Umgebungsvariable kontrolliert, ob die Support-Automatisierung-Funktion konfiguriert wird. Wenn das Kontrollkästchen deaktiviert ist, kann Support-Automatisierung konfiguriert werden, andernfalls ist eine Konfiguration nicht möglich. Die Umgebungsvariable wirkt sich auf das Verhalten einiger Webformulare aus.

Wenn Sie von einer eigenständigen CA CMDB-Umgebung aktualisieren und eigenständige CA CMDB-Funktionen in CA SDM r12.9 verwenden möchten, können Sie Support-Automatisierung nicht konfigurieren.

8. Schließen Sie die Konfiguration entsprechend den Anforderungen in Ihrer Umgebung ab.

Migration zu CA SDM r12.9 unter einem Linux/UNIX-64-Bit-Betriebssystem

Hinweis: Diese Informationen beziehen sich lediglich auf 64-Bit-Versionen von Linux/UNIX.

Gehen Sie wie folgt vor:

1. Installieren Sie den 32-Bit-Oracle-Client.
2. Stellen Sie eine Verbindung mit Oracle_Server_SID her.
3. Erstellen Sie einen lokalen Netzdienstnamen, und testen Sie die Verbindung.
4. Export der TWO_TASK-Variable.
5. Bearbeiten Sie, wie im folgenden Beispiel dargestellt, die Variablen ORACLE_HOME und PATH, um oracle_client zum Stammverzeichnis zu machen, und entfernen Sie das Serverstammverzeichnis:

```
ORACLE_HOME= /opt/app/product/11.2.0/client_1  
PATH= /opt/app/product/11.2.0/client_1/bin
```

Hinweis: Aktualisieren Sie die Variable "ORACLE_HOME" in der Datei "NX.env", wie im vorherigen Beispiel angezeigt.

6. Legen Sie, wie im folgenden Beispiel dargestellt, LD_LIBRARY_PATH und LIBPATH auf "client-lib" (32-Bit-Binärdateien) fest:

```
LD_LIBRARY_PATH=/opt/app/product/11.2.0/client_1/lib
```

7. Führen Sie, wie im folgenden Beispiel dargestellt, pdm_configure aus, wobei ORACLE_HOME auf "client_home" festgelegt ist.

```
C:\app\Administrator\product\11.2.0\client_1\
```

8. Installieren Sie CA SDM r12.9.

Migration zu CA SDM r12.9 unter einem Windows-64-Bit-Betriebssystem

Hinweis: Diese Informationen beziehen sich lediglich auf 64-Bit-Versionen von Windows.

Führen Sie folgende Schritte aus, um Daten nach CA SDM r12.9 zu migrieren:

1. Installieren Sie den 32-Bit-Oracle-Client.
2. Stellen Sie eine Verbindung mit Oracle_Server_SID her.
3. Erstellen Sie einen Local Net-Servicenamen, und testen Sie die Verbindung.
4. Bearbeiten Sie, wie im folgenden Beispiel dargestellt, die Variable PATH, um oracle_client zum Stammverzeichnis zu machen, und entfernen sie das Serverstammverzeichnis aus PATH:
`C:\app\Administrator\product\11.2.0\client_1\bin`
5. Führen Sie, wie im folgenden Beispiel dargestellt, pdm_configure aus, wobei ORACLE_HOME auf "client_home" festgelegt ist.
`C:\app\Administrator\product\11.2.0\client_1\`
6. Installieren Sie CA SDM r12.9.

Beispiel: Migrieren von einer nicht unterstützten Windows-Umgebung

In diesem Beispiel ist CA SDM r11.2 unter Windows 2003 (32-Bit) mit SQL Server 2005 installiert. Sie möchten eine Migration Ihrer Daten und ein Upgrade auf CA SDM r12.9 unter einem Windows 2008 64-Bit-System mit SQL Server 2008 erfolgreich durchführen.

Gehen Sie wie folgt vor:

1. Migrieren Sie CA SDM r12.9 auf dem gleichen Computer.
2. Führen Sie ein Upgrade von SQL Server 2005 auf 2008 durch.
3. Sichern Sie die MDB-Datenbank.
4. Installieren Sie CA SDM r12.9 unter Windows 2008 (64-Bit).
5. Laden Sie MDB-Sicherung, die Sie unter Schritt 3 durchgeführt haben.
6. Verschieben Sie den Ordner "\$NX_ROOT\site\mod" aus dem älteren Computer in den neuen Computer.
7. Aktualisieren Sie die Datei "NX.env" mit den angepassten Variablen.
8. Kopieren Sie den Anhangsordner aus dem älteren Computer in den neuen Computer.

9. Führen Sie die Konfiguration auf dem neuen Computer erneut aus.
10. Aktualisieren Sie die Computerdetails an den erforderlichen Stellen im Optionsmanager.

Beispiel: Migrieren von einer nicht unterstützten Windows-Umgebung

In diesem Beispiel ist CA SDM r11.2 unter Redhat Enterprise Linux 4 mit Oracle 10g installiert. Sie möchten eine Migration Ihrer Daten und ein Upgrade auf CA SDM r12.9 unter einem Redhat Enterprise Linux 6-System mit Oracle 11g R2 erfolgreich durchführen.

Gehen Sie wie folgt vor:

1. Migrieren Sie CA SDM r12.5 auf dem gleichen Computer.
2. Sichern Sie die MDB-Datenbank.
3. Installieren Sie CA SDM r12.5 unter Redhat Enterprise Linux 6 mit Oracle 11g R2.
4. Laden Sie MDB-Sicherung, die Sie unter Schritt 2 durchgeführt haben.
5. Verschieben Sie den Ordner "\$NX_ROOT\site\mod" aus dem älteren Computer in den neuen Computer.
6. Aktualisieren Sie die Datei "NX.env" mit den angepassten Variablen.
7. Kopieren Sie den Anhangsordner aus dem älteren Computer in den neuen Computer.
8. Führen Sie die Konfiguration auf dem neuen Computer erneut aus.
9. Aktualisieren Sie die Computerdetails an den erforderlichen Stellen im Optionsmanager.
10. Migrieren Sie von CA SDM r12.5 auf r12.9.

Support-Automatisierung-Datenmigration

Sie können Daten aus CA Support-Automatisierung r6.0 SR1 eFix5 aus den folgenden Umgebungen nach CA SDM r12.9 migrieren:

- Unicenter Service Desk r11.2
- CA SDM r12,0
- CA SDM r12,1
- CA Support-Automatisierung r6.0 SR1 eFix5 ohne CA SDM.

Hinweis: Es können nur Daten von CA Support-Automatisierung r6.0 SR1 eFix5 migriert werden. Es wird empfohlen, vor der Migration eine vollständige Sicherung der Datenbank von CA Support-Automatisierung r6.0 SR1 eFix5 vorzunehmen.

Wichtig! Branding-Anpassungen von CA Support-Automatisierung r6,0 SR1 eFix5 werden nicht automatisch nach CA SDM r12.9 migriert. Sie sollten Branding-Anpassungen überprüfen, um sicherzustellen, dass sie dem Branding von CA SDM entsprechen. Kopieren Sie bei Bedarf Kopf- und Fußzeilen sowie CSS URL-Daten jedes Organisationsbereichs, und fügen Sie diese in den entsprechenden Mandanten (oder in den öffentlichen Bereich) in CA SDM ein, um die Brandingdaten zu migrieren.

Migrieren von Support-Automatisierung-Datenbanken

Sie können das Migrations-Tool so konfigurieren, dass Daten aus der Support-Automatisierung-Datenbank in die CA SDM-Datenbank migriert werden, einschließlich Support-Automatisierung-Namenstransformationen in die CA SDM-Datenbankkonventionen. Migrieren Sie die Daten aus der Support-Automatisierung-Datenbank in die CA SDM-Datenbank, bevor Sie Support-Automatisierung zum ersten Mal verwenden.

Der folgende Prozess beschreibt, wie die Daten migriert werden:

1. [Exportieren](#) (siehe Seite 52) Sie die CA Support-Automatisierung-Daten anhand des Skripts auf dem Installationsdatenträger.

Das Export-Tool konvertiert die Daten in das .DAT-Format Während der Datenmigration führt das Tool im Wesentlichen die folgenden Schritte aus:

- Importieren des Support-Automatisierung-Datenbankschemas in die CA SDM-Datenbank.

Dieses Schema erstellt die notwendigen Tabellen, die von Support-Automatisierung verwendet werden.

- Migrieren der Daten aus der Support-Automatisierung-Datenbankmigrations-XML in die CA SDM-Datenbank.

Das CA SDM-Migrations-Tool erzeugt die notwendigen UUIDs und erstellt die benötigten Datensätze, die die Beziehungen zwischen der Support-Automatisierung-ID und der CA SDM-UUID darstellen.

2. Kopieren Sie den Exportordner mit den CA Support-Automatisierung-Daten in das folgende Verzeichnis auf dem CA SDM-Server:

NX_ROOT/site/sbmigration/SA60

Der Datenexport wird abgeschlossen.

3. [Importieren](#) (siehe Seite 54) Sie die Daten mithilfe des CA Support-Automatisierung Migrationstools in CA SDM.

Die Daten werden in die Datenbank geladen und die Migration wird abgeschlossen.

Verlaufsdatenmigration

Wenn Sie nicht alle Verlaufsdaten aus der CA Support-Automatisierung r6.0 SR1 eFix5-Datenbank migrieren möchten, können Sie einen Teil der Verlaufsdaten löschen. Sie können die Anzahl Tage für die Aufbewahrung in der Einrichtung des Lösch-Skripts konfigurieren.

Das Lösch-Skript können Sie vom folgenden Speicherort herunterladen:

ftp://ftp.ca.com/pub/supportbridge/6,0/patch-01/purge_history_6,0_sp1.zip

Konvertieren von Bereichen zu Mandanten

Bereiche können Sie nur von CA Support-Automatisierung r6,0 SR1 eFix5 migrieren. Die Bereiche werden in Mandanten konvertiert, um mehrere Mandanten in einer Support-Automatisierung-Umgebung zu verwenden. Jeder Bereich kann getrennt als eigener Mandant migriert werden. Während des anfänglichen Datenimports werden alle Zeilen in Tabellen mit optionalen Mandanten in Mandantenzeilen umgewandelt.

Wichtig! Diese Daten werden migriert, bevor Sie Support-Automatisierung in CA SDM aktivieren.

Sie können Bereiche wie folgt an Mandanten migrieren:

1. [Exportieren](#) (siehe Seite 52) Sie die Bereichsdaten anhand des Skripts auf dem Installationsdatenträgern.

Sie können einen einzelnen Bereich oder alle Bereiche exportieren.

2. Das Export-Tool konvertiert die Daten in das *.DAT*-Format.

Das Tool zeigt den Status des Bereichsexports an.

3. Kopieren Sie den Exportordner mit den CA Support-Automatisierung-Daten in das folgende Verzeichnis auf dem CA SDM-Server:

`NX_ROOT/site/sbmigration/SA60`

Der Datenexport wird abgeschlossen.

4. [Importieren](#) (siehe Seite 54) Sie die Daten mithilfe des CA Support-Automatisierung Migrationstools in CA SDM.

Die Daten werden in die Datenbank geladen und die Migration wird abgeschlossen.

Hinweis: Weitere Informationen zum Konfigurieren von Support-Automatisierung finden Sie in der *Online-Hilfe*.

Exportieren von CA Support-Automatisierung-Daten

Daten aus CA Support-Automatisierung r6.0 SR1 eFix5 werden exportiert, indem sie in das von CA SDM verwendete .DAT-Format konvertiert werden. Sie können Bereiche in getrennte Mandanten exportieren und die Daten in eine öffentliche Umgebung importieren. Das Export-Tool protokolliert den Prozess und zeigt das Ausgabeverzeichnis der Protokolldatei an, nachdem der Export abgeschlossen ist. Der Exportprozess zeichnet die erfolgreiche Ausgabe der einzelnen Tabellen auf und gibt alle festgestellten unerwarteten Bedingungen oder Fehler an.

Wichtig! Bereiche können Sie nur von CA Support-Automatisierung r6,0 SR1 eFix5 migrieren.

So exportieren Sie CA Support-Automatisierung-Daten

1. Führen Sie das "SA60Export"-Skript vom Installationsdatenträger im folgenden Verzeichnis aus:

`/casd.nt/SAMigration`

Hinweis: Die Dateierweiterung hängt von Ihrem Betriebssystem ab. Windows verwendet beispielsweise "bat", UNIX verwendet "sh" für das Bourne-Shell-Skript, "csh" für die C-Shell und "ksh" für die Korn-Shell, usw.

Das CA Support-Automatisierung-Migrations-Tool wird angezeigt.

2. Tun Sie Folgendes:
 - a. Geben Sie das übergeordnete Installationsverzeichnis für CA Support-Automatisierung r6.0 SR1 eFix5 "WEB-INF" ein.
 - b. Geben Sie ein Verzeichnis zum Exportieren der CA Support-Automatisierung-Daten an.

Hinweis: Verschieben Sie diesen Ordner nach Abschluss des Exports in das Verzeichnis "NX_ROOT/site/sbmigration/SA60" auf dem CA SDM-Server.

- c. (Optional) Geben Sie an, ob Kennwörter exportiert werden können. Wenn Sie diese Option auswählen, werden Kennwörter für Benutzer, Standardanmeldeinformationen, und Anmeldeinformationen der automatisierten Aufgaben exportiert.
 - d. (Optional) Exportieren Sie einen einzelnen Bereich oder alle Bereiche. Wenn Sie diese Option auswählen, zeigt eine Dropdown-Liste alle aktiven Bereiche an.
3. Klicken Sie auf "Start".

Der Prozessstatus zeigt Informationen über den Export an, wie z. B. die migrierte Datenbanktabelle und eine Zählung der Datensätze in der Tabelle.

Eine Meldung wird angezeigt, wenn das Tool nicht wiederherstellbare Fehler feststellt.

Hinweis: Sie können den Export anhalten, indem Sie "Anhalten" aus der Symbolleiste oder dem Menü "Datei" auswählen.

Der Datenexport wird abgeschlossen.

4. Konfigurieren und implementieren Sie Support-Automatisierung entsprechend Ihrer Umgebung.

Hinweis: Weitere Informationen zum Konfigurieren von Support-Automatisierung-Optionen finden Sie in der *Online-Hilfe*.

Importieren von Support-Automatisierung-Daten

Support-Automatisierung-Daten werden importiert, nachdem sie in das *.DAT*-Format konvertiert wurden. Sie können die Daten mit Hilfe des Support-Automatisierung-Migrationsskripts in CA SDM importieren. Rufen Sie das Dienstprogramm nach dem Installieren und Konfigurieren von CA SDM auf. Sie können *"sa_migrate.pl"* auch über den Befehl *"pdm_perl"* ausführen.

Auf das Skript können Sie im Verzeichnis *"NX_ROOT\bin\"* zugreifen. Das Migrationsskript führt Aufgaben wie das Verarbeiten von Tabellen zum Verwalten von Datenbankbeschränkungen aus, erstellt entsprechende CA SDM-Objekte, ordnet Mandantenspaltenwerte zu usw.

Der Standardspeicherort für migrationsbezogene Dateien in der CA SDM-Installation ist das Verzeichnis *"NX_ROOT/site/sbmigration"*. Zum Beispiel befindet sich die Importkonfigurationsdatei im Ordner *"NX_ROOT/site/sbmigration/config"*. In der Datei *sa_migration_config.dat* sind die Spalten *"id"*, *"prop_name"*, *"value"* und *"prop_description"* im CA SDM-Datenformat gespeichert.

In dem Verzeichnis werden Exportdaten für CA Support-Automatisierung r6.0 SR1 eFix5, Migrations-Hilfsprogrammcode, Perl-Skripts usw. gespeichert.

So importieren Sie Support-Automatisierung-Daten

1. Starten Sie den CA SDM-Service.

Der Service startet, und Sie können überprüfen, dass er ausgeführt wird.

2. Geben Sie an der Befehlszeile den folgenden Befehl ein:

```
pdm_perl <NX_ROOT>\bin\sa_migrate.pl
```

Die Support-Automatisierung-Daten werden aus dem Exportpaket in die Datenbank geladen.

Konfigurieren des Support-Automatisierung-Rollenzugriffs nach der Migration

Wenn Sie Support-Automatisierung vor der Migration konfigurieren, wird der Rollenzugriff richtig konfiguriert. Wenn Sie Support-Automatisierung nach der Migration konfigurieren, legen Sie für das sa>-Zugriffsfeld für jede Rolle den entsprechenden Wert fest. Wenn der Rollenzugriff nicht richtig eingerichtet wird, können Sie nicht auf die Support-Automatisierung-Analystenschnittstelle oder die Endbenutzerschnittstelle zugreifen.

Der folgende Prozess beschreibt, wie der Support-Automatisierung-Rollenzugriff nach der Migration konfiguriert wird:

1. Installieren Sie die Option *"supportautomation_url"*.

2. Legen Sie das Support-Automatisierung-Zugriffsfeld für jede Rolle fest, die Zugriff auf Support-Automatisierung haben soll.

Hinweis: Weitere Informationen zum Installieren der Option "*supportautomation_url*" oder zum Erstellen von Support-Automatisierung-Zugriffsrollen finden Sie in der *Online-Hilfe*.

Migrieren eines benutzerdefinierten CA Business Intelligence-Universums

Ein benutzerdefiniertes Universum kann folgendermaßen migriert werden:

1. Folgen Sie den Anweisungen, um ein benutzerdefiniertes Universe mit dem CA SDM-Universum zu verknüpfen.
2. Erstellen Sie eine Sicherungskopie der *BIAR*-Datei von allen standortdefinierten Universen oder Berichten.
3. Installieren Sie ein Universum der aktuellen Version.
4. Verknüpfen Sie das benutzerdefinierte Universum mit dem Universum der aktuellen Version.

Erstellen einer Sicherungskopie von einem benutzerdefinierten Universum

Wenn Sie ein benutzerdefiniertes Universum mit dem CA SDM Universum verknüpft haben, führen Sie die folgenden Schritte aus, bevor Sie das CA SDM r12.9-Universum und Berichte installieren:

1. Verwenden Sie den Importassistenten, um eine Sicherungs-"*BIAR*"-Datei von standortdefinierten Universen oder Berichten zu erstellen.
2. Starten Sie Universe Designer.
3. Importieren Sie Ihr benutzerdefiniertes Universe.
4. Speichern Sie eine Kopie des Universe auf Ihrem lokalen Laufwerk.

Es wurde eine Sicherungskopie des benutzerdefinierten Universums erstellt.

Weitere Informationen:

[Verschieben aus der Entwicklung in die Produktion](#) (siehe Seite 528)

Installieren eines CA Business Intelligence-Universums

Sie installieren das Universum, um das CA Business Intelligence-r12.0-Universum und Berichte zu ersetzen.

So installieren Sie das Universum:

1. Führen Sie auf der CA Service Desk Manager-DVD 2 die Datei "setup.exe" aus.
2. Wählen auf die Registerkarte "Produktinstallationen" aus.
3. Scrollen Sie nach unten und wählen Sie "CA Business Intelligence-Konfiguration" aus.

Der Installationsassistent für CA Service Desk Manager-Komponenten wird angezeigt.

4. Klicken Sie auf "Weiter", und geben Sie Ihre Anwenderanmeldeinformationen ein.

Hinweis: Wenn CA SDM auf diesem Computer nicht installiert ist, geben Sie den CA SDM-Hostnamen ein.

5. Klicken Sie auf "Fertig stellen".

Das CA Business Intelligence-r12.0-Universum und die Berichte wurden ersetzt, und die r12.9-Berichte wurden in den Unterordnern erstellt.

Aktualisieren einer Universe-Verbindung

Obwohl der Universumsname in CA SDM r12.9 unverändert bleibt, *müssen* Sie den Universumslink zum Universum aktualisieren. Andernfalls können Universe-Verbindungsprobleme auftreten, wenn Sie Ihre Berichte ausführen das Universe importieren. Die folgende Fehlermeldung kann auftreten:

Unable to resolve core universe ID

So aktualisieren Sie die Universe-Verknüpfung:

1. Starten Sie Universe Designer auf dem gleichen Computer, auf dem Sie eine Sicherungskopie des benutzerdefinierten Universe erstellt hatten.
2. Wählen Sie "Datei" > "Öffnen", um Ihr benutzerdefiniertes Universum zu öffnen.
3. Wählen Sie "Datei" > "Parameter".

Das Dialogfeld "Universe-Parameter" wird angezeigt.

4. Klicken Sie auf die Registerkarte "Links".
5. Klicken Sie unter der Spalte "Name" auf das CA SDM-Universum.
Die Schaltfläche "Change Source" wird aktiviert.
6. Klicken Sie auf die Schaltfläche "Change Source".

7. Navigieren Sie zum Speicherort der *UNV*-Datei von CA SDM.
Hinweis: Die *UNV*-Datei befindet sich der Regel im CA-Universenordner.
8. Klicken Sie auf "Öffnen" und anschließend auf "OK".
Die Universe-Verknüpfung ist aktualisiert.
9. Exportieren Sie das benutzerdefinierte Universe.

Konfiguration nach der Aktualisierung

Sobald die Aktualisierung abgeschlossen ist, können Sie das Produkt konfigurieren. Mit dem Konfigurations-Assistenten können Sie durchgeführte Anpassungen überprüfen.

Hinweis: Wenn der Konfigurationsdialog geschlossen wird, ohne dass die Konfiguration nach der Aktualisierung vollständig ist, führen Sie *pdm_configure -s* über die Befehlszeile aus.

Inaktive Server, die keine primären oder sekundären Server sind

Nachdem Sie den Upgrade durchgeführt haben, werden alle Server, die nicht als Primärserver in der *usp_servers*-Tabelle eingegeben worden sind, in Sekundärserver konvertiert. Wenn Sie vor dem Upgrade Server zur Tabelle "*usp_servers*" hinzugefügt haben, die keine Primär- oder Sekundärserver sind, deaktivieren Sie diese nach dem Upgrade. Sie können Server über die Web-Schnittstelle des Primärservers deaktivieren.
Hinweis: Weitere Informationen finden Sie in der *Online-Hilfe*.

Vorhandene Kunden mit EEM 8.4-Server unterstützen

CA SDM r12.9 verwendet EEM 12.5 SDK, das mit EEM 8.4-Servern nicht kompatibel ist. Um die vorhandenen Kunden zu unterstützen, die EEM 8.4-Server verwenden, muss das EEM 8.4 SDK-Patch auf dem CA SDM r12.9-Server angewandt werden. Die Patchdetails finden Sie bei CA Support Online.

Aktualisieren von CA Workflow und CA EEM

CA Workflow und CA EEM installieren Sie separat in CA SDM r12.9.

Für die Migration auf r12.9 müssen Sie ein Upgrade auf CA EEM r8.4 SP4 und CA Workflow r1.1.132 durchführen.

Hinweis: Von CA EEM r8.1 können Sie direkt auf r8.4 SP4 aktualisieren.

Um CA EEM und CA Workflow zu aktualisieren, führen Sie die folgenden Aufgaben durch:

1. Überprüfen Sie, dass Sie CA SDM r12.9 erfolgreich aktualisiert haben.
2. Legen Sie den Installationsdatenträger in Ihr Laufwerk ein.
3. Installieren von CA EEM
4. Installieren Sie CA Workflow.

Nachdem Sie CA Workflow und CA EEM installiert haben, legen Sie die entsprechenden Optionen im Optionsmanager manuell fest. Überprüfen Sie die aktualisierten Optionen sorgfältig. Der Standard-Tomcat-Port für CA Workflow ist nicht mehr Port 8080, und die Standard-Prozessmanager-URL lautet nicht mehr "pmService".

Hinweis: Die Option "cawf_pm_url" wurde in den Standardwert `http://<wf_hostname>:<wf_tomcat_port>/pm/service/pmService2` geändert. Sie *müssen* manuell "pmService" in "pmService2" ändern, damit die CAWF-Kommunikation weiterhin funktioniert.

Wichtig! Nach dem Upgrade von CA EEM *müssen* Sie die Optionen `eiam_hostname`, `use_eiam_artifact` und `use_eiam_authentication` im Optionsmanager unter "Sicherheit" festlegen, wenn zuvor die eIAM-Anwenderauthentifizierung für CA SDM verwendet wurde. Weitere Informationen zu diesen Optionen finden Sie in der *Online-Hilfe*.

Vorherige Serverkonfiguration beibehalten

In den früheren Versionen von CA SDM wurden die Informationen zur Serverprozesskonfiguration (mit dem Skript "pdm_edit.pl" erstellt) im Verzeichnis "\$NX_ROOT/samples/pdmconf" in der Datei "pdm_startup.dat" gespeichert. Um diese Serverprozesskonfiguration in CA SDM r12.9 beizubehalten, muss die Datei "pdm_startup.dat" so bearbeitet werden, dass sie diese Konfiguration generiert, die dann mithilfe des Befehls "pdm_configure" angewandt werden kann.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei der Web-Benutzeroberfläche des Primärservers an, und fügen Sie ggf. alle Sekundärserver hinzu, die Teil der früheren CA SDM-Version waren. Weitere Informationen finden Sie in der *Online-Hilfe*.
2. Wechseln Sie in das Verzeichnis "SNX_ROOT/bin", und führen Sie das Befehlszeilentool "pdm_edit_migration" aus. Dieses Tool ist nur für die konventionelle CA SDM-Konfiguration verwendbar.

Wenn dieses Tool erfolgreich ausgeführt wird, wird eine neue Konfiguration mit aktivem Status. Anderenfalls wird eine neue Konfiguration mit inaktivem Status erstellt. Überprüfen Sie die neue Konfiguration von der CA SDM-Web-Schnittstelle Systeme, Konfiguration in der Registerkarte "Verwaltung". Nur aktive Konfigurationen können auf einem Server angewandt werden.

Hinweis: Wenn das Tool nicht erfolgreich ausgeführt wird, korrigieren Sie die Problemeingaben in der Datei "pdm_startup.dat", und führen Sie das Tool erneut aus.

3. Führen Sie "pdm_configure" auf dem Primärserver aus, um diese neue Konfiguration anzuwenden. Weitere Informationen finden Sie in der *Hilfe zur Serverkonfiguration*.

Integration von CA SDM und CA IT PAM aktivieren

Nach dem Upgrade müssen Sie sicherstellen, dass die Integration von CA SDM mit IT PAM 4.0 oder höher erfolgt ist, indem Sie folgende Schritte ausführen:

1. Gehen Sie zu Optionsmanager, CA IT PAM-Workflow, und ändern Sie den Wert der folgenden Optionen:
2. Legen Sie den Wert von caextwf_processdisplay_url auf `http://<wf_hostname>:<wf_tomcat_port>/itpam/Web.jsp?page=runtimeeditor&ROID= fest`
3. Legen Sie den Wert von caextwf_worklist_url auf `http://<wf_hostname>:<wf_tomcat_port>/itpam?page=tasklist fest`

Wichtig! Wenn CA SDM in CA IT PAM integriert wird, welches CA EEM 8.4 verwendet, müssen Sie das CA EEM 8.4 SDK-Patch auf CA SDM anwenden. Die Patchdetails finden Sie bei CA Support Online.

Löschen des Cache von Web-Engine und Browser

Nachdem Sie auf CA SDM r12.9 aktualisiert haben, löschen Sie den Cache von Web-Engine und Browser mit dem Dienstprogramm "pdm_webcache".

```
pdm_webcache -b -H
```

-b

Weist den Anwender darauf hin, dass der Browser-Cache gelöscht werden muss.

-H

Löscht den Web-Engine-Cache.

Konfigurieren des Web-Director und der Server

Nachdem Sie ein Upgrade durchgeführt haben, empfehlen wir Ihnen, dass Sie die Server und Web-Director konfigurieren.

So konfigurieren Sie WebDirector und Server

Wenn die Vorgängerversion konfiguriert wurde, um zusätzliche Server oder Web-Directors zu verwenden, können Sie die Server und Web-Director konfigurieren und die Konfiguration nach dem Upgrade anwenden.

Weitere Informationen hierzu finden Sie auch im *Administrationshandbuch*.

LREL nach der Migration

Führen Sie nach der Migration die folgenden Prüfschritte durch:

1. Fragen Sie den Inhalt der neuen Tabellen ab, um zu überprüfen, dass die Tabellen die richtigen Daten enthalten.
2. Aktualisieren Sie jeden standortspezifischen Bericht, um zu überprüfen, dass die Berichtsdaten aus den neuen LREL-Tabellen stammen.
3. Testen Sie standortdefinierte Berichte.

Veraltete Objekte und Tabellen

Die folgenden Objekte und Tabellen sind in dieser Version von CA SDM veraltet. Während der Migration kopiert das System die Daten in r12.9-LREL-Tabellen. Vom System werden die LREL-Tabellen und -Objekte verwendet. Zu Referenzzwecken werden in den alten Tabellen jedoch die Daten beibehalten, die zum Zeitpunkt der Aktualisierung vorhanden waren.

Hinweis: Weitere Informationen zu LREL finden Sie im *Technischen Referenzhandbuch*.

DBMS-Name:	Objektname
Attachment_Lrel	attmnt_lrel
Business_Management_Repository_Lrel	bmlrel
Chgcat_Group	chgcat_grp
Chgcat_Loc	chgcat_loc
Chgcat_Workshift	chgcat_workshift
Group_Loc	grp_loc
Isscat_Group	isscat_grp
Isscat_Loc	isscat_loc
Isscat_Workshift	isscat_workshift
Knowledge_Lrel_Table	kmlrel
Lrel_Table	lrel1
Pcat_Group	pcat_grp
Pcat_Loc	pcat_loc
Pcat_Workshift	pcat_workshift
Wftpl_Group	wftpl_grp

LREL-Tabellen und -Objekte

Durch die Migration werden automatisch die folgenden Tabellen und Objekte zum Verwalten von m:m-Datenbeziehungen erstellt:

DBMS-Name:	Objektname
usp_lrel_asset_chgnr	lrel_asset_chgnr
usp_lrel_asset_issnr	lrel_asset_issnr
usp_lrel_att_cntlist_macro_ntf	lrel_att_cntlist_macro_ntf
usp_lrel_att_ctplist_macro_ntf	lrel_att_ctplist_macro_ntf
usp_lrel_att_ntflist_macro_ntf	lrel_att_ntflist_macro_ntf
usp_lrel_attachments_changes	lrel_attachments_changes
usp_lrel_attachments_issues	lrel_attachments_issues
usp_lrel_attachments_requests	lrel_attachments_requests
usp_lrel_aty_events	lrel_aty_events

usp_lrel_bm_reps_assets	lrel_bm_reps_assets
usp_lrel_bm_reps_bmhiers	lrel_bm_reps_bmhiers
usp_lrel_cenv_cntref	lrel_cenv_cntref
usp_lrel_dist_cntlist_mgs_ntf	lrel_dist_cntlist_mgs_ntf
usp_lrel_dist_ctplist_mgs_ntf	lrel_dist_ctplist_mgs_ntf
usp_lrel_dist_ntflist_mgs_ntf	lrel_dist_ntflist_mgs_ntf
usp_lrel_false_action_act_f	lrel_false_action_act_f
usp_lrel_false_bhv_false	lrel_false_bhv_false
usp_lrel_kwrds_crsolref	lrel_kwrds_crsolref
usp_lrel_notify_list_cntchgntf	lrel_notify_list_cntchgntf
usp_lrel_notify_list_cnttssntf	lrel_notify_list_cnttssntf
usp_lrel_notify_list_cntntf	lrel_notify_list_cntntf
usp_lrel_ntfr_cntlist_att_ntfrlist	lrel_ntfr_cntlist_att_ntfrlist
usp_lrel_ntfr_ctplist_att_ntfrlist	lrel_ntfr_ctplist_att_ntfrlist
usp_lrel_ntfr_macrolist_att_ntfrlist	lrel_ntfr_macrolist_att_ntfrlist
usp_lrel_ntfr_ntflist_att_ntfrlist	lrel_ntfr_ntflist_att_ntfrlist
usp_lrel_oenv_orgref	lrel_oenv_orgref
usp_lrel_status_codes_tsktypes	lrel_status_codes_tsktypes
usp_lrel_svc_grps_svc_chgcat	lrel_svc_grps_svc_chgcat
usp_lrel_svc_grps_svc_isscat	lrel_svc_grps_svc_isscat
usp_lrel_svc_grps_svc_pcat	lrel_svc_grps_svc_pcat
usp_lrel_svc_grps_svc_wftpl	lrel_svc_grps_svc_wftpl
usp_lrel_svc_locs_svc_chgcat	lrel_svc_locs_svc_chgcat
usp_lrel_svc_locs_svc_groups	lrel_svc_locs_svc_groups
usp_lrel_svc_locs_svc_isscat	lrel_svc_locs_svc_isscat
usp_lrel_svc_locs_svc_pcat	lrel_svc_locs_svc_pcat
usp_lrel_svc_schedules_chgcat_svc	lrel_svc_schedules_chgcat_svc
usp_lrel_svc_schedules_isscat_svc	lrel_svc_schedules_isscat_svc
usp_lrel_svc_schedules_pcat_svc	lrel_svc_schedules_pcat_svc
usp_lrel_true_action_act_t	lrel_true_action_act_t
usp_lrel_true_bhv_true	lrel_true_bhv_true

Überprüfen der LREL-Konvertierung

Während der Datenmigration fügt das System LREL-Tabellen hinzu, um n:m-Beziehungen zu verwalten. Sie können den Inhalt der neuen Tabellen, des aktualisierten standortdefinierten Codes und der Berichte überprüfen.

So überprüfen Sie Daten in den LREL-Tabellen

1. Fragen Sie den Inhalt der Tabellen ab, um zu überprüfen, dass sie die richtigen Daten enthalten.
2. Aktualisieren Sie jeden standortspezifischen Bericht, um zu überprüfen, dass die Berichtsdaten aus den neuen LREL-Tabellen stammen.
3. Aktualisieren Sie die Abfragen mit den neuen DBMS-Tabellenverweisen.
4. Testen Sie die standortdefinierten Berichte und den Code. Aktualisieren Sie den Code, um die neuen LREL-Tabellen und eine unterstützte Schnittstelle wie Webservices zu verwenden. Aktualisieren Sie ggf. Tabellennamen im Code.

Überprüfen der Datenbankanpassungen

Sie können überprüfen, dass Ihre Datenbankanpassungen korrekt in die aktuelle Produktversion migriert wurden.

So überprüfen Sie Datenbankanpassungen

1. Überprüfen Sie alle angepassten Tabellen, die entweder Ihr Datenbank-Management-Produkt oder WSP verwenden.
2. Überprüfen Sie, dass die angepassten Dateien im folgenden Verzeichnis vorhanden sind:

`$NX_ROOT/site/mods/`

Überprüfen der Anpassungen von Webformularen

Sie können überprüfen, ob Ihre Webformularanpassungen in der aktuellen Produktversion ordnungsgemäß funktionieren.

Überprüfen der Anpassungen von Webformularen

1. Überprüfen Sie, dass Ihre angepassten Formulare im Verzeichnis "`$NX_ROOT/site/mods/www/html`" vorhanden sind.
2. Überprüfen Sie, dass das Webformular korrekt in einem Browser geöffnet wird.
3. Überprüfen Sie, ob das Webformular korrekt in "Web Screen Painter" geöffnet wird.

Bearbeiten von Zugriffstypen

Wenn Sie von CA SDM r11.2 auf die aktuelle Produktversion aktualisieren, werden durch diesen Prozess automatisch Rollen für alle Zugriffstypen erstellt und den Rollen die richtigen Berechtigungen zugewiesen. Wenn Sie die neuen Rollen in r12.9 nutzen wollen, können Sie Rollen für Zugriffstypen erstellen.

So erstellen Sie Rollen für Zugriffstypen:

1. Melden Sie sich bei der Web-Schnittstelle als Benutzer mit der Berechtigung zum Zugriff auf die Registerkarte "Administration" an.
2. Klicken Sie auf die Registerkarte "Verwaltung".
3. Wählen Sie links in der Baumstruktur "Sicherheits- und Rollenmanagement" > "Zugriffstypen".

Es werden alle verfügbaren Zugriffstypen angezeigt.

4. Klicken Sie auf einen verfügbaren Zugriffstyp.

Die Detailseite für die Zugriffstypen wird angezeigt.

5. Klicken Sie auf die Registerkarte "Rollen".

6. Wählen Sie eine neue Rolle für den Zugriffstyp, und klicken Sie auf "Rollen aktualisieren".

Die neue Rolle wird dem Zugriffstyp zugewiesen.

Hinweis: Sie können auch eine benutzerdefinierte Rolle erstellen und diese dem Zugriffstyp zuweisen. Informationen über das Erstellen von Rollen finden Sie im *Administrationshandbuch*.

Aktivieren der Prioritätsberechnung

Die *Prioritätsberechnung* ist ein Wertesatz, mit dem automatisch die Werte für Priorität, Dringlichkeit und Auswirkung für Probleme und Incidents festgelegt werden. Für neue CA SDM-Installationen ist die Standard-Prioritätsberechnung für Problem- und Incident-Tickettypen standardmäßig aktiviert. Wenn Sie jedoch eine frühere Version aktualisieren, ist die Standard-Prioritätsberechnung deaktiviert.

Wenn Sie eine andere Prioritätsberechnung erstellen und aktivieren, entsprechen die Ticket-Werte den Einstellungen in der aktiven Prioritätsberechnung, die einem Incident oder Problem zugeordnet ist. Wenn keine Prioritätsberechnung aktiv ist, können die Anwender die Priorität und andere Ticket-Werte manuell festlegen.

Hinweis: Die angepassten Formulare der Mitarbeiter- und Kundenschnittstelle funktionieren genauso wie in den Vorgängerversionen. Die Self-Service-Anwender können die Priorität direkt und ungeachtet der Einstellungen der Prioritätsberechnung ändern.

Führen Sie die folgenden Schritte aus, um die Prioritätsberechnung nach der Migration zu aktivieren:

1. Wählen Sie auf der Registerkarte "Administration" die Optionen "Service Desk" > "Requests/Incidents/Probleme" > "Prioritätsberechnung".

Die Prioritätsberechnungsliste wird angezeigt.

2. Klicken Sie mit der rechten Maustaste auf die Standard-Prioritätsberechnung oder eine andere Prioritätsberechnung, und wählen Sie im Kontextmenü "Bearbeiten" aus.

Die Seite "Prioritätsberechnung aktualisieren" wird angezeigt.

3. Legen Sie den Status auf "Aktiv" fest.
4. Wählen Sie einen oder mehrere der folgenden Ticket-Typen aus:

Incidents

Aktiviert diese Prioritätsberechnung zum Verwalten von Incident-Tickets. Nur eine aktive Prioritätsberechnung kann Incidents verwalten.

Probleme

Aktiviert diese Prioritätsberechnung zum Verwalten von Problem-Tickets. Nur eine aktive Prioritätsberechnung kann Probleme verwalten.

5. Klicken Sie auf "Speichern".

Solange Sie keine andere Prioritätsberechnung aktivieren, werden auf neue Tickets die Werte der Standard-Prioritätsberechnung angewendet. Bei neuen Tickets, die eine Prioritätsberechnung verwenden, ist das Feld "Priorität" schreibgeschützt.

Hinweis: Informationen zum Definieren einer Prioritätsberechnung für Mandanten und Tickets finden Sie im *Administrationshandbuch* und in der *Online-Hilfe*.

Hinzufügen des Felds "Incident-Priorität" zu Incidents

Die *Incident-Priorität* ist die Summe der Dringlichkeits- und Auswirkungswerte. Die Incident-Priorität gilt nur für den Ticket-Typ "Incident". Der Incident-Prioritätswert wird für die Incidents angezeigt, nachdem Sie die Option "use_incident_priority" installiert und dem Incident-Detailseitenformular mit Web Screen Painter hinzugefügt haben.

Führen Sie die folgenden Schritte aus, um das Incident-Prioritätsfeld für Incidents hinzuzufügen:

1. Installieren Sie die Option "use_incident_priority" über "Optionsmanager" > "Request-Manager".
2. Verwenden Sie Web Screen Painter, um das Incident-Prioritätsfeld den Incident-Detailseiten hinzuzufügen.

Der Incident-Prioritätswert wird auf der gespeicherten Incident-Detailseite angezeigt, wenn die Option "use_incident_priority" installiert ist. Wenn die Option "use_incident_priority" nicht installiert ist, ist der Wert für "Incident-Priorität" Null.

Hinweis: Die Option "use_incident_priority" verwaltet nur den Incident-Prioritätswert. Diese Option hängt nicht mit der Prioritätsberechnung zusammen.

Weitere Informationen:

[Festlegen des Dringlichkeitsbereichs für Self-Service-Benutzer](#) (siehe Seite 68)

Hinzufügen des Felds "Dringlichkeit" zu Mitarbeiter-Tickets

Standardmäßig wird das Feld "Dringlichkeit" nicht in Mitarbeiter-Incidents oder -Anfragen angezeigt. Über die Option "urgency_on_employee" können Sie das Feld "Dringlichkeit" jedoch hinzufügen.

Hinweis: Wenn Sie die Option "urgency_on_employee" deinstallieren und die Prioritätsberechnung deaktivieren, wird das Feld "Priorität" auf den Anfragen- und Incident-Detailseiten für Self-Service-Benutzer angezeigt.

Um das Feld "Dringlichkeit" in Mitarbeiter-Tickets hinzuzufügen, installieren Sie die Option "urgency_on_employee" über "Optionsmanager" > "Anfragenmanager". Das Feld "Dringlichkeit" wird in Mitarbeiter-Incidents oder -Anfragen angezeigt. Self-Service-Benutzer können den Wert im Incident überschreiben.

Festlegen von Ticket-Werten für Self-Service-Benutzer

Sie können die Dringlichkeits- und Prioritätswerte steuern, die den Self-Service-Benutzern angezeigt werden. Über die Eigenschaften, die Sie in der "web.cfg"-Datei festlegen, werden die Auswahlmöglichkeiten gesteuert, die den Benutzern beim Erstellen oder Bearbeiten von Tickets angezeigt werden.

Beim Festlegen von Ticket-Werten für Self-Service-Benutzer sollten Sie Folgendes berücksichtigen:

1. Für jeden Überschriftswert im "web.cfg"-Parameter geben Sie einen oder mehrere Werte an.
2. Für [Dringlichkeitswerte](#) (siehe Seite 69) geben Sie eine oder mehrere Zahlen von 0 bis 4 an.
3. Für [Prioritätswerte](#) (siehe Seite 70) geben Sie eine oder mehrere Zahlen von 1 bis 5 oder das Wort "None" an.
4. Trennen Sie die einzelnen Werte durch Leerzeichen.
5. Geben Sie den ersten Wert, der in der Liste angezeigt wird, als Standardwert für Tickets an. Ggf. können Sie den Standardwert für eine bessere Lesbarkeit in der Liste wiederholen.

Weitere Informationen:

[Festlegen des Dringlichkeitsbereichs für Self-Service-Benutzer](#) (siehe Seite 68)

[Werte für die Dringlichkeitseigenschaft](#) (siehe Seite 69)

[Festlegen des Prioritätsbereichs für Self-Service-Benutzer](#) (siehe Seite 69)

[Prioritätseigenschaftswerte](#) (siehe Seite 70)

Festlegen des Dringlichkeitsbereichs für Self-Service-Benutzer

Für Self-Service-Incidents und -Anfragen können Sie die Standard-Dringlichkeitswerte in der Datei "*web.cfg*" festlegen. Wenn Sie einen Dringlichkeitswertebereich festlegen, können Self-Service-Benutzer wie Mitarbeiter, VIP-Mitarbeiter oder Gäste Dringlichkeitswerte für Tickets festlegen. Die Wahlmöglichkeiten, die den Self-Service-Benutzern angezeigt werden, basieren auf dem Wertebereich, den Sie in "*web.cfg*" festlegen.

So legen Sie den Standard-Dringlichkeitsbereich für Self-Service-Benutzer fest

1. Gehen Sie zur Datei "*web.cfg*" im entsprechenden Verzeichnis:
 - (Windows) %NX_ROOT%\bopcfg\www\
 - (UNIX) \$NX_ROOT/bopcfg/www/
2. Geben Sie für jeden Parameter > einen oder mehrere [Dringlichkeitseigenschaftswerte](#) (siehe Seite 69) an. Trennen Sie die einzelnen Werte durch Leerzeichen.

ESCEmpUrg

Gibt an, wie VIP-Mitarbeiter die Dringlichkeit auf Tickets überschreiben können.

EmpUrg

Gibt an, wie Mitarbeiter die Dringlichkeit auf Tickets überschreiben können.

AnonymousUrg

Gibt gültige Prioritäten für Tickets an, die von Gastbenutzern erstellt werden.

3. Speichern Sie die Datei *web.cfg*.

Für neue Tickets können Mitarbeiter, VIP-Mitarbeiter oder Gäste Dringlichkeitswerte auf der Grundlage des Wertebereichs in "*web.cfg*" festlegen.

Beispiel: Für Gäste nur zwei Dringlichkeitswerte auf einer Anfrage anzeigen

1. Öffnen Sie die Datei *web.cfg*.
2. Legen Sie den Parameter "*AnonymousUrg*" als "0 4" fest. Beispiel: "*AnonymousUrg* 0 4".
3. Speichern Sie die Datei *web.cfg*.

Die Dringlichkeitswerte, die dem Self-Service-Benutzer angezeigt werden, sind "1-Wenn möglich" und "5-Sofort". Die Standarddringlichkeit ist "1-Wenn möglich".

Werte für die Dringlichkeitseigenschaft

"*web.cfg*" enthält Einstellungen, mit denen gesteuert wird, wie Self-Service-Benutzer die Dringlichkeit auf Tickets überschreiben können. Die folgenden Werte der Dringlichkeitseigenschaft sind verfügbar:

- **0**-Der Benutzer kann die Dringlichkeit auf "1-Wenn möglich" festlegen.
- **1**-Der Benutzer kann die Dringlichkeit auf "2-Bald" festlegen.
- **2**-Der Benutzer kann die Dringlichkeit auf "3-Schnell" festlegen.
- **3**-Der Benutzer kann die Dringlichkeit auf "4-Sehr schnell" festlegen.
- **4**-Der Benutzer kann die Dringlichkeit auf "5-Sofort" festlegen.

Festlegen des Prioritätsbereichs für Self-Service-Benutzer

Sie können eine Reihe gültiger Prioritäten festlegen, um es Self-Service-Benutzern zu ermöglichen, die Prioritätswerte der Tickets zu überschreiben. Wenn Sie den Prioritätsbereich festlegen, können Kunden, Mitarbeiter oder Gäste Prioritätswerte auf der Grundlage des Wertebereichs in "*web.cfg*" festlegen.

So legen Sie den Prioritätsbereich für Self-Service-Benutzer fest

1. Gehen Sie zur "*web.cfg*"-Datei im entsprechenden Verzeichnis:
 - (Windows) %NX_ROOT%\bopcfg\www\
 - (UNIX) \$NX_ROOT/bopcfg/www/
2. Geben Sie für jeden der Parameter einen oder mehrere [Prioritätseigenschaftswerte](#) (siehe Seite 70) an.

CstPrio

Gibt an, wie Kunden die Priorität auf Tickets überschreiben können.

EmpPrio

Gibt an, wie Mitarbeiter die Priorität auf Tickets überschreiben können.

AnonymousPrio

Gibt an, wie Mitarbeiter die Priorität auf Tickets überschreiben können.

3. Speichern Sie die Datei *web.cfg*.

Für neue Tickets können Kunden, Mitarbeiter oder Gäste Prioritätswerte auf der Grundlage des Wertebereichs in "*web.cfg*" festlegen.

Beispiel: Gästen nur zwei Prioritätswerte anzeigen

1. Öffnen Sie die Datei *web.cfg*.
2. Setzen Sie den Parameter *AnonymousPrio* auf den Wert "None 4". Beispiel:
AnonymousPrio None 4.

3. Speichern Sie die Datei *web.cfg*.

Wenn ein Gast mit Tickets arbeitet, sind die Werte für Dringlichkeit "Keine" oder "4". Der Standardwert ist "Keine".

Prioritätseigenschaftswerte

"*web.cfg*" enthält Einstellungen, mit denen gesteuert wird, wie Self-Service-Benutzer die Priorität auf Tickets überschreiben können. Die folgenden Prioritätseigenschaftswerte sind verfügbar:

- **Keine** - Der Benutzer kann die Priorität auf "Keine" festlegen.
- **1**-Der Benutzer kann die Priorität auf "1" festlegen (höchste Priorität)
- **2**-Der Benutzer kann die Priorität auf "2" festlegen
- **3**-Der Benutzer kann die Priorität auf "3" festlegen
- **4**-Der Benutzer kann die Priorität auf "4" festlegen
- **5**-Der Benutzer kann die Priorität auf "5" festlegen (niedrigste Priorität)

Aktivieren von Statusübergängen

Nach der Aktualisierung sind alle vordefinierten Statusübergänge inaktiv, also nicht in Kraft. Sie können diese Statusübergänge aktivieren und ändern, um sie dem gewünschten Statusübergangsablauf für Tickets anzupassen.

Hinweis: Alle Beschreibungen von angepassten Statuscodes, die auf Ticketformularen angezeigt werden, werden während des Aktualisierungsvorgangs beibehalten.

So aktivieren Sie einen Statusübergang

1. Erweitern Sie auf der Registerkarte "Administration" den Knoten "Service Desk", und wählen Sie einen der folgenden Ticket-Typen aus:
 - Änderungsaufträge
 - Change-Übergänge
 - Problemanfragen
 - Issue-Übergänge
 - Anfragen/Incidents/Probleme
 - Incident-Übergänge
 - Problemübergänge
 - Anfrageübergänge

Die Übergangsliste wird angezeigt.

2. Wählen Sie auf der Übergänge-Listenseite die Option "Filter anzeigen".
Im oberen Teil der Seite werden weitere Suchfelder angezeigt.
3. Wählen Sie im Feld "Datensatzstatus" die Option "Inaktiv", und klicken Sie auf "Suchen".
Die Übergangsliste unten auf der Seite zeigt alle inaktiven Übergänge an.
4. Öffnen Sie den Übergang zum Bearbeiten.
5. Wählen Sie in der Dropdown-Liste die Option "Aktiv".
6. Klicken Sie auf "Speichern" und "Fenster schließen".
7. Klicken Sie auf "Suche".
In der Übergangsliste wird der aktive Übergang angezeigt.

Hinweis: Weitere Informationen zu Statusübergängen finden Sie im *Administrationshandbuch* und der *Online-Hilfe*.

Aktivieren von Übergangstypen

Da alle mit dem Produkt gelieferten vordefinierten Übergangstypen standardmäßig inaktiv sind, sind keine Statusübergangsschaltflächen aktiviert. Sie können diese Übergangstypen aktivieren und ändern, um sie dem gewünschten Statusübergangsablauf anzupassen.

So aktivieren Sie einen 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 Übergangstyp und wählen Sie im Menü die Option "Bearbeiten".
4. Wählen Sie in der Dropdown-Liste 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.

Anpassen der Bereiche für funktionalen Zugriff

Ein *funktionaler Zugriffsbereich* ist eine Gruppe von Objekten, mit denen Sie Anwenderzugriff einschränken können. In Vorgängerversionen von CA SDM gab es acht feste funktionale Zugriffsgruppen, um den Zugriff auf Codekomponenten zu beschränken.

Während der Migration migrieren die funktionalen Zugriffsgruppen zu neuen funktionalen Zugriffsbereichen für jede Rolle. Bei der Migration werden die Majic-Änderungen, die Standardbezugsdaten und die Rollenzuweisung zu den neuen funktionalen Zugriffsbereichen automatisch bearbeitet.

Nach der Migration haben Sie die Möglichkeit, die folgenden Aktionen auszuführen:

- Prüfen Sie, wie die Objekte den vorhandenen und neuen funktionalen Zugriffsbereichen und die Rollenberechtigungen den einzelnen Bereichen zugeordnet sind. Verwenden Sie Web Screen Painter, um die funktionalen Zugriffsbereiche zu überprüfen.
- Verwenden Sie CA SDM, um Berechtigungen neu zuzuordnen oder zu ändern. Stellen Sie sicher, dass Anwender den richtigen Zugriff auf Funktionen und Objekte haben.

Hinweis Einzelheiten zu Standardberechtigungen und der Zuordnung von Objekten zu den neuen funktionalen Zugriffsbereichen finden Sie auf der Produktsupport-Website. Informationen zum Ändern oder Hinzufügen von funktionalen Zugriffsbereichen finden Sie in der *Online-Hilfe*.

In der folgenden Tabelle werden funktionale Zugriffsbereiche Codekomponenten zugeordnet:

Funktionaler Zugriffsbereich	Codekomponente	Neu
Administration	admin	No
Incident/Problem/Request	call_mgr	No
Change	change_mgr	No
Inventar	inventory	No
Issue	issue_mgr	No
Knowledge-Dokument	kd	No
Benachrichtigung	notify	No
Referenz	Referenz	No
Sicherheit	security	No
Ankündigung	Ankündigung	Ja

Incident-/Problem-/Request-Referenz	call_mgr_reference	Ja
Incident-/Problem-/Request-Vorlage	call_mgr_template	Ja
Change-Vorlage	change_mgr_template	Ja
Change-Referenz	change_reference	Ja
Configuration Item	ci	Ja
Configuration-Item-Gemeinsamkeit	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
Benachrichtigungsreferenz	notification_reference	Ja
Organisation	organization	Ja
Priorisierung	Priorisierung	Ja
Service-Ebene	service_level	Ja
Site	Standort	Ja
Gespeicherte Abfrage	stored_queries	Ja
Survey	Umfrage	Ja
Mandanten-Admin	tenant_admin	Ja
Zeitzone	timezone	Ja
Workflow-Referenz	workflow_reference	Ja
Schicht	Schichten	Ja

Geänderte Zugriffsebenen nach der Migration

Nach der Migration können Sie die funktionalen Zugriffsebenen für jede Rolle überprüfen. Da die Objekte in andere funktionale Zugriffsbereiche verschoben wurden, kann es vorkommen, dass Benutzer in einigen Situationen auf Bildschirme zugreifen können, zu denen ihnen zuvor der Zugriff verweigert wurde. Ebenso kann ihnen der Zugriff auf Formulare verweigert werden, die ihnen vorher zugänglich waren. Beide Situationen können auftreten, wenn ein neuer funktionaler Zugriffsbereich Berechtigungen für zwei der ursprünglichen funktionalen Zugriffsbereiche verwaltet.

Hinweis Einzelheiten zu Standardberechtigungen und der Zuordnung von Objekten zu den neuen funktionalen Zugriffsbereichen finden Sie auf der Produktsupport-Website. Informationen zum Ändern oder Hinzufügen von Zugriffsebenen finden Sie in der *Online-Hilfe*.

Die Datei SITEMODS.JS

Die Codezeilen, die der Datei "sitemods.js" in der früheren Version hinzugefügt und von einer HTML-Seite aufgerufen wurden, müssen mit der aktuellen "sitemods.js"-Datei zusammengeführt werden, bevor der Code funktionieren kann.

Anpassen von Zugriffstypen

Bei Verwendung von benutzerdefinierten Zugriffstypen und Datenpartitionen in der Vorgängerversion von CA SDM können nach der Aktualisierung Probleme mit den Einstellungen für die Knowledge Management-Datenpartitionen auftreten. Dadurch können weitere Probleme mit den Berechtigungsgruppen-Einstellungen für Kategorien und Dokumente entstehen. Beispielsweise erhält ein Benutzer Zugriff auf eingeschränkte Informationen.

Hinweis: Selbst wenn Sie eine Datenpartition oder einen Zugriffstyp nach dem Löschen neu erstellt haben, müssen Sie Ihre Einstellungen für Zugriffstyp und Datenpartition nach der Aktualisierung überprüfen.

So passen Sie Zugriffstypen an:

1. Klicken Sie auf die Registerkarte "Verwaltung".
Die Seite "Administration" wird angezeigt.
2. Klicken Sie auf "Sicherheits- und Rollenmanagement" > "Rollenmanagement" > "Rollenliste".
Die Rollenliste wird angezeigt.

3. Führen Sie für jede Rolle die folgenden Schritte durch:
 - a. Klicken Sie mit der rechten Maustaste auf die Rolle, und wählen Sie "Bearbeiten" aus.
 - b. Überprüfen Sie das Feld "Name der Datenpartition" unter der Registerkarte "Autorisierung".

Wenn dieses Feld leer ist, ist dem ausgewählten Zugriffstyp keine Datenpartition zugewiesen. Dies bedeutet, es bestehen keine Einschränkungen für den Benutzer, und er kann auf alle Dokumente oder Kategorien im Produkt zugreifen, selbst wenn Sie Berechtigungsgruppen eingerichtet haben.

Diese Aktion ist eventuell für Administratoren angemessen, jedoch nicht für alle Rollen. Wenn der Rolle keine Datenpartition zugewiesen ist, können Sie eine erstellen oder ändern.

Anpassen von Datenpartitionseinstellungen

Sie können Partitionseinschränkungen einstellen, nachdem Sie die Rollen in Ihrem System konfiguriert haben. Die Partitionseinschränkungen werden eingestellt, um zu überprüfen, dass die entsprechenden Genehmigungen richtig funktionieren, nachdem Sie auf die aktuelle Version des Produkts aktualisiert haben.

So stellen Sie Datenpartitionseinschränkungen ein:

1. Wählen Sie auf der Registerkarte "Administration" die Option "Sicherheits- und Rollenmanagement" > "Datenpartitionen" > "Datenpartitionseinschränkungen".
Die Seite "Datenpartitionseinschränkungen - Liste" wird geöffnet.
2. Überprüfen Sie die Einstellungen für die Majic-Codeeinschränkungen für die folgenden Tabellen:

SKELETONS

Gibt die Tabelle an, die für Knowledge-Dokumente verwendet wird.

O_INDEXES

Gibt die Tabelle an, die für Knowledge-Kategorien verwendet wird.

Die Tabelleneinschränkungseinstellungen werden überprüft.

3. Klicken Sie auf "Filter anzeigen", und geben Sie die vorher verwendeten Datenpartitionen ein.

Hinweis: Sie können das Feld "Tabellenname" im Suchbereich verwenden, um die Liste zu begrenzen. Sie können z. B. "*SKELETONS*" oder "*O_INDEXES*" im Feld "Tabellenname" eingeben und auf die Schaltfläche "Suchen" klicken.

Ändern von Helpsets nach der Aktualisierung der Rollen

Nach einer Aktualisierung stellt CA SDM allen migrierten Rollen die vollständige *Online-Hilfe* bereit. Die Helpsets können Sie für alle Rollen entsprechend der Anforderungen Ihres Online-Hilfesystems ändern.

So ändern Sie Helpsets für eine Rolle:

1. Gehen Sie auf der Registerkarte "Administration" zu "Sicherheits- und Rollenmanagement" > "Rollenliste".
Die Seite "Rollenliste" wird angezeigt.
2. Öffnen Sie die gewünschte Rolle, um sie zu ändern (z. B. *Kunde*).
Die Seite "Rolle - Detail" wird angezeigt.
3. Klicken Sie auf "Bearbeiten".
4. Wählen Sie die Registerkarte "Web-Schnittstelle".
Klicken Sie auf "Hilfeansicht".
Die Liste der verfügbaren Helpsets für die ausgewählte Rolle wird angezeigt.
5. Wählen Sie ein Helpset, wie beispielsweise "Kunde", aus.
6. Speichern Sie die Rolle.
Die Hilfeansicht für die Rolle ändert sich entsprechend des ausgewählten Helpsets.

Sie können auch die unter einem Online-Helpset verfügbaren Themen anzeigen. Dazu wählen Sie das Helpsetdetail aus und klicken auf die Schaltfläche "Hilfe anzeigen".

Standardeinstellungen für Einschränkungen

Nachfolgend werden die typischen Standardeinstellungen für Einschränkungen aufgeführt:

Einschränkungseinstellungen bei Datenpartitionen für z. B. Kunden und Mitarbeiter

Die Einschränkungseinstellungen bei Datenpartitionen für z. B. Kunden und Mitarbeiter sollten wie folgt lauten:

Tabelle „SKELETONS“

Ansichtsbeschränkung:

'SKELETONS READ_PGROUPE in @root.pgroups or READ_PGROUPE.[pgroup]
contained_roles.role in @root.id) and ACTIVE_STATE = 0'

Vor-Aktualisierungs- und Löscheschränkung:

'id = 0' (id=0 bedeutet kein Zugriff)

Tabelle „O_INDEXES“

Ansichtsbeschränkung:

READ_PGROU in @root.pgroups or READ_PGROU.[pgroup]
 contained_roles.role in @root.id

Vor-Aktualisierungs- und Löscheschränkung:

WRITE_PGROU in @root.pgroups OR WRITE_PGROU.[pgroup]
 contained_roles.role IN @root.role

Einschränkungseinstellungen bei Datenpartitionen für z. B. CA SDM-Analysten, Knowledge Manager und Knowledge-Entwickler

Die Einschränkungseinstellungen bei Datenpartitionen für z. B. CA SDM-Analysten, Knowledge Manager und Knowledge-Entwickler sollten wie folgt lauten:

Tabelle „SKELETONS“

Ansichtsbeschränkung:

(ACTIVE_STATE >= 0)and (READ_PGROU in @root.pgroups or
 READ_PGROU.[pgroup] contained_roles.role in @root.id) OR (ACTIVE_STATE
 > 0 AND ASSIGNEE_ID = @root.id) OR (ACTIVE_STATE = 0 AND OWNER_ID =
 @root.id)) Active

Vor-Aktualisierungs- und Löscheschränkung:

(ACTIVE_STATE >= 0) AND (WRITE_PGROU in @root.pgroups OR
 WRITE_PGROU.[pgroup] contained_roles.role IN @root.role) OR
 (ACTIVE_STATE > 0 AND ASSIGNEE_ID = @root.id) OR (ACTIVE_STATE = 0 AND
 OWNER_ID= @root.id)) Active

Tabelle „O_INDEXES“

Ansichtsbeschränkung:

READ_PGROU in @root.pgroups or READ_PGROU.[pgroup]
 contained_roles.role in @root.id

Vor-Aktualisierungs- und Löscheschränkung:

WRITE_PGROU in @root.pgroups OR WRITE_PGROU.[pgroup]
 contained_roles.role IN @root.role

Starten der IIS-Web-Schnittstelle (CAisd)

Nach der Aktualisierung von CA SDM r11.2 unter Windows mit integrierten IIS wird die CA SDM-IIS-Web-Schnittstelle (CAisd) beendet. Wenn Sie die IIS-Integration weiterhin nutzen möchten, müssen Sie CAisd nach der Aktualisierung manuell starten.

Wichtig! Wenn Sie IIS 7.0 nutzen wollen, *müssen* Sie das CGI und Metabase Compatability-Komponenten installieren.

Ändern von angepassten HTML-Formularen

Nachdem Sie CA SDM aktualisiert haben, ändern Sie alle angepassten HTML-Formulare, die zuvor Steuerungen für Notizbücher enthielten, um die Webmakros einzuschließen und korrekte Registerkartengruppennamen anzugeben.

Verwenden Sie WSP für jedes angepasste Formular, um die <PDM_NOTEBOOK>-Anweisung auf die <PDM_MACRO name=startNotebook>- und <PDM_TAB>-Anweisungen in <PDM_MACRO name=TAB> zu ändern.

Hinweis: Weitere Informationen über die Verwendung von WSP finden Sie in der *Online-Hilfe zum Web Screen Painter*.

Weitere Informationen:

[Ändern einer Datenrasterliste auf einem Listenformular](#) (siehe Seite 427)

[Ändern von Notizbüchern auf einem Detailformular](#) (siehe Seite 429)

Aktualisieren von Knowledge Management von Version r11.2

Beim Aktualisieren auf CA SDM r12.9 von r11.2 wird die Knowledge Management-Umgebung automatisch aktualisiert. Sobald die Aktualisierung abgeschlossen ist, führen Sie die folgenden Schritte durch:

1. Ordnen Sie die in einer Lösung eines Dokuments erstellten Verknüpfungen der Datenbank zu, um fehlerhafte Verknüpfungen zu lokalisieren.

Hinweis: Um fehlerhafte Verknüpfungen zu finden, verwenden Sie die Richtlinie *Fehlerhafte Verknüpfungen markieren*.

2. Wählen Sie "Knowledge", "Automatisierungsrichtlinien", "Ablaufplanung" auf der Registerkarte "Verwaltung".

Die Seite "Automatisierungsrichtlinien" wird angezeigt.

3. Aktivieren Sie das Kontrollkästchen "Automatisierungsrichtlinien berechnen".
4. Wählen Sie das Zeitintervall aus, um die Berechnung vorzunehmen und die Berechnung durchzuführen. Klicken Sie anschließend auf "Speichern".

Die Richtlinien werden zum angegebenen Datum und zur festgelegten Uhrzeit verarbeitet.

5. Wählen Sie "Knowledge", "Systeme", "Allgemeine Einstellungen" auf der Registerkarte "Verwaltung" aus.

Die Seite "System" wird geöffnet.

6. Geben Sie die folgenden Informationen an:

Pfad für EBR-Indexdateien

Definiert den Speicherort für das Speichern der EBR-Indexdateien. CA SDM erstellt EBR-Indexdateien, wenn Sie ein beliebiges Knowledge-Dokument speichern und veröffentlichen. Beachten Sie abhängig von Ihrem Konfigurationstyp die folgenden Punkte, wenn Sie den EBR-Indexdateipfad definieren:

- Konventionell: Wenn Sie ein Upgrade von CA SDM r12.9 von r11.2 oder r12.X durchführen, können Sie auswählen, den freigegebenen UNC-Pfad nicht zu verwenden. Wenn Sie keinen UNC-Pfad erstellt haben, verwendet CA SDM den standardmäßigen Pfad, um EBR-Indexdateien zu speichern. Wenn Sie ein freigegebenes UNC-Laufwerk verwenden, dann kopieren Sie den Ordner "ebr/ebr_ADM" manuell vom standardmäßigen Speicherort (\$NX_ROOT/site/) in den freigegebenen UNC-Pfad.
- Erweiterte Verfügbarkeit: Wenn Sie ein Upgrade auf eine Konfiguration für erweiterte Verfügbarkeit von CA SDM r11.2 oder r12.X durchführen, dann müssen Sie den freigegebenen UNC-Pfad erstellen und diesen verwenden, um EBR-Indexdateien zu speichern. Die UNC-Daten sind für den Standardpfad nicht erforderlich. Nachdem Sie ein UNC-Laufwerk erstellt haben, kopieren Sie den Ordner "ebr/ebr_ADM" manuell vom standardmäßigen Speicherort (\$NX_ROOT/site/) in den freigegebenen UNC-Pfad.

Wichtig! Der Pfad der EBR-Indexdateien und der KEIT-Dateien müssen sich auf die gleichen UNC-Daten beziehen, und der Pfad muss sich auf dem gleichen Server befinden, um dies zu unterstützen.

Standard: \$NX_ROOT/site/ebr

Pfad für Knowledge-Import-/Exportdateien

Definiert den Speicherort, in dem KEIT-Import-/Exportpakete während eines Import-/Exportvorgangs gespeichert werden. Beachten Sie abhängig von Ihrem Konfigurationstyp die folgenden Punkte, wenn Sie den KEIT-Dateipfad definieren:

- Konventionell: Wenn Sie ein Upgrade auf CA SDM r12.9 von r11.2 oder r12.X durchführen, können Sie auswählen, den freigegebenen UNC-Pfad nicht zu verwenden. Wenn Sie keinen UNC-Pfad erstellt haben, verwendet CA SDM den standardmäßigen Pfad, um die KEIT-Dateien zu speichern. Wenn Sie ein freigegebenes UNC-Laufwerk verwenden, dann kopieren Sie die Paketordner "Import/Export" manuell vom standardmäßigen Speicherort (\$NX_ROOT/site/keit) in den freigegebenen UNC-Pfad.

- **Erweiterte Verfügbarkeit:** Wenn Sie ein Upgrade auf eine Konfiguration für erweiterte Verfügbarkeit von CA SDM r11.2 oder r12.X durchführen, dann müssen Sie den freigegebenen UNC-Pfad erstellen und diesen verwenden, um KEIT-Dateien zu speichern. Die UNC-Daten sind für den Standardpfad nicht erforderlich. Nachdem Sie ein UNC-Laufwerk erstellt haben, kopieren Sie die Paketordner "Import/Export" manuell vom standardmäßigen Speicherort (\$NX_ROOT/site/keit) in den freigegebenen UNC-Pfad.

Wichtig! Der Pfad der EBR-Indexdateien und der KEIT-Dateien müssen sich auf die gleichen UNC-Daten beziehen, und der Pfad muss sich auf dem gleichen Server befinden, um dies zu unterstützen.

Standard: \$NX_ROOT/site/keit

UNC-Daten

Sie können diese Option verwenden, um UNC-Daten für den Zugriff auf das freigegebene Netzlaufwerk zu erstellen, um auf EBR-Indexdateien und Import-/Exportpakete zuzugreifen. Verwenden Sie die Verknüpfung "UNC-Daten", um die UNC-Daten zu erstellen.

Hinweis: UNC-Pfade und UNC-Daten sind bei der Konfiguration für erweiterte Verfügbarkeit erforderlich. Starten Sie den CA SDM-Service neu, wenn Sie die UNC-Details ändern (UNC-Pfade oder UNC-Daten). Weitere Informationen über das Erstellen von UNC-Daten finden Sie in der *Online-Hilfe*.

7. Führen Sie "pdm_k_reindex" wie folgt aus:

pdm_k_reindex -pm

Legt die Dokumentverknüpfungen und eingebetteten Bilder im Lösungsfeld fest.

Wichtig! Nach der Aktualisierung kann ein kritischer Fehler auftreten, wenn "pdm_k_reindex -pm" ausgeführt wird. Wenn Sie diesen Fehler erhalten, gehen Sie zu "Knowledge", "Manager für den Genehmigungsvorgang", "Einstellungen für den Genehmigungsvorgang", und ändern Sie die Option "Berechtigungen zum Bearbeiten von Dokumenten nach der Veröffentlichung" zu "Anwender mit vollen Berechtigungen können Dokumente bearbeiten". Führen Sie dann "pdm_k_reindex" aus.

pdm_k_reindex -ml

Legt die Dokumentverknüpfungen im Lösungsfeld fest und ordnet sie der Datenbank zu.

pdm_k_reindex

Indiziert die Dokumente, damit in Ihrer Knowledge-Umgebung danach gesucht werden kann.

Die Knowledge Management-Umgebung ist nun auf r12.9 aktualisiert.

Hinweis: Nach der Aktualisierung kann es vorkommen, dass beim Drucken von Knowledge-Dokumenten nach dem Lösungsabschnitt im Dokument ein großer Leerraum eingefügt wird. Die Ursache für diesen Leerraum ist ein Problem beim Aktualisieren von Dokumentvorlagen aus einer früheren Version. Weitere Informationen zum Beheben dieses Druckproblems finden Sie in den *Versionshinweisen*.

Wichtig! Nach der Aktualisierung verwenden Knowledge Management-Benachrichtigungsdaten aus früheren Versionen von CA SDM die r12.9-Benachrichtigungs-Engine. Es gibt beispielsweise Standardaktivitätsbenachrichtigungen und Benachrichtigungsregeln für Objekttypen wie die Knowledge-Berichtskarte.

So aktualisieren Sie Knowledge Management von CA SDM r12.x.

Beim Aktualisieren auf CA SDM r12.9 von r12 oder r12.1 wird automatisch die Knowledge Management-Umgebung aktualisiert. Sobald die Aktualisierung abgeschlossen ist, führen Sie die folgenden Schritte durch:

1. Ordnen Sie die in einer Lösung eines Dokuments erstellten Verknüpfungen der Datenbank zu, um fehlerhafte Verknüpfungen zu lokalisieren.

Hinweis: Um fehlerhafte Verknüpfungen zu finden, verwenden Sie die Richtlinie *Fehlerhafte Verknüpfungen markieren*.

2. Wählen Sie auf der Registerkarte "Administration" die Option "Knowledge" > "Automatisierungsrichtlinien" > "Richtlinien" > "Zeitplanung" aus.

Die Seite "Ablaufplanung" wird angezeigt.

3. Aktivieren Sie das Kontrollkästchen "Berechnung ausführen" im Feld "Letzte Aktualisierung".
4. Geben Sie ein Datum in das Textfeld für die Zeitplanung ein, oder klicken Sie auf das Kalendersymbol, um ein Datum auszuwählen.
5. Wählen Sie das Zeitintervall aus, um die Berechnung vorzunehmen und die Richtlinien auszuführen.
6. Klicken Sie auf "Speichern".

Die Richtlinien werden zum angegebenen Datum und der festgelegten Uhrzeit verarbeitet.

7. Navigieren Sie auf der Registerkarte "Administration" zu "Knowledge", "Systeme", "Allgemeine Einstellungen".

Die Seite "Allgemeine Einstellungen" wird geöffnet.

8. Geben Sie die folgenden Informationen an:

Pfad für EBR-Indexdateien

Definiert den Speicherort für das Speichern der EBR-Indexdateien. CA SDM erstellt EBR-Indexdateien, wenn Sie ein beliebiges Knowledge-Dokument speichern und veröffentlichen. Beachten Sie abhängig von Ihrem Konfigurationstyp die folgenden Punkte, wenn Sie den EBR-Indexdateipfad definieren:

- Konventionell: Wenn Sie ein Upgrade von CA SDM r12.9 von r11.2 oder r12.X durchführen, können Sie auswählen, den freigegebenen UNC-Pfad nicht zu verwenden. Wenn Sie keinen UNC-Pfad erstellt haben, verwendet CA SDM den standardmäßigen Pfad, um EBR-Indexdateien zu speichern. Wenn Sie ein freigegebenes UNC-Laufwerk verwenden, dann kopieren Sie den Ordner "ebr/ebr_ADM" manuell vom standardmäßigen Speicherort (\$NX_ROOT/site/) in den freigegebenen UNC-Pfad.
- Erweiterte Verfügbarkeit: Wenn Sie ein Upgrade auf eine Konfiguration für erweiterte Verfügbarkeit von CA SDM r11.2 oder r12.X durchführen, dann müssen Sie den freigegebenen UNC-Pfad erstellen und diesen verwenden, um EBR-Indexdateien zu speichern. Die UNC-Daten sind für den Standardpfad nicht erforderlich. Nachdem Sie ein UNC-Laufwerk erstellt haben, kopieren Sie den Ordner "ebr/ebr_ADM" manuell vom standardmäßigen Speicherort (\$NX_ROOT/site/) in den freigegebenen UNC-Pfad.

Wichtig! Der Pfad der EBR-Indexdateien und der KEIT-Dateien müssen sich auf die gleichen UNC-Daten beziehen, und der Pfad muss sich auf dem gleichen Server befinden, um dies zu unterstützen.

Standard: \$NX_ROOT/site/ebr

Pfad für Knowledge-Import-/Exportdateien

Definiert den Speicherort, in dem KEIT-Import-/Exportpakete während eines Import-/Exportvorgangs gespeichert werden. Beachten Sie abhängig von Ihrem Konfigurationstyp die folgenden Punkte, wenn Sie den KEIT-Dateipfad definieren:

- Konventionell: Wenn Sie ein Upgrade auf CA SDM r12.9 von r11.2 oder r12.X durchführen, können Sie auswählen, den freigegebenen UNC-Pfad nicht zu verwenden. Wenn Sie keinen UNC-Pfad erstellt haben, verwendet CA SDM den standardmäßigen Pfad, um die KEIT-Dateien zu speichern. Wenn Sie ein freigegebenes UNC-Laufwerk verwenden, dann kopieren Sie die Paketordner "Import/Export" manuell vom standardmäßigen Speicherort (\$NX_ROOT/site/keit) in den freigegebenen UNC-Pfad.

- **Erweiterte Verfügbarkeit:** Wenn Sie ein Upgrade auf eine Konfiguration für erweiterte Verfügbarkeit von CA SDM r11.2 oder r12.X durchführen, dann müssen Sie den freigegebenen UNC-Pfad erstellen und diesen verwenden, um KEIT-Dateien zu speichern. Die UNC-Daten sind für den Standardpfad nicht erforderlich. Nachdem Sie ein UNC-Laufwerk erstellt haben, kopieren Sie die Paketordner "Import/Export" manuell vom standardmäßigen Speicherort (\$NX_ROOT/site/keit) in den freigegebenen UNC-Pfad.

Wichtig! Der Pfad der EBR-Indexdateien und der KEIT-Dateien müssen sich auf die gleichen UNC-Daten beziehen, und der Pfad muss sich auf dem gleichen Server befinden, um dies zu unterstützen.

Standard: \$NX_ROOT/site/keit

UNC-Daten

Sie können diese Option verwenden, um UNC-Daten für den Zugriff auf das freigegebene Netzlaufwerk zu erstellen, um auf EBR-Indexdateien und Import-/Exportpakete zuzugreifen. Verwenden Sie die Verknüpfung "UNC-Daten", um die UNC-Daten zu erstellen.

Hinweis: UNC-Pfade und UNC-Daten sind bei der Konfiguration für erweiterte Verfügbarkeit erforderlich. Starten Sie den CA SDM-Service neu, wenn Sie die UNC-Details ändern (UNC-Pfade oder UNC-Daten). Weitere Informationen über das Erstellen von UNC-Daten finden Sie in der *Online-Hilfe*.

9. (Für Schlüsselwortsuchimplementierungen) Geben Sie den folgenden Befehl an der Eingabeaufforderung ein:

```
pdm_k_reindex factory:all
```

Wichtig! Die Variable *all* unterscheidet zwischen Groß- und Kleinschreibung. Wenn Sie "factory:ALL" verwenden, werden Fehler in den Protokolldateien angezeigt.

Die Knowledge Management-Umgebung ist nun auf r12.9 aktualisiert.

Hinweis: Nach der Aktualisierung kann es vorkommen, dass beim Drucken von Knowledge-Dokumenten nach dem Lösungsabschnitt im Dokument ein großer Leerraum eingefügt wird. Die Ursache für diesen Leerraum ist ein Problem beim Aktualisieren von Dokumentvorlagen aus einer früheren Version. Weitere Informationen zum Beheben dieses Druckproblems finden Sie in den *Versionshinweisen*.

Wichtig! Nach der Aktualisierung verwenden Knowledge Management-Benachrichtigungsdaten aus früheren Versionen von CA SDM die r12.9-Benachrichtigungs-Engine. Es gibt beispielsweise Standardaktivitätsbenachrichtigungen und Benachrichtigungsregeln für Objekttypen wie die Knowledge-Berichtskarte.

Kapitel 3: Planung

Dieses Kapitel enthält folgende Themen:

- [Standardports und empfohlene Ports für CA SDM](#) (siehe Seite 85)
- [So planen Sie für erweiterte Verfügbarkeit](#) (siehe Seite 88)
- [Planen der CA MDB-Installation](#) (siehe Seite 99)
- [Planen der CA SDM-Installation](#) (siehe Seite 102)
- [Planen der Installation von CA NSM](#) (siehe Seite 116)
- [Planen der Installation von CA EEM und CA Workflow](#) (siehe Seite 116)
- [Planen der Integration von CA Process Automation](#) (siehe Seite 123)
- [Installationsplanung für CA Business Intelligence](#) (siehe Seite 128)
- [Implementierungsstrategien](#) (siehe Seite 134)
- [Aktivieren der Windows-Authentifizierung in Firefox](#) (siehe Seite 135)

Standardports und empfohlene Ports für CA SDM

Für die Installation von CA SDM müssen verschiedene Ports und Portnummernbereiche in der Firewall geöffnet werden. Die Port-Informationen unterstützen Sicherheits- und Systemadministratoren bei der Installation und Konfiguration von CA SDM sowie bei der Integration von weiteren CA Technologies-Lösungen oder Produkten anderer Hersteller.

Welche offenen Ports in Ihrer Firewall vorhanden sein müssen, hängt von den Einstellungen in der Datei *NX.env* ab. Standardmäßig wählt CA SDM den entsprechenden Port je nach Verfügbarkeit. Das System reserviert Ports mit Nummern unter 1024, kann aber auch hohe Portnummern wie z. B. 65335 anfordern.

Die folgenden *NX.env*-Variablen legen den Anfangs- (2100) und die inkrementale Erhöhung (plus 1) fest, die das System beim Suchen nach einem offenen Port verwendet, um den Prozess starten zu können:

- `NX_SLUMP_FIXED_SOCKETS=1`
- `NX_SLUMP_SECONDARY_SOCKET=2100`

In der folgenden Liste sind die Standardports und empfohlenen Ports (und Portnummernbereiche) für eine typische CA SDM-Installation aufgeführt:

Datenbank

- Oracle: 1521
- SQL Server: 1433

CA SDM

- FTP: 21
- SMTP: 25

- HTTP: 80
- HTTPS: 8080
- HTTPS (sekundär): 8081
- POP3: 110
- IMAP: 143
- LDAP: 389
- WebEx: 1270
- mstsc: 1389
- oaserver: 1706
- Slump Socket: 2100
- qserver: 2234
- Proctor Socket: 2300
- Kommunikation: 2365
- Apache Tomcat: 8080
- Apache Tomcat Shutdown:
- SSL auf Apache Tomcat: 8443

CA CMDB

- Visualizer: 9080
- Visualizer Apache Tomcat Shutdown: 9085
- CA Cohesion ACM: 9000
- CA Cohesion ACM Tomcat Shutdown: 9005

CA EEM

Administrationsport: 5250

CA Workflow

- Apache Tomcat: 8090
- Apache Tomcat Shutdown: 8095

REST

- Apache Tomcat: 8050
- Apache Tomcat Shutdown: 8055

CA Business Intelligence

Hinweis: Informationen über das Verwalten von Firewall-Ports für BusinessObjects finden Sie im Bereitstellungs- und Konfigurationshandbuch zu BusinessObjects Enterprise XI r2.

- Apache Tomcat: 8080
- **Empfohlen:** 8070
- Apache Tomcat Redirect: 8443
- Apache Tomcat Shutdown: 8075
- Sekundärer Apache Tomcat Shutdown: 8005
- ODBC-Treiber: 1706
- BusinessObjects Central Management Server (CMS): 8080
- BusinessObjects Application Server: 6400
- ODBC DSN (OpenAccess-Datenbank): 1706
- BEA WebLogic: 7001

EBR-Suche

- Basisport: 13000

Portal-Server

- Apache Tomcat: 8080
- Apache Tomcat Shutdown: 8085
- SSL-Funktionalität: 8443
- Portal_Safe_List: 8444

Support-Automatisierung

- Main Server (Socket Server) Intern: 7005
- Main Server (Socket Server) Extern: 10443
- Socket-Proxy-Server (Socket-Konfiguration Main Server) Intern: 7005
- Socket-Proxy-Server (Socket-Konfiguration Main Server) Extern: 10444
- Routing-Server für Meldungen (Socket-Konfiguration) Extern: 10444
- Apache Tomcat: 8070
- Apache Tomcat Shutdown: 8075

Visualizer

- Apache Tomcat: 9080
- Apache Tomcat Shutdown: 9085

So planen Sie für erweiterte Verfügbarkeit

Erweiterte Verfügbarkeit ist ein Konfigurationsmodell, das verbesserte Ausfallsicherheit bei Serverausfällen und höhere Anwendungsverfügbarkeit bietet sowie eine kontinuierliche Wartung mit minimalen Unterbrechungen für Endanwender unterstützt. Diese Konfiguration erfordert einen Hintergrundserver, einen oder mehrere Standby-Server sowie einen oder mehrere Anwendungsserver. Die vorherige Konfiguration mit Primärservern und Sekundärservern ist jetzt als konventionelle Konfiguration bekannt.

Sie können CA SDM konfigurieren, um entweder eine konventionelle Konfiguration oder eine Konfiguration für erweiterte Verfügbarkeit zu verwenden. Sie können auch von einer Konfiguration in eine andere Konfiguration konvertieren.

Die Konfiguration für erweiterte Verfügbarkeit verbessert die allgemeine Verfügbarkeit von CA SDM auf folgende Weise:

- Minimiert die Ausfälle der CA SDM-Anwendung, die sich aus Anwendungsfehlern, Hardwarefehlern oder Wartungen ergeben, indem Fehlerquellen reduziert werden.
- Minimiert die CA SDM-Ausfallzeit, indem die parallele Wartung von Servern unterstützt wird. Das bedeutet, die Anwender können weiter in der Anwendung arbeiten, während einer der Server gewartet wird.

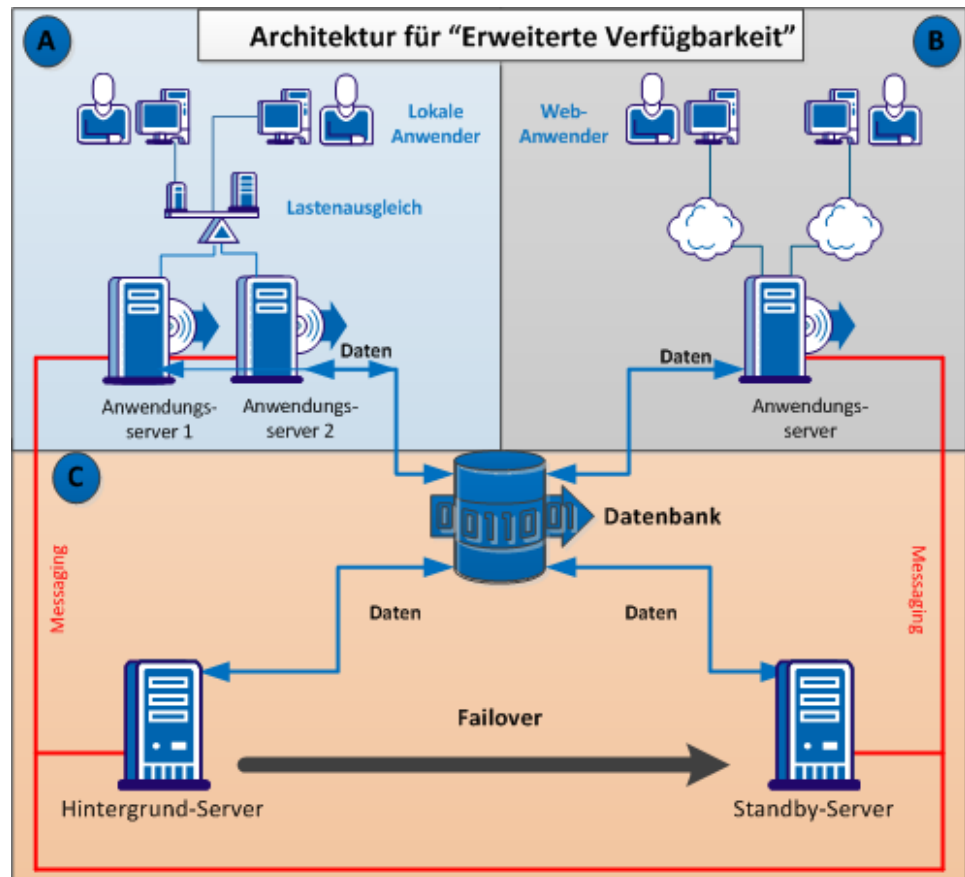
Weitere Informationen zur Planung und Konfiguration der erweiterten Verfügbarkeit finden Sie im *Implementierungshandbuch*, oder verwenden Sie die erweiterten Verfügbarkeitszenarien direkt vom Bookshelf.

Stellen Sie sicher, dass Sie folgende Planungsüberlegungen überprüfen, bevor Sie die Konfiguration für erweiterte Verfügbarkeit einrichten:

- [CA SDM-Architektur für erweiterte Verfügbarkeit](#) (siehe Seite 89)
- [Entscheidung zur Konfiguration für erweiterte Verfügbarkeit](#) (siehe Seite 91)
- [Überlegungen zur Konfiguration für erweiterte Verfügbarkeit](#) (siehe Seite 91)

CA SDM-Architektur für erweiterte Verfügbarkeit

Die Konfiguration für erweiterte Verfügbarkeit umfasst einen Hintergrundserver, mindestens einen Standby-Server und mindestens einen Anwendungsserver. Um zentrale Fehlerquellen zu reduzieren, hat jeder dieser Server eine direkte Verbindung zur Datenbank. Alle Komponenten der Architektur kommunizieren mithilfe eines internen CA-Protokolls. Folgendes Diagramm zeigt ein Beispiel der CA SDM-Implementierung:



Die Architektur wird über die drei verschiedenen Lokationen A, B und C verteilt. Lokation A hat zwei Anwendungsserver, die Anwender über einen Lastenausgleich bedienen. Die Lokation B hat einen Anwendungsserver, der die Anwender direkt bedient, und die Lokation C hat den Hintergrundserver, den Standby-Server und die Datenbank. Jeder der Server hat eine direkte Verbindung zur Datenbank. Die blauen Linien markieren den Ablauf zu und von der Datenbank. Die roten Zeilen stellen die interne Kommunikation zwischen den Komponenten dar.

Hintergrundserver

Der Hintergrundserver ist der Architekturkern der erweiterten Verfügbarkeit. Dieser Server stellt zusätzliche Dienste für andere Server bereit und führt alle Singleton-Prozesse von CA SDM aus. Ein Prozess kann als Singleton festgelegt werden, wenn auch nur eine einzige Kopie davon in der SDM-Installation aktiv sein kann. Nur Anwender mit dem Zugriffstyp für Administratoren können auf den Hintergrundserver zugreifen. Um die Verfügbarkeit zu steigern, verfolgt der Standby-Server den Hintergrundserver. Sie können den Standby-Server in den Hintergrundserver wechseln, wenn ein Fehler auftritt oder wenn eine parallele Wartung ausgeführt wird.

Standby-Server

Die Hauptfunktion des Standby-Servers ist es, als betriebsbereiter Standby-Server für den Hintergrundserver zu agieren. Der Standby-Server hat die gleiche Hardware und BS-Plattform wie der Hintergrundserver. Der Standby-Server kann alle Prozesse ausführen, die auf dem Hintergrundserver ausgeführt werden. Der Standby-Server wird während des Normalbetriebs des Systems nicht genutzt. Jedoch wird der kritische Cache-Speicher weiterhin aktualisiert, indem die internen CA SDM-Systemmeldungen auf Datenbankänderungen überwacht werden. Wenn der Hintergrundserver fehlschlägt oder eine parallele Wartung benötigt, können Sie den Standby-Server als Hintergrundserver hochstufen. Dies führt zu einer minimalen Unterbrechung für die Anwendungsserver und Endanwender. Sie können ein Hilfsprogramm aufrufen, um diesen Switchover auszuführen.

Der Standby-Server führt nur eine kleine Teilmenge der Prozesse aus, die normalerweise auf dem Hintergrundserver ausgeführt werden. Sie können sich nicht bei der Webschnittstelle auf dem Standby-Server anmelden.

Anwendungsserver

Der Anwendungsserver hat alle erforderlichen CA SDM-Komponenten, die die Endanwender über verschiedene Schnittstellen wie Web-, SOAP- und RESTful-Webservices verwenden. Die Anwendungsserver sind unabhängig voneinander und für einen kurzen Zeitraum stabil gegenüber den Ausfällen des Hintergrundservers. Anwender greifen auf die Anwendungsserver zu. Sie können die Anwendungsserver individuell entfernen und zum Service zurückkehren, indem Sie die neue Einrichtung zur Stilllegung verwenden. Die Einrichtung zur Stilllegung ermöglicht es den aktuellen Anwendern, ihre Arbeit abzuschließen und sich anschließend auf einem alternativen Anwendungsserver anzumelden.

Entscheidung zur Konfiguration für erweiterte Verfügbarkeit

Die Konfiguration für erweiterte Verfügbarkeit stellt eine höhere Verfügbarkeit bereit, reduziert Ausfallzeiten und unterstützt die parallele Wartung. Sie sollten die Konfiguration für erweiterte Verfügbarkeit in Betracht ziehen, wenn folgende Faktoren zutreffen:

- Sie benötigen ein hohes Maß an CA SDM-Verfügbarkeit.
- Es ist erforderlich, dass die CA SDM-Server unabhängiger und stabiler gegenüber Fehlern sind.
- Sie müssen in der Lage sein, CA SDM-Server zu entfernen und wieder in Betrieb zu nehmen, ohne dabei die gesamte CA SDM-Installation anzuhalten.
- Sie benötigen während der parallelen Wartung eine sehr geringe Ausfallzeit.

Überlegungen zur Konfiguration für erweiterte Verfügbarkeit

Wir empfehlen Ihnen, folgende Punkte zu berücksichtigen, bevor Sie die Konfiguration für erweiterte Verfügbarkeit implementieren:

Allgemeine Hinweise

Alle Planungsüberlegungen der konventionellen Konfiguration sind gültig für die Konfiguration für erweiterte Verfügbarkeit. Weitere Informationen zur Planung konventioneller Konfigurationen finden Sie im *Implementierungshandbuch*.

- Es werden zusätzliche Hardwarekosten erwartet, da Sie einen Hintergrundserver, mindestens einen Standby-Server und mindestens einen Anwendungsserver benötigen. Die Konfiguration des Standby-Servers und des Hintergrundservers muss identisch sein.
- Es ist erforderlich, dass ein Remote-Datenbankserver und ein Server die Indexdateien des Knowledge Tool, die Import-/Exportdateien des Knowledge Tool, die Ausgabedateien der Archivbereinigung und die Anhang-Repositorys gemeinsam nutzen. Um es dem Hintergrundserver und dem Standby-Server zu ermöglichen, auf diese Dateien zuzugreifen, ist ein freigegebener Speicherort erforderlich. Linux- und Unix-Installationen können NFS-Bereitstellungen verwenden. UNC-Support wurde für Windows-Installationen hinzugefügt.

- Es wird erwartet, dass die CA SDM-Leistung auch mit den zusätzlichen Servern für Hintergrund- und Standby-Vorgänge gleich bleibt. Wenn Sie weitere Anwendungsserver bereitstellen, wird sich die Leistung möglicherweise verbessern.
- Jeder der Server ist direkt mit der Datenbank verbunden. Dies führt zu erhöhten Ressourcenkonflikten auf der DBMS-Ebene. Wir empfehlen, die Hardware-Konfiguration des DBMS-Servers zu erhöhen. Weitere Informationen finden Sie in den Systeminformationen.
- Das Konvertieren einer konventionellen Konfiguration in eine Konfiguration für erweiterte Verfügbarkeit ist ein manueller Aufwand. Die größeren Implementierungen sind normalerweise komplexer, und möglicherweise müssen Sie CA Services zur Unterstützung einbeziehen.
- Um zur Konfiguration für erweiterte Verfügbarkeit zu migrieren, führen Sie ein Upgrade auf CA SDM r12.9 in der konventionellen Konfiguration durch, und führen Sie anschließend die Konvertierung zur Konfiguration für erweiterte Verfügbarkeit durch.
- Installieren Sie den Hintergrundserver und den Standby-Server auf dem gleichen Subnetz des Netzwerks, sodass Ping-Zeiten und Latenzen von verschiedenen Anwendungsservern sich ähneln.
- Sie sollten in Betracht ziehen, den Hintergrundserver und den Standby-Server in einer zentralen Lokation mit einer guten Netzwerkverbindung für alle Anwender unterzubringen. Die Anwendungsserver können entweder zentral bereitgestellt werden oder sie können weltweit verteilt werden.
- Eine Konfiguration für erweiterte Verfügbarkeit muss immer einen Hintergrundserver und mindestens einen Standby-Server haben.
 - (Empfohlen) Stellen Sie sicher, dass sowohl die Hintergrundserver als auch alle anderen Standby-Server ähnlich konfiguriert sind. Dieser Vorgang stellt sicher, dass ein Standby-Server, der während eines Failover als neuer Hintergrundserver festgelegt wird, genau wie der alte Hintergrundserver funktioniert.
 - Es kann eine beliebige Anzahl an Standby-Servern konfiguriert werden. Um die CA SDM-Verfügbarkeit zu steigern, sollten Sie in Betracht ziehen, einen Standby-Server in Ihre Datenzentrale der Sicherung oder in den Disaster Recovery-Standort zu platzieren.
 - Die minimale Implementierung der erweiterten Verfügbarkeit benötigt einen Anwendungsserver. Wir empfehlen Ihnen, über zwei Anwendungsserver zu verfügen, um die Verfügbarkeit zu steigern, und Sie sollten über einen Lastenausgleich verfügen, um den Webdatenverkehr zu regeln.
 - Abgesehen von CA SDM-Administratoren dürfen sich keine anderen Anwender beim Hintergrundserver anmelden. Außerdem dürfen sich keine Anwender bei den Standby-Servern anmelden.

- Wir können E-Mail-Benachrichtigungen von allen CA SDM-Servern senden. Es gibt derzeit keine Möglichkeit, diese Option zu beschränken oder zu konfigurieren. Jeder Server in der erweiterten Verfügbarkeitskonfiguration muss eine Verbindung zum Mail-Server haben.
 - Eine E-Mail-Benachrichtigung, die aus einer Endanwenderinteraktion resultiert, wird von dem Anwendungsserver gesendet, an den der Anwender angeschlossen wird.
 - Eine E-Mail-Benachrichtigung aufgrund von Hintergrundvorgängen (wie die Animator-Verarbeitung eines angehängten Ereignisses) werden von dem pdm_mail_nxd-Hilfsprogramm gesendet, das auf dem Hintergrundserver ausgeführt wird.
 - Während eines Hintergrundserverfehlers werden die in der Warteschlange vorhandenen E-Mails gesendet, wenn der Hintergrundserver als Standby-Server hochgefahren wird.

Hinweise zum Failover

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

- Die neuen Anwender können sich nicht anmelden.
- Während des Failovers werden folgende Aktionen bei bereits verbundenen Anwendern nicht funktionieren. Nach dem Failover muss der Anwender versuchen, diese Aktionen erneut durchzuführen:
 - Beim Erstellen von Tickets mit Anhängen.
 - Beim Herunterladen von Anhängen.
 - Suchen nach Knowledge-Dokumenten.
 - Beim Indizieren von neuen Knowledge-Dokumenten.
 - Bei eingehenden E-Mails.
 - Bei SLA-Events, die nicht ausgelöst werden, bis das Failover abgeschlossen ist.
- **Wichtig!** Wenn Sie das Tool eines Drittanbieters so konfiguriert haben, dass Auto-Failover für die CA SDM-Server aktiviert ist, müssen Sie dies deaktivieren, bevor Sie mit der Rolling-Wartung.

Hinweise zur Datenbank

- Eine direkte Verbindung ist zwischen den Servern sowie zur Datenbank vorhanden. Wenn der CA SDM-Server innerhalb DMZ ist, müssen Sie für diese Konnektivität die Firewall-Ports öffnen oder eine Tunneling-Proxy-Technologie implementieren. Beachten Sie auch die Lizenzvereinbarungen mit Ihrem DBMS-Anbieter.
- Stellen Sie sicher, dass der Datenbank-Client auf allen CA SDM-Servern installiert ist.

- In der Konfiguration für erweiterte Verfügbarkeit werden alle Server immer noch mit einer einzelnen Datenbank verbunden. Da die Datenbank eine zentrale Fehlerquelle sein kann, sollten Sie die Vorteile des Datenbank-Clustering nutzen, um die Verfügbarkeit von DBMS zu steigern.
- Microsoft SQL Server wird nur systemeigen auf der Windows-Plattform unterstützt. Wenn Ihre Implementierung zum Beispiel aus Servern mit heterogenen Betriebssystemen wie Windows und Linux besteht, dann wählen Sie "Oracle" als DBMS aus, da Microsoft SQL Server unter Linux nicht unterstützt wird.
- Das pdm_isql-Hilfsprogramm kann nur auf den Anwendungsserver ausgeführt werden.

Systemkonfiguration, Administration und Vorgang

- SOAP-Webservices und RESTful-Webservices werden nur auf den Anwendungsservern unterstützt. Web-Directors können auf allen CA SDM-Servern konfiguriert werden.
- Da die Anwendungsserver unabhängig voneinander sind, können Web-Directors nur Web-Engines bedienen, die auf dem gleichen Anwendungsserver ausgeführt werden. Web-Directors können keine Web-Engines über die Anwendungsserver bedienen.
- Da die Server in der Konfiguration für erweiterte Verfügbarkeit einen höheren Grad an Unabhängigkeit haben, funktionieren die meisten Befehlszeilenprogramme nur auf dem lokalen Server. Zum Beispiel zeigt Ihnen "pdm_status" nur die ausgeführten CA SDM-Prozesse auf dem Server, auf dem Sie den Befehl ausführen. Das Hilfsprogramm "pdm_webcache" aktualisiert nur die Formular-Caches auf dem Server, auf dem es ausgegeben wurde.
- Im Gegensatz zur konventionellen Konfiguration, bei der Sie CA SDM-Prozesse auf dem Primärserver mit "pdm_d_mgr" starten und anhalten, werden bei der erweiterten Verfügbarkeit die Prozesse auf jedem Server unabhängig gesteuert.
- Verwenden Sie den neuen Befehl "pdm_server_control" anstelle des Befehls "pdm_halt", um Anwendungsserver herunterzufahren. Vor dem Herunterfahren können Sie die aktiven Anwender darum bitten, zu einem anderen Anwendungsserver zu wechseln. Dies kann ausgeführt werden, indem man die Anwender mithilfe der Option zur Stilllegung benachrichtigt.
- Das Hilfsprogramm "pdm_edit" wurde durch eine neue grafische Benutzeroberfläche ersetzt, bei der die vielen manuellen Änderungen an der "pdm_d_mgr"-Konfigurationsdatei nicht mehr erforderlich sind.

- In der erweiterten Verfügbarkeitskonfiguration können Sie im Gegensatz zur konventionellen Konfiguration die Option "bopauth_host" vom Optionsmanager der Web-Benutzeroberfläche des Hintergrundservers verwenden, um die Details zum Authentifizierungsserver anzugeben. Für die Konfiguration für erweiterte Verfügbarkeit führen Sie diese Konfigurationsänderung in "pdm_edit" nicht mehr durch. Anwender können sich nicht anmelden, wenn der Authentifizierungsserver nicht verfügbar ist.

Hinweis: Bei der konventionellen Konfiguration können Sie einen Sekundärserver verwenden, um CA SDM mit einem Authentifizierungssystem zu integrieren, das auf einem anderen System oder sogar auf einer anderen Hardware-Plattform ausgeführt wird.

- Um zu verhindern, dass Rogue-Server der Konfiguration für erweiterte Verfügbarkeit beitreten, müssen alle Server über die Web-Schnittstelle des Hintergrundservers angegeben werden, bevor sie konfiguriert werden können.
- Die Rolle und andere Informationen für einen Server in der Konfiguration für erweiterte Verfügbarkeit können auf der Registerkarte "Administration" geändert werden. Halten Sie die CA SDM-Services an, bevor Sie versuchen, eine Serverdefinition zu ändern. Die Neukonfiguration des Servers ist erforderlich, damit die Änderungen wirksam werden.
- Sie können einen Server zwischen der konventionellen Konfiguration und der Konfiguration für erweiterte Verfügbarkeit wechseln, indem Sie das Konfigurationshilfsprogramm ausführen. Stellen Sie sicher, alle Server in der Implementierung zu ändern. Ihre Daten bleiben unverändert, aber die manuellen Aktualisierungen sind erforderlich, um die Einstellungen zu ändern.
- Verwenden Sie die aktuellsten "pdm_startup"-Dateien, während Sie auf CA SDM r12.9 migrieren. Verwenden Sie keine Dateien aus Vorgängerversionen von CA SDM. Zum Beispiel Dateien, die vom Hilfsprogramm "pdm_edit" generiert wurden.
- Es wurden neue Umgebungsvariablen zu "NX.env" hinzugefügt, um die erweiterte Verfügbarkeit zu unterstützen, und das System verwaltet die variablen Werte automatisch.

Wichtig! Ändern Sie "NX.env" nicht manuell, sofern Sie nicht dazu aufgefordert werden.

- Eine neue Einrichtung generiert Ticketnummern und numerische Datensatzschlüssel. Um eine mögliche Datenbankkorruption zu vermeiden, sollten Sie niemals versuchen, die Tabelle "Key_Control" zu laden oder manuell zu ändern.
- Sie können die Knowledge Tools-Daemons nicht auf einen anderen Server in der Konfiguration für erweiterte Verfügbarkeit verschieben. Der "kt_daemon" wird jetzt auf allen Servern ausgeführt. Alle anderen Knowledge Tools-Daemons werden als Singletons auf dem Hintergrundserver ausgeführt.
- Knowledge Tools unterstützen jetzt UNC-Dateipfade unter Windows für den Speicherort der EBR-Indexdateien und der Eingabe-/Ausgabedateien, die von der Einrichtung "Knowledge-Export" bzw. "Knowledge-Import" verwendet werden. Diese Funktion ist sowohl für die erweiterte Verfügbarkeit als auch für die konventionellen Konfigurationen verfügbar.

Wichtig! Der Pfad der EBR-Indexdateien und der KEIT-Dateien müssen sich auf die gleichen UNC-Daten beziehen, und der Pfad muss sich auf dem gleichen Server befinden, um dies zu unterstützen.

- Die Versionskontrolle verteilt die Dateien (zum Beispiel HTMPL, MAJ, MOD und SCH), die in der Datei "server_secondary_custom.ver" vom Hintergrundserver konfiguriert sind. Beim Starten führt der Standby-Server oder der Anwendungsserver den Client der Versionskontrolle aus, um aktualisierte Dateien vom Hintergrundserver abzurufen.
- Archivieren/Löschen wird auf dem Hintergrundserver ausgeführt, und UNC-Dateipfade für Ausgabedateien werden unter Windows unterstützt. Diese Funktion ist für die erweiterte Verfügbarkeit und für die konventionellen Konfigurationen verfügbar.
- Wenn sich das Repository auf einem Remote-Server befindet, werden die Anhänge der eingehenden E-Mails jetzt mit "pdm_maileater" gespeichert.
- Stellen Sie sicher, dass der Daemon-Manager berechtigt ist, die procsets zu ändern; führen Sie nicht den pdm_dmnmode-Befehl für diese Aktion aus.

Allgemeine Hinweise zur Web-Anwenderschnittstelle

- Ein Webserver ist auf allen Servern mit Konfiguration für erweiterte Verfügbarkeit erforderlich.
- Wenn der Hintergrundserver aufgrund eines Failovers nicht verfügbar ist, wird den Web-Anwendern das Formular "Serverantwort verzögert" angezeigt. Anwender können ihre Arbeit fortsetzen, wenn der Standby-Server als Hintergrundserver hochgestuft wird.
- Der Wert der Option "web_cgi_url" muss auf Folgendes verweisen:
 - Auf den Lastenausgleich, wenn Sie mehr als einen Anwendungsserver haben.
 - Auf den Anwendungsserver, wenn Sie nur einen Anwendungsserver haben.

Hinweise zu Anhängen

- Sie können die Verfügbarkeit von Anhängen steigern, indem Sie mehrere Dokument-Repository-Prozesse so konfigurieren, dass auf ein freigegebenes Datei-Repository zugegriffen wird.

Hinweise zur Web Screen Painter

- Sie können Web Screen Painter (WSP) nur auf dem Hintergrundserver verwenden.
- Befolgen Sie das empfohlene Verfahren, um WSP-Formularänderungen zu veröffentlichen, sodass die aktualisierten Formulare auf allen Servern der Installation verteilt werden. Weitere Informationen finden Sie in den Szenarien *So passen Sie das Schema mithilfe von Web Screen Painter an* und *So passen Sie die Web-Schnittstelle mithilfe von Web Screen Painter an*.
- Die Daemons der virtuellen Datenbankebene können auf allen Servern ausgeführt werden. Installieren Sie die CA SDM-Datenbankanpassungen und Objektdefinitionen auf allen Servern.

Hinweise zu Berichten

- CA Business Intelligence kann Daten aus alternativen Anwendungsservern automatisch abrufen. Sie können diese Funktion konfigurieren, um die Verfügbarkeit der CA SDM-Berichterstellung zu steigern.
- BOXI wird nicht mit dem Hintergrundserver integriert. Daher können Sie keine Berichte über die Web-Benutzeroberfläche des Hintergrundservers anzeigen. Eine Fehlermeldung wird angezeigt, wenn Sie die Registerkarte "Berichte" über die Web-Benutzeroberfläche des Hintergrundservers auswählen.

Hinweise zum Optionsmanager

- Mit dem Optionsmanager können Sie Optionen nur über die Web-Benutzeroberfläche des Hintergrundservers installieren oder deinstallieren. Verwenden Sie den Vorgang zur parallelen Wartung, um die Änderungen auf alle Server in der Konfiguration zu übertragen. Weitere Informationen über das Ausführen der parallelen Wartung finden Sie im Szenario *"Ausführen der parallelen Wartung auf dem CA SDM-Server"*.

Hinweise zu Webservices

- Sie können Webservices nur auf den Anwendungsservern konfigurieren.
- Die Option "webservices_domsrvr" ist nicht mehr im Optionsmanager vorhanden. Sie können die Variable "NX_WEBSERVICES_DOMSRVR" unabhängig auf jedem Anwendungsserver konfigurieren, indem Sie "NX.env" ändern.

Allgemeine Hinweise zur Integration

- Die URL zur CA SDM-Web-Anwenderschnittstelle muss auf einen Anwendungsserver verweisen, der ordnungsgemäß konfiguriert ist. Die "ca_application_registration" enthält eine URL zu Ihrer CA SDM-Installation, die von anderen CA-Produkten verwendet wird. Diese URL verweist auf den CA SDM-Server, der zuerst konfiguriert ist. Normalerweise ist dies der Hintergrundserver. Nur die CA SDM-Administratoren können den Wert durch die Administrationseinrichtung ändern. Wenn Sie einen Lastenausgleich verwenden, verweisen Sie diese URL auf den Lastenausgleich anstatt auf einen einzelnen Anwendungsserver. Hinweis: Weitere Informationen finden Sie in der *Online-Hilfe*.
- Die meisten Interaktionen und Integrationen der Endanwender mit anderen Softwareprodukten werden auf Anwendungsserverebene ausgeführt. Es gibt kein Failover für die Anwendungsserver. Wenn der Anwendungsserver nicht verfügbar ist, dann sind die Webservices für den Anwendungsserver auch nicht verfügbar. Um die Anwendungsverfügbarkeit zu steigern, können Sie einen Lastenausgleich bereitstellen, um Requests zwischen verschiedenen Anwendungsservern weiterzuleiten.
- Sie können NSM nur mit einem einzelnen Anwendungsserver integrieren, da die IP-Adressen betroffen werden. Die NSM-Integration ist nicht verfügbar, wenn dieser Server ausgefallen ist.
- CA Workflow muss auf einem der Anwendungsserver installiert werden. Wenn dieser Anwendungsserver ausfällt, ist die CA Workflow-Integration nicht verfügbar.

Weitere Aspekte bei den Umwandlungsfunktionen

- Sie können nur den Hintergrundserver in einen Primärserver konvertieren.
- Sie können nur den Primärserver in einen Hintergrundserver konvertieren.
- Sie können nur den Sekundärserver in einen Standby-Server oder einen Anwendungsserver konvertieren.
- Sie können nur den Standby-Server oder einen Anwendungsserver in den Sekundärserver konvertieren.

Föderierte Such-Überlegungen

- Um die föderierte Suchfunktion zu aktivieren und zu verwenden, wählen Sie die föderierte Suchoption aus, während Sie die Anwendungsserver konfigurieren.

Planen der CA MDB-Installation

Folgende Informationen unterstützen Sie beim Planen einer erfolgreichen CA MDB-Installation und Konfiguration. Damit suchen und erfassen Sie die richtigen Informationen.

- **Suchen:** Lesen Sie die *Übersicht über die Management-Datenbank von CA*, und machen Sie sich mit CA MDB vertraut. Legen Sie dann Ihre Implementierungsstrategie fest, und lesen Sie die Informationen über SQL Server- oder Oracle-Probleme, die Sie kennen sollten, wenn Sie CA MDB mit CA SDM verwenden.
- **SQL Server:** Um sicherzustellen, dass Sie die Software und die zugehörigen Komponenten erfolgreich auf SQL Server konfigurieren können, führen Sie die folgenden Schritte durch:
 - Aktivieren Sie TCP/IP auf dem Computer, auf dem Sie die Installation und die Konfiguration durchführen wollen.
 - Folgende Informationen sollten Sie zur Hand haben:
 - Die genannte Serverinstanz, die SQL Server gerade ausführt.
 - Anwendername und Kennwort des SQL Server-Datenbankanwenders
 - Portnummer der SQL Server-Datenbank.
- **Oracle:** Folgende Informationen sollten Sie zur Hand haben:
 - Handelt es sich um eine lokale oder Remote-Oracle-Datenbank?
 - Müssen Tablespaces erstellt werden?
 - Name des Netzdienstes
 - Anwendername und Kennwort des DBA-Anwenders
 - Name des Daten- und Index-Tablespace
 - Der vollständige Pfad für den Tablespace
 - JDBC-Verbindungsdaten einschließlich der System-IDs (SID) und des Empfangsports

Hinweis: Informationen zu den erforderlichen Eingaben für Ihre Datenbank finden Sie in der *Online-Hilfe zur Serverkonfiguration*.

Weitere Informationen:

[So installieren Sie CA MDB](#) (siehe Seite 156)

Hinweise zu CA MDB

Bevor Sie die CA MDB installieren, lesen Sie die folgenden Informationen, um eine erfolgreiche Implementierung sicherzustellen

- **AIX:** Auf einigen AIX-Rechnern ist der maximal zulässige Speicherplatz der ARG/ENV-Liste zu klein für die Installation der CA MDB. Führen Sie den Befehl *lsattr -lsys0 -ancargs -Fvalue* aus, um die aktuelle Einstellung für die maximal zulässige Größe der ARG/ENV-Liste zu suchen. Ist der zurückgegebene Wert kleiner als 50, erhöhen Sie den Wert durch den folgenden Befehl: *chdev -l sys0 -a ncargs=50*

- **Oracle:** Beachten Sie die folgenden Informationen:

- Führen Sie vor einem CA MDB-Patch eine Oracle-Sicherung durch. Die Sicherung kann von einem Datenbankadministrator oder über ein Patch-Skript ausgeführt werden. Das Patch-Skript verwendet den Oracle Recovery Manager (RMAN), um die Datenbank mit Hilfe der Betriebssystemauthentifizierung zu sichern. Für Ihre RMAN-Konfiguration ist es möglicherweise erforderlich, die Archivprotokollierung (ARCHIVELOG mode) in der Datenbank zu aktivieren. Wenn der DBA eine Sicherung durchgeführt hat, können Sie als Alternative die Sicherung mit Hilfe des Patch-Skripts und der Angabe "no" für den Parameter -ORA_BACKUP unterdrücken.

Hinweis: Bei Patch-Vorgängen wird der RMAN-Befehl mit Betriebssystemauthentifizierung verwendet.

- Der Oracle-Anwender, der die CA MDB-Installation ausführt, muss über die folgenden Datenbank-Administratorrechte verfügen:
 - Die dba-Rolle (verbinden Sie "sys" als "sysdba"; erteilen Sie "dba"-Rechte an "installation_user").
 - Die sysdba-Rolle (verbinden Sie "sys" als "sysdba"; erteilen Sie "sysdba"-Rechte an "installation_user").
 - Die Fähigkeit, dem Anwender "mdbadmin" Berechtigungen für verschiedene Systemtabellen und -ansichten zu gewähren (Verbindung zu "sys" als "sysdba" herstellen; alle Berechtigungen auf "sys" gewähren). <TABLE_NAME> an "installation_user" mit Hilfe der Option zum Erteilen von Rechten). Dabei kann "TABLE_NAME" die folgenden Werte annehmen: COL\$, DBA_CONSTRAINTS, DBA_CONS_COLUMNS, DBA_INDEXES, DBA_IND_COLUMNS, DBA_OBJECTS, DBA_OBJECT_TABLES, DBA_REGISTRY, DBA_TABLES, DBA_TABLESPACES, DBA_TAB_COLUMNS, DBA_TAB_PRIVS, DBA_VIEWS, DBMS_REGISTRY, EXPDEPACT\$, EXPDEPOBJ\$, EXPPKGACT\$, EXPPKGOBJ\$, KOPM\$, OBJ\$, TS\$, USER\$

- **Remote-Clients (UNIX und Linux):** Wenn die CA MDB über einen Remote-Client erstellt wird, wird dieser Vorgang mit einem Rückgabecode 95 und der Fehlermeldung *Tablespace kann nicht erstellt werden* im Installationsprotokoll beendet, es sei denn, das im Tablespace angegebene Verzeichnis ist sowohl auf dem Client-Rechner als auch auf dem Oracle-Server vorhanden.
- **Installation von CA MDB-Komponenten (SQL):** Im Installationsprogramm der CA MDB-Komponente wird das Feld "Name des Datenbankservers" angezeigt. Dieses Feld identifiziert den lokalen Servernamen oder bei Clusterung den Namen des Cluster-Knotens. Verwenden Sie den Netzwerknamen für die Verbindung mit dem SQL Server.
- **Sonderzeichen (UNIX, Linux und Windows):** Beachten Sie folgende Informationen:
 - (UNIX und Linux): Die Anwender-ID des Datenbankadministrators, die zum Erstellen der CA MDB verwendet wird, darf keine Sonderzeichen enthalten. Zusätzlich gelten folgende Einschränkungen:
 - Die Namen von DBA-Anwender und Tablespace unterstützen die Sonderzeichen # und _. Alle anderen Sonderzeichen werden nicht unterstützt.
 - Das DBA-Kennwort und das MDBADMIN-Kennwort unterstützen die Sonderzeichen ~, #, %, ^, -, +, _, {, }, [,], :, . und ? Alle anderen Sonderzeichen werden nicht unterstützt.
 - Der Oracle-Tablespace-Pfad, das MDB-Zielverzeichnis, das MDB-Quellverzeichnis und das MDB-Patchverzeichnis DIR unterstützen die Sonderzeichen ~, %, ^, _, -, +, [,], {, }, :, (einschließlich <space>, wenn der Pfad in doppelten Anführungszeichen steht. Aufeinanderfolgende Leerzeichen sind jedoch nicht zulässig).
 - (Windows): Die Anwender-ID des Datenbankadministrators, die zum Erstellen der CA MDB verwendet wird, *darf keine* Sonderzeichen enthalten. Zusätzlich gelten folgende Einschränkungen:
 - Der Name von DBA-Anwendern und Tablespace unterstützt die Zeichen #, \$ und _. Alle anderen Sonderzeichen werden nicht unterstützt.
 - Das DBA-Kennwort und das MDBADMIN-Kennwort unterstützen die Sonderzeichen ~, !, #, \$, *, (,), _ +, ` , -, {, }, [, \ , ; , ' , ? , . , / und @. Alle anderen Sonderzeichen werden nicht unterstützt.
 - Der Oracle-Tablespace-Pfad, das MDB-Zielverzeichnis, das MDB-Quellverzeichnis und das MDB-Patchverzeichnis unterstützen die Sonderzeichen ~, !, #, \$, (,), _ +, ` , -, {, } und [(einschließlich <space>, wenn der Pfad in doppelten Anführungszeichen steht).

- **Tablespaces:** Beachten Sie die folgenden Informationen:
 - Die CA MDB verwendet den temporären System-Tablespace, um temporäre Tabellen zu speichern. Für diesen Zweck sollten mindestens 50 MB an Speicherplatz verfügbar sein. Wenn Sie sich bei der CA MDB für die Verwendung vorhandener Tablespaces entscheiden, erfordern die Tablespaces mindestens 200 MB verfügbaren Speicher. Steht dieser Speicherplatz nicht zur Verfügung, schlägt die CA MDB-Erstellung fehl.
 - Wird die CA MDB-Erstellung zur Generierung eines Daten- oder Index-Tablespace verwendet und ist der Größenparameter nicht numerisch, wird ein Rückgabecode von 350 ausgegeben. Außerdem zeigt das CA MDB-Installationsprotokoll einen Fehler (rc=189) an, wonach während des Vorgangs kein Tablespace erstellt werden konnte.
- **Anwender- und Administratorrechte:** Wenn die CA MDB mit einem Anwender ohne Administratorrechte erstellt wird, schlägt der Erstellungsvorgang fehl. Das CA MDB-Installationsprotokoll zeigt den Fehler *"ORA-00942: Tabelle oder Ansicht ist nicht vorhanden"* an.

Weitere Informationen:

[So installieren Sie CA MDB](#) (siehe Seite 156)

Planen der CA SDM-Installation

Folgende Informationen unterstützen Sie beim Planen einer erfolgreichen CA SDM-Installation und Konfiguration. Damit suchen und erfassen Sie die richtigen Informationen.

- **Anmeldeberechtigungen:** Führen Sie die folgenden Schritte durch:
 - (Windows) Melden Sie sich als Administrator mit allen Administratorberechtigungen an.
 - (UNIX) Melden Sie sich als Root-Anwender mit den entsprechenden Berechtigungen für das Root-Anwenderkonto an.
 - **Nachforschung:** Führen Sie die folgenden Schritte aus:
 - Lesen Sie *sowohl* die Versionshinweise als auch die optionale Readme-Datei (sofern vorhanden). Starten Sie Ihre Installation erst, wenn Sie diese Informationen gelesen und verstanden haben.
- Hinweis:** Die aktuellste Version der Versionshinweise mit den jeweils gültigen Systembedingungen und der optionalen Readme-Datei (sofern verfügbar) finden Sie unter <http://ca.com/support>.

- Vergewissern Sie sich, dass Sie über den Installationsdatenträger verfügen.

Hinweis: Falls Ihr Computer nicht über ein für den Installationsdatenträger geeignetes Laufwerk verfügt, können Sie den Medieninhalt auf den Computer kopieren, auf dem Sie CA SDM installieren möchten. Starten Sie die Installation dann erneut. Bei einer Remote-Installation über das Netzwerk müssen Sie eventuell ein Laufwerk bzw. einen Netzwerkordner freigeben und dann zum Starten der Installation die Verbindung herstellen.

Wichtig! Verwenden Sie die CA SDM Installations-DVDs nicht unter einem Windows-XP-Betriebssystem, da einige Installationsdateien nicht gefunden werden und die Installation fehlschlägt.

- Suchen Sie in der Zertifizierungsmatrix die Liste mit Softwareprodukten anderer Hersteller, die für die Verwendung mit CA SDM zertifiziert sind.

Hinweis: Die aktuelle Version der Zertifizierungsmatrix finden Sie unter <http://ca.com/support>.

- Lesen Sie die Informationen über die Produktkomponenten, um die wesentlichen Merkmale kennenzulernen.
 - Machen Sie sich mit den verschiedenen Implementierungsstrategien für das Produkt vertraut. Berücksichtigen Sie bei der Entscheidung für eine für Ihr Unternehmen am besten geeignete Implementierungsstrategie auch die Netzwerkverfügbarkeit, die nutzbare Bandbreite sowie die Antwortzeiten.
 - Überprüfen Sie die Implementierungshinweise für jede zu installierende Komponente.
- **Installations-Stammverzeichnis:** Führen Sie die folgenden Schritte aus:
 - Bestimmen Sie das Stammverzeichnis, in dem Sie das Produkt installieren wollen. Das Standardverzeichnis für das Produkt ist C:\Programme\CA\Service Desk Manager.
 - Bestimmen Sie das Stammverzeichnis, in dem Sie die gemeinsamen Komponenten dieses Produkts installieren möchten (zum Beispiel Java Runtime Environment (JRE) und Apache Tomcat). Das Standardverzeichnis für die gemeinsamen Komponenten ist C:\Programme\CA\SC.
 - **Datenbank:** Entscheiden Sie, welche Datenbank (entweder SQL Server oder Oracle) Sie mit CA SDM verwenden möchten, und installieren Sie diese. Führen Sie dann die folgenden Schritte aus:
 - **SQL Server.** Aktivieren Sie TCP/IP auf dem Computer, auf dem Sie die Installation und die Konfiguration durchführen wollen.

- **Primärserver, sekundärer Server und Anwenderkonfiguration:** Führen Sie die folgenden Schritte aus:
 - Um sicherzustellen, dass Sie als letzten Schritt der Produktinstallation sowohl den Primärserver als auch optionale sekundäre Server konfigurieren können, sollten Sie die folgenden Informationen zur Hand haben:
 - Domain Name System (DNS) des Primärservers und der sekundären Server
 - Name oder Alias des Servers
 - Name oder Alias des Objektmanagers, zu dem Sie eine Verbindung herstellen wollen.
 - Name oder IP-Adresse des sekundären Servers
 - Slump-Socket-Port zur Kommunikation mit CA SDM
 - Den Proctor-Socket-Port, der vom sekundären Server verwendet wird, um Meldungen vom primären Server zu empfangen.
 - Um sicherzustellen, dass Sie am Ende der Produktinstallation die Kontoinformationen für die Produktverwaltung konfigurieren können, sollten Sie Name und Kennwort eines berechtigten und eines eingeschränkten Anwenders zur Hand haben.
 - (UNIX und Linux) Erstellen Sie Ihren berechtigten Anwender manuell. Unter Windows wird dieser Anwender während der Produktkonfiguration automatisch erstellt. Unter UNIX und Linux muss der Anwender jedoch manuell erstellt werden.

Hinweis: Im Szenario "So konfigurieren Sie Server für erweiterte Verfügbarkeit" finden Sie Informationen über die Serverkonfiguration für erweiterte Verfügbarkeit.

- **Konfiguration der Web-Schnittstelle:** Führen Sie die folgenden Schritte aus:
 - Um sicherzustellen, dass Sie am Ende der Produktinstallation die Web-Schnittstelle konfigurieren können, sollten die folgenden Informationen verfügbar sein:
 - Webhostname und Webserver
 - (nur Windows NT) die vom CA SDM-Server verwendete Website
 - Tomcat-Portnummer und Socket-Portnummer für Shutdown-Aufforderungen
- **Browser und Antivirussoftware:** Führen Sie die folgenden Schritte aus:
 - (Firefox) Aktivieren Sie optional die Windows-Authentifizierung (Single Sign On für Unternehmen).
 - Deaktivieren Sie vorübergehend jede Antivirussoftware, denn diese verlangsamt den Installationsvorgang. Stellen Sie sicher, dass Sie nach der Installation die Antivirussoftware wieder aktivieren.

- **Web Screen Painter:** Web Screen Painter wird bei der CA SDM-Installation automatisch auf dem Primärserver installiert. Mit Hilfe des Installationsdatenträgers können Sie Web Screen Painter auf separaten Computern installieren.
- **Erstellen von Dateinamen:** CA SDM erfordert die Erstellung von 8.3-Dateinamen. Weitere Informationen über das Erstellen von 8.3-Dateinamen und den Registry-Eintrag "disable8dot3" finden Sie in der Dokumentation und Online-Hilfe zu Ihrem Betriebssystem.

Weitere Informationen:

[So installieren Sie CA SDM](#) (siehe Seite 165)

[Serverkomponenten](#) (siehe Seite 17)

[Implementierungsstrategien](#) (siehe Seite 134)

[Aktivieren der Windows-Authentifizierung in Firefox](#) (siehe Seite 135)

Hinweise zu CA SDM

Bevor Sie CA SDM installieren, lesen Sie die folgenden Informationen, um eine erfolgreiche Implementierung sicherzustellen:

- **Apache-Server (UNIX und Linux):** Bei Installation des Apache-Servers unter UNIX oder Linux wird in manchen Fällen die Option "FollowSymLinks" im Stammverzeichnis deaktiviert. Diese Option deaktiviert die standardmäßige Apache-Integration für CA SDM, da die Konfigurationsdatei die symbolische Verknüpfung "/opt/CAisd" verwendet, die während der CA SDM-Installation erstellt wird. Damit CA SDM mit Apache verwendet werden kann, können Sie "FollowSymLinks" im Stammverzeichnis zulassen (in der Datei "httpd.conf" festzulegen) oder die Datei "\$NX_ROOT/bopcfg/www/CAisd_apache.conf" so ändern, dass die symbolische Verknüpfung durch den tatsächlichen Pfad ersetzt wird. Ändern Sie in der Datei "CAisd_apache.conf" alle Einträge "/opt/CAisd" in den tatsächlichen CA SDM-Speicherort (z. B. "/opt/CA/ServiceDeskManager"). Speichern Sie die Änderung, stoppen Sie den Apache-Server, und starten Sie ihn erneut, damit die Änderungen wirksam werden.

- **Browser:** Beachten Sie die folgenden Informationen:
 - (Firefox) Beachten Sie die folgenden Informationen:
 - Eventuell tritt der Fehler "*Unprivileged Script*" auf, wenn Sie die Ausschneide-/Kopier-/Einfügefunktion auf der HTML-Editor-Seite in den Knowledge-Kategorien verwenden. Klicken Sie auf "OK", um einen technischen Hinweis von mozilla.org darüber zu erhalten, wie ein Skript Zugriff auf die Zwischenablage erhält.
 - Wenn Sie den Inhalt eines Dateianhangs anzeigen, dessen Dateiname Zeichen aus dem erweiterten Latin-1-Zeichensatz enthält, wird ein Dialogfeld "Speichern unter" angezeigt. Sie können auf Festplatte speichern oder auf "Öffnen" klicken und eine Anwendung auswählen, um den Anhang zu öffnen.
 - (Internet Explorer 8 unter Windows 2008) Wenn die Internetsicherheit auf "Hoch" eingestellt ist, müssen Sie die CA SDM-URL und "*about:blank*" den vertrauenswürdigen Sites hinzufügen, damit die Webseiten ordnungsgemäß angezeigt werden.
 - (Google-Toolbar) Möglicherweise wird in der CA SDM-Web-Schnittstelle der Text in der Titelleiste oben im Fenster nicht korrekt angezeigt.
 - (Internet Explorer 8.0) Beim Zugriff auf die CA SDM-Web-Schnittstelle kann es zeitweise zu einer erhöhten Speichernutzung kommen. Dies ist ein bekanntes Problem in dieser Version von Internet Explorer. Um Speicher freizugeben, sollten Sie von Zeit zu Zeit die Haupt-Webseite von CA SDM minimieren.
- **CA Workflow:** Beachten Sie die folgenden Informationen:
 - Wenn die Informationen für berechnigte Anwender während der Konfiguration falsch angegeben werden, kann CA SDM ausgeführt werden, doch die Ausführung von CA Workflow schlägt fehl. Sind diese Anmeldeinformationen nicht richtig, können folgende Probleme auftreten:
 - CA Workflow wird nicht installiert. Die Datei "*/site/Workflow/wekinstall.log*" enthält einen ungültigen Anwendernamen oder ein ungültiges Kennwort.
 - Tomcat nimmt zu viel Prozessorleistung in Anspruch und/oder die Protokolldatei "*/log/pdm_tomcat_CAWF.log*" enthält zu viele Sicherheits-Manager-Ausnahmen und "*AbandonedObjectPool is used*"-Meldungen.

Um dies zu korrigieren, überprüfen Sie den Anwendernamen und das Kennwort des berechtigten Anwenders, indem Sie sich beim Betriebssystem mit diesen Anmeldeinformationen anmelden. Führen Sie dann die CA SDM-Konfiguration aus, und geben Sie den/das richtige Anwendernamen/Kennwort des berechtigten Anwenders ein. Wird das Kennwort des berechtigten Anwenders geändert, muss die Konfiguration ausgeführt werden, um das neue Kennwort einzustellen.

- Wenn die Anmeldeinformationen des berechtigten Anwenders geändert werden, nachdem die CA Workflow-Installation abgeschlossen wurde, kann der CA Workflow-Prozess fehlschlagen. Führen Sie die folgenden Schritte aus:
 - a. Melden Sie sich beim CA Workflow IDE an, um den standardmäßigen CA SDM-Webservice-Akteur zu ändern.
 - b. Wählen Sie die Registerkarte "Akteur" aus, erweitern Sie die Struktur "JavaScript", und klicken Sie auf den USD-Initialisierer.
 - c. Doppelklicken Sie auf "Globale Attribute abrufen".
 - d. Geben Sie den berechtigten Anwendernamen und das Kennwort für CA SDM in folgende Felder unter dem Skriptabschnitt ein:
`USD_Username = ""`
`USD_Password = ""`
 - e. Ändern Sie diese Werte in der Datei
`"$NX_ROOT\data\workflow\actors\r12_Service_Desk_Actors_en_US.xml"`.

■ **Datenbanken (alle unterstützt):** Beachten Sie die folgenden Informationen:

- Wurde CA SDM mit einer Datenbank konfiguriert und wird die Konfiguration dann ein zweites Mal ausgeführt und ein anderer Datenbanktyp ausgewählt, schlägt die Konfiguration fehl. Wenn Sie zum Beispiel zuerst SQL Server konfigurieren und bei einer zweiten Konfiguration dann eine Oracle-Datenbank wählen. Um dieses Problem zu vermeiden, starten Sie den Rechner vor dem Ausführen der zweiten Konfiguration neu.
- Informationen zur Datenbankverbindung werden, falls abweichend, in späteren Konfigurationen nicht übernommen. Sollte aufgrund veränderter Informationen zur Datenbankverbindung eine zusätzliche Konfiguration notwendig sein, löschen Sie die Datei "`$NX_ROOT\NX.env`", bevor Sie fortfahren.
- Wenn Sie von Argis 8.0 auf CA Asset Portfolio Management r11.2 aktualisieren und Sie die CA MDB (Datenbank) gemeinsam mit CA SDM nutzen, können beim Hinzufügen oder Aktualisieren von Assets in Asset-Familien mit CA SDM Probleme auftreten. Um Fehler zu vermeiden, müssen Sie die Asset-Erweiterungstabellen mit einer der folgenden Methoden für CA SDM definieren:
 - Verwenden Sie WSP, um Tabellen und Formulare für das Anzeigen und Bearbeiten der Tabelleneinträge zu definieren.
 - Bearbeiten Sie die Tabellen und Formulare unter Berücksichtigung der folgenden Richtlinien manuell:
 - a. Die Datei "`$NX_ROOT\bopcfg\majic\assetx.maj`" enthält eine Vorlage zur Erstellung einer majic-Datei, mit der die Spalten in der Asset-Erweiterungstabelle für CA SDM identifiziert werden können. Kopieren Sie diese Datei, und bearbeiten Sie sie unter Berücksichtigung der in der Datei enthaltenen Anweisungen.

- b. Erstellen Sie eine .sch-Datei im Verzeichnis "\$NX_ROOT\site\mods", um die Datenbankspalten zu definieren. Die Dateien "\$NX_ROOT\site\assetx_schema.sch" und "\$NX_ROOT\site\assetx_index.sch" können als Vorlagen verwendet, kopiert und den vorliegenden Ressourcenerweiterungstabellen entsprechend bearbeitet werden.

Hinweis: Das Formular zum Anzeigen der Asset-Erweiterungsdaten können Sie mit WSP erstellen.

■ **SQL Server:** Beachten Sie die folgenden Informationen:

- Für die neue Version von SQL Server sind strengere Kennwortregeln als in den Vorgängerversionen von SQL Server festgelegt. Stellen Sie sicher, dass das Kennwort für die CA SDM-Datenbank den Anforderungen der in SQL Server definierten Kennwortrichtlinien entspricht. Wenn das CA SDM-Datenbankkennwort der SQL Server 2005-Kennwortrichtlinie nicht entspricht, funktioniert die CA SDM-Konfiguration nicht.
- (Microsoft-Cluster-Umgebung unter SQL Server 2005) In einem Cluster müssen Sie für den SQL Virtual-Knotennamen einen Alias erstellen. Auf diese Weise kann CA SDM auch bei einem Cluster-Failover die Verbindung mit dem selben Servernamen herstellen. Dabei spielt es keine Rolle, welcher Clusterknoten aktiv ist.

■ **Oracle:** Beachten Sie die folgenden Informationen:

- Wenn Sie CA SDM auf einem UNIX-basierten System mit einer Oracle-Datenbank installieren, muss der berechtigte Anwender der während der Oracle-Installation angegebenen Gruppe angehören. Die Oracle-Installationsgruppe finden Sie in der Datei "*oralnst.loc*".
- Wenn Sie eine 64-Bit-Oracle-Datenbank auf einem 64-Bit-Rechner konfigurieren, muss der Systembibliothekspfad (LD_LIBRARY_PATH unter Oracle Solaris unter Linux und LIBPATH unter AIX) auf die 32-Bit-Oracle-Bibliotheken verweisen. Die 32-Bit-Oracle-Bibliotheken finden Sie unter \$ORACLE_HOME/lib32. Dies gilt für die Konfiguration und für die Laufzeit.
- Zum Konfigurieren einer 64-Bit-Oracle 11g-Datenbank auf einem 64-Bit-Computer *müssen* Sie auch den Oracle-32-Bit-Client auf dem Server installieren. Wenn die Datenbank konfiguriert wird, *muss* der Systembibliothekspfad (LD_LIBRARY_PATH unter Oracle Solaris und Linux, LIBPATH unter AIX) auf die 32-Bit-Oracle-Bibliotheken verweisen. Dieser Schritt ist sowohl für die Konfiguration als auch für die Laufzeit erforderlich. Erstellen Sie auch einen Netzdienstnamen auf dem Oracle-Client, der auf die Oracle-Datenbankserver-Instanz verweist.
- Wenn Sie eine Oracle-Datenbank einsetzen und vorhandene Tablespaces verwendet werden sollen, müssen Sie einen Daten-Tablespace mit mindestens 400 MB und einen Index-Tablespace mit mindestens 100 MB erstellen, bevor Sie CA SDM konfigurieren.

- **Extern gemountete Laufwerke:** Bei Installationen von CA SDM unter Linux mit 20 oder mehr extern gemounteten Laufwerken wird die Seite über den Installationsfortschritt eventuell mit einer Verzögerung nach den Seiten des Installationsassistenten angezeigt. Dieses Verhalten ist normal, die Installation wird nach der Verzögerung fortgesetzt.
- **InstallShield und InstallAnywhere:** Beachten Sie die folgenden Informationen:
 - Wenn Sie bei dem Versuch, CA SDM zu installieren, eine InstallShield-Fehlermeldung erhalten, warten Sie, bis *msiexec.exe* nicht mehr ausgeführt wird. Versuchen Sie dann, das Produkt zu installieren.
 - Wenn Sie die CA SDM-Installation unter UNIX oder Linux starten und dann anhalten, sehen Sie möglicherweise ein Verzeichnis namens *install.dir.####*. Dies ist ein Merkmal von InstallAnywhere. Diese Dateien werden nicht benötigt, d. h. Sie können sie problemlos löschen.
- **Installations-Stammverzeichnis:** Installieren Sie die gemeinsamen CA-Komponenten nicht im selben Verzeichnis wie CA SDM (NX_ROOT).
- **International:** Beachten Sie die folgenden Informationen:
 - Bei einer Installation unter Multibyte-Betriebssystemen dürfen Sie weder für den Anwendernamen, unter dem Sie angemeldet sind, noch für den Namen des berechtigten Anwenders für CA SDM Multibyte-Zeichen wie das vereinfachte Chinesisch oder Japanisch verwenden. Die Installation würde in diesem Fall fehlschlagen.
 - Geben Sie während der Installation und Konfiguration keine Multibyte-Zeichen in Dateipfadnamen an. Die Installation und/oder die Konfiguration würden in diesem Fall fehlschlagen.
 - CA SDM muss auf Linux- und UNIX-Plattformen mit dem UTF-8-Gebietsschema ausgeführt werden.
 - Die Symbole für die Zeitspanne (Registerkarte "Administration", "Service Desk", "Anwendungsdaten", "Codes", "Zeitspannen"), die standardmäßig mit CA SDM geliefert werden, liegen auf Englisch vor. z. B. TODAY, YESTERDAY, THIS MONTH usw. Für lokalisierte Versionen des Produkts können Administratoren neue, lokalisierte Zeitspannen je nach Bedarf definieren. Die Standardzeitspannen sollten Sie jedoch nicht löschen oder ändern.
 - Die Datumsformate in CA SDM unterstützen keine internationalen Datumsbezeichner (wie z. B. "tt/MM/JJJJ" für Deutsch). Die Syntax ist auf allgemeine Bezeichner wie "DD/MM/YYYY" beschränkt. Dennoch können mit Hilfe dieser allgemeinen Bezeichner viele internationale, kurze Datums-/Uhrzeitmuster konstruiert werden (z. B. "YYYY.MM.DD" würde ein übliches japanisches kurzes Datumsformat ergeben).

- Für ausgehende E-Mail-Benachrichtigungen in unformatiertem Text müssen die Optionen `NX_SMTP_HEADER_CHARSET` und `NX_SMTP_HEADER_CHARSET` möglicherweise angepasst werden (direkt in der Datei "NX.env"), um die E-Mail-Nachricht mit der von der internationalen Betriebsumgebung verwendeten Zeichencodierung zu versehen. So kann sie auf den E-Mail-Systemen der Empfänger korrekt interpretiert und angezeigt werden. Die Standardwerte für diese Optionen werden auf allen Plattformen auf UTF-8 gesetzt.
- Bei nicht-englischen Oracle-Installationen auf UNIX- oder Linux-Systemen müssen Sie die Umgebungsvariable `NLS_LANG` vor dem Ausführen von "pdm_init" festlegen. Der Oracle-Datenbankadministrator sollte die erforderliche Wertzuweisung für `NLS_LANG` in der Oracle-Dokumentation nachschlagen.

Wichtig! Wenn Sie `NLS_LANG` nicht setzen, lautet die Standareinstellung des Oracle-Clients *American_America.US7ASCII*. Um zum Beispiel Multibyte-Japanisch in Ihrer Umgebung zu testen, setzen Sie `NLS_LANG` auf *JAPANESE_JAPAN.UTF8*.

Hinweis: Die `NLS_LANG`-Variable muss in derselben Shell festgelegt werden, bevor "pdm_init" ausgeführt wird. Beispiel: `setenv NLS_LANG GERMAN_GERMANY.WE8ISO8859P1`

- Internationale Anwender werden möglicherweise die Eigenschaft "DateFormat" in der Datei "web.cfg" anpassen, um das für ihre Region geeignetste Datumsformat zu verwenden.
- Internationale Anwender werden möglicherweise das standardmäßige Wörterbuch (die Option `LEX_LANG` im Optionsmanager) durch ein Wörterbuch für die eigene Sprache ersetzen wollen.
- Die englische Version des CA SDM-Servers ist für die Verwendung in neun nicht-englischsprachigen Betriebsumgebungen zertifiziert. Bei Windows muss es sich dabei um vollständig übersetzte Versionen der unterstützten Windows Server-Betriebssysteme handeln. Insbesondere werden Windows-Betriebsumgebungen, die ein Language Interface Pack oder ein MUI auf einem englischsprachigen Kern verwenden, nicht unterstützt.

Außerdem werden lokalisierte Versionen von CA SDM nur auf den entsprechenden lokalisierten Windows Server-Betriebsumgebungen unterstützt. In allen Fällen muss die "Sprache für Programme, die Unicode nicht unterstützen" (Standard: Windows ANSI-Codepage) in den Ländereinstellungen und Sprachoptionen der Systemsteuerung sorgfältig konfiguriert werden, damit die zertifizierte Zielsprache unterstützt wird.

Hinweis: Weitere Informationen über die lokalisierten Versionen von Windows Server-Betriebssystemen finden Sie in der Liste lokalisierter Microsoft-Betriebssysteme im globalen Microsoft-Portal für Entwicklung und Computing.

- Die Knowledge-Suche mit japanischen Multibyte-Zeichen für internationale Anwender von CA SDM und Knowledge Management funktioniert mit SQL Server nur dann einwandfrei, wenn SQL Server mit der Windows-Sortierfolge installiert wurde. Vergewissern Sie sich, dass Sie für Ihre Daten während der SQL Server-Installation die Option Collation (Sortierung) angeben.

- **IPv4:** Bei der Installation auf Linux-Plattformen muss die Datei `"/etc/hosts"` einen IPv4-Eintrag mit der IP-Adresse, dem Rechnernamen und dem vollständigen Rechnernamen enthalten. Nachfolgend sehen Sie einen Beispieleintrag:

```
127.0.0.1 localhost.localdomain localhost
141.202.211.11 usbep11.ca.com usbep11
```

- **Kurze Dateinamen:** Wenn Sie kurze Dateinamen unter Windows deaktiviert haben, sollten Sie diese vor der Installation von CA SDM aktivieren. Außerdem müssen Sie die Umgebungsvariablen TEMP und TMP auf einen kurzen Dateinamen setzen, z. B. auf `"c:\temp"`. Führen Sie diesen Vorgang durch, nachdem Sie kurze Dateinamen aktiviert haben und bevor Sie mit der Installation beginnen.

Hinweis: Weitere Informationen finden Sie im Artikel 121007 über die Microsoft-Wissensbasis auf der Microsoft-Support-Website.

- **Sonderzeichen und Leerzeichen (Verzeichnis, Medienpfad und Ordnername):**

Beachten Sie die folgenden Informationen:

- (UNIX und Linux) Stellen Sie beim Kopieren des Installationsdatenträgers auf eine lokale Festplatte sicher, dass der Verzeichnispfad keine Leerzeichen oder Sonderzeichen (z. B. #) enthält. Wenn der Verzeichnispfad Leerzeichen oder Sonderzeichen enthält, funktioniert die Installation nicht.
- (UNIX, Linux und Windows) Geben Sie *keine* Leerzeichen im Installationspfad und im Ordnernamen an. Anderenfalls schlägt die Installation fehl.

- **Tomcat:** Beachten Sie die folgenden Informationen:

- Tomcat wird während der Produktinstallation als Standardwebserver für CA SDM festgelegt. Wenn Sie IIS (unter Windows) oder Apache (unter UNIX oder Linux) als Standardwebserver verwenden wollen, führen Sie die Konfiguration aus und wählen bei der entsprechenden Eingabeaufforderung IIS oder Apache aus. Sie können auch die Konfiguration erneut ausführen und dabei IIS oder Apache wählen.
- Ist Tomcat auf dem Primärserver mit externer Authentifizierung konfiguriert, müssen Sie einen sekundären Server mit Webengine- und Repository-Daemons einrichten, damit nicht authentifizierte Anwender Anhänge verwenden können. Die Tomcat-Installation auf dem sekundären Server kann keine externe Authentifizierung verwenden.

- Die CA SDM-Installation setzt den Tomcat-Port auf 8080. Andere Produkte von CA, wie z. B. CA Asset Portfolio Management oder die Service Delivery Suite-Produkte, setzen den Tomcat-Port standardmäßig ebenfalls auf 8080. Falls Sie auf demselben Server mehrere Produkte von CA installieren, stellen Sie sicher, dass Sie für künftige CA Technologies-Produktinstallationen einen anderen Port als 8080 wählen, damit diese Produkte einwandfrei funktionieren. Um für CA SDM eine andere Tomcat-Portnummer als 8080 zu wählen, installieren Sie das Produkt. Sofern es bereits installiert ist, führen Sie die Produktkonfiguration erneut aus und geben eine verfügbare Portnummer für Tomcat an, wenn Sie dazu aufgefordert werden.
- Nach einem Neustart wird der CA SDM Tomcat-Prozess möglicherweise nicht ordnungsgemäß gestartet. Ist dies der Fall, verwenden Sie die folgenden Befehle, um TOMCAT anzuhalten und neu zu starten:

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

■ **Anwender und Authentifizierung:** Beachten Sie die folgenden Informationen:

- Die Anwenderauthentifizierung funktioniert nicht, wenn das System Schattendateien verwendet und ein "x" im Kennwortfeld der Datei "/etc/passwd" vorhanden ist.
- Wenn Sie auf HP-Systemen die Sicherheitseinstellungen so konfiguriert haben, dass Systemkennwörter in "/etc/shadow" gespeichert werden (z. B. wenn anstelle eines Kennworts ein "x" in "/etc/passwd" gespeichert ist), schlägt die CA SDM-Anwenderauthentifizierung fehl, und Anwender sind nicht in der Lage, sich bei CA SDM anzumelden.
- Die Kennwörter, die für den berechtigten Anwender angegeben werden, müssen den Einschränkungen der Kennwortrichtlinie entsprechen, die von der Netzwerkdomäne vorgegeben sind. Wenn sie den von der Domäne auferlegten Einschränkungen nicht entsprechen, funktioniert die CA SDM-Konfiguration nicht.

■ **Web-Schnittstelle und Internet-Informationsdienste (IIS):** Um die Web-Schnittstelle unter Windows 2008 mit IIS 7.0 zu konfigurieren, müssen Sie die CGI- und Metabase-Compatibility-Komponenten von IIS 7.0 installieren. Sie können diese Komponenten mit Hilfe der Rollen im Server-Manager hinzufügen, indem Sie die Module von IIS-Management-Kompatibilität installieren.

■ **Web Screen Painter:** Beachten Sie die folgenden Informationen:

- Wenn Sie WSP als Teil von CA SDM installieren, muss er konfiguriert werden, damit er richtig funktioniert.
- In einer Web Screen Painter-Vorschauansicht im Testmodus werden Suchfilter in neuen, noch nicht veröffentlichten Tabellen ignoriert.

Weitere Informationen:

[So installieren Sie CA SDM](#) (siehe Seite 165)

CA CMDB-Komponenten

CA CMDB bietet die folgenden Standardkomponenten:

CA CMDB-Web-Schnittstellenseiten

- Definiert und verfolgt Eigenschaften von CIs und Beziehungen zwischen diesen
- Unterstützt Änderungsauswirkungs- und Ursachenanalyse

CMDB Visualizer

- Stellt Beziehungen zwischen CIs grafisch dar
- Unterstützt die Planungsfunktion

Versionskontrolle

- Zeigt den Änderungsverlauf von CIs sowie deren Beziehungen an
- Vergleicht Snapshots und benannte Meilensteine.

Common Asset Viewer

- Bietet eine gemeinsame Ansicht von Asset-Attributen mehrerer Produkte
- Bietet den Startpunkt für die Unterstützung von Produkten

Abstimmung von CIs

- Ordnet importierte Daten von CIs bestehenden CIs in der CMDB zu
- Verwendet bestehende Asset-Registrierungs-API

Repository

- Bietet einen Datenspeicher für CIs, Beziehungen, Familien und so weiter.
- Ist in der MDB vorhanden.

Integration

- Ermöglicht die standardmäßige, vordefinierte Integration in CA Service Desk, CA NSM, CA Asset Portfolio Management, CA EEM und andere Produkte

Berichterstellung

Liefert die folgenden Berichte für CIs:

- Übersicht
- Detail
- Geänderte CIs
- CI-Familie
- CI-Beziehung
- Baumstruktur einer Beziehung

Support-Automatisierung-Planungs-Überlegungen

Die folgenden Informationen können Sie dabei unterstützen, Informationen zusammenzutragen, mit denen sich eine erfolgreiche Support-Automatisierung-Konfiguration planen lässt.

- In den Versionshinweisen finden Sie die Anforderungen für Support-Automatisierung.
- **Server und Netzwerk** - Beachten Sie die folgenden unterstützten Support-Automatisierung-Servermodi:
 - **Hauptserver** - Support-Automatisierung verwendet Hauptanwendungsserver. Der Server stellt socket-basierte und HTTP-basierte Kommunikationen bereit.
 - **Socket-Proxy-Server**-Support-Automatisierung <verwendet einen Socket-Proxy auf der gleichen Stufe wie der Webserver, der Verschlüsselungs- und Entschlüsselungsprozesse vom Hauptserver für direkte Socket-Verbindungen herunterlädt, um die Skalierbarkeit zu unterstützen.
 - **Nachrichtenroutingserver (MRS)**-Support-Automatisierung trennt Datenverkehr mit hoher Bandbreite und unvorhersehbaren Datenverkehr vom Hauptanwendungsserver, um die Serverskalierbarkeit zu unterstützen und eine Routing-Abkürzung im Netzwerk für geografische Skalierbarkeit über Remote-Steuerungsverbindungen bereitzustellen.
- **Bestimmung der Servergröße** - Berücksichtigen Sie die folgenden Servervariablen:
 - **Netzwerkmerkmale von Endanwender- und Analystenverbindungen** - Die Serverlast ist direkt proportional zu den Daten der Routing-Komponente für Meldungen. Niedrige Bandbreite, hohe Latenz und hoher Datenpaketverlust tragen deutlich zum Absenken der Servergeschwindigkeit bei. Wenn die Netzbedingungen optimal sind (hohe Bandbreite, geringe Latenz, geringer Datenpaketverlust), ist die Geschwindigkeit auf dem Server wesentlich viel höher. Die Gesamtzahl von gleichzeitigen Analyst-Anwendern und Endanwenderanmeldungen pro Minute, einschließlich Self-Service-Anwendern, können eine starke Belastung für den Server bedeuten.

- **Verbindungstyp** - Die-Anzahl von Socket-Verbindungen wirkt sich im Vergleich zur Anzahl von HTTP-Verbindungen wie folgt auf die Server aus:
 - Wenn Sie hauptsächlich Socket-Verbindungen herstellen, ist die Serverlast so gering, dass die Anwendung, falls leistungsstarke Hardware zur Verfügung steht, eher netzgebunden als CPU-gebunden ist. Die Hardware beschränkt die Anzahl von gleichzeitigen Verbindungen nicht; diese kann aber vom Netzwerk beschränkt werden.
 - Wenn Sie HTTP-Verbindungen herstellen, ist die Last im Netz und auf den Anwendungsservern höher, und die Anwendung ist CPU-gebunden, falls nicht deutlich skaliert wird.
- **Remote-Steuerungsnutzung** - Die Remote-Steuerung verwendet fortdauernd bedeutende Netzbandbreite, sooft sie ausgeführt wird. Der gesamte zwischen Endanwendern und Analysten geleitete Datenverkehr läuft über den Server. Die Anzahl gleichzeitiger Remote-Steuerungsverbindungen spielt eine bedeutende Rolle bei allen Größenbestimmungen.

Hinweis: Die Remote-Steuerung ist das einzige Tool mit hoher Bandbreite unter den Live-Unterstützungs-Tools. Chat und Automatisierung haben eine niedrige Bandbreite. Screenshot und Dateiübertragung können für kurze Zeiträume hohe Bandbreiten nutzen, während Dateien übertragen werden.

Überlegungen zu Netzwerk und Bandbreite für Support-Automatisierung

Die am Endanwender-Computer benötigte Bandbreite hängt wie folgt von den verwendeten Tools ab.

- Für die Chat- und Automatisierungsfunktionen wird nur wenig Bandbreite benötigt. Ein DFÜ-Modem von 56 Kbps oder weniger ist ausreichend, um diese Funktionen zu unterstützen.
- Für die Remote-Steuerungsfunktion wird mehr Bandbreite benötigt. Die Remote-Steuerung der Live-Unterstützung wird jedoch automatisch an Umgebungen mit geringer Bandbreite angepasst, indem die Bildqualität und die Aktualisierungsrate der Remote-Steuerungssitzung eingeschränkt werden.

Die erforderliche Bandbreite hängt auch vom verwendeten Verbindungsmodell ab. Zwei Verbindungsmodelle sind verfügbar:

- **HTTP Konnektivität** - Verwenden Sie dieses Modell, wenn sich der Endanwender hinter einem restriktiven Firewall befindet, der nur HTTP-Verbindungen zum Server zulässt.
- **SSL - direkter Socket** - Verwenden Sie dieses Modell, wenn der Endbenutzer die Serververbindung über eine Verbindung mit dem SSL-Port 443 herstellt.

Die folgende Tabelle veranschaulicht die erforderliche Bandbreite je nach den verwendeten Tools.

Tools/Bandbreite	Chat/Automatisierung	Remote Control
< 3 KBps (28,8 KBps DFÜ)	Sehr schnell und reaktionsbereit	Langsam
< 5 KBps (< 56 KBps DFÜ)	Sehr schnell und reaktionsbereit	Angemessen mit schlechterer Bildqualität
< 50 KBps (Kabel/ADSL)	Sehr schnell und reaktionsbereit	Sehr schnell und reaktionsbereit
< 100 KBps (LAN)	Sehr schnell und reaktionsbereit	Sehr schnell und reaktionsbereit

Planen der Installation von CA NSM

Um eine erfolgreiche CA NSM-Installation und -Konfiguration zu erleichtern, lesen Sie in der CA NSM-Dokumentation sowohl die *Versionshinweise* als auch die optionale Readme-Datei (falls vorhanden).

Planen der Installation von CA EEM und CA Workflow

Die folgenden Informationen unterstützen Sie beim Planen einer erfolgreichen Installation und Konfiguration von CA EEM und CA Workflow. Damit suchen und erfassen Sie die richtigen Informationen.

- **Nachforschung:** Führen Sie die folgenden Schritte aus:
 - Lesen Sie Ihre CA EEM- und CA Workflow-Dokumentation einschließlich der zugehörigen Versionshinweise und optionalen Readme-Dateien (falls verfügbar).
Hinweis: CA EEM ist keine Konfigurationsoption in CA SDM. CA EEM erfordert eine separate Installation.
 - Finden Sie heraus, ob Sie Ihre vorhandene CA EEM-Installation mit CA Workflow verwenden können. In diesem Fall dürfen Sie CA EEM *nicht* nochmals installieren. Installieren Sie stattdessen CA Workflow, und verweisen Sie auf Ihre vorhandene CA EEM-Installation.
 - Notieren Sie Ihr CA EEM-Administratorkennwort, denn Sie benötigen es für die Installation.

- **CA Workflow-Installation:** Führen Sie die folgenden Schritte durch:
 - Bevor Sie versuchen, CA Workflow zu installieren, stellen Sie sicher, dass CA EEM installiert ist. Sie können CA Workflow nicht installieren, bis dieses Produkt installiert wird.
 - Wenn Sie CA Workflow mit CA SDM r12.9 verwenden wollen, laden Sie die CA SDM-r12.7-ISO von CA Support Online herunter, bevor Sie CA Workflow installieren.
 - Die Tomcat-Portnummer für CA SDM ist standardmäßig 8080 und für CA Workflow 8090. Wenn diese Portnummern bereits von einem anderen Produkt verwendet werden, ändern Sie die Portnummern für CA SDM und CA Workflow, um mögliche Konflikte zu vermeiden.
- **CA EEM und AIX:** Wenn Sie CA EEM unter AIX installieren und AIX für Network Information Service (NIS) konfiguriert ist, fügen Sie einen Anwender namens *dsa* hinzu, bevor Sie CA EEM und CA SDM installieren. Führen Sie in diesem Fall die folgenden Schritte aus:
 1. Erstellen Sie einen Anwender mit der Anwenderkennung *dsa*.
 2. Legen Sie `/opt/CA/eTrustDirectory/dxserver` als *dsa*-Stammverzeichnis fest. Wenn die Verzeichnisse nicht vorhanden sind erstellen Sie diese manuell.

Hinweis: Dieser Schritt ist nur erforderlich für CA EEM Release 8.3 und frühere Versionen. Das Stammverzeichnis für CA EEM 8.4 hat sich geändert in `/opt/CA/Directory/dxserver` und wird automatisch während der Installation erstellt.
 3. Machen Sie *dsa* zum Eigentümer von `/opt/CA/eTrustDirectory` und allen Unterverzeichnissen. Um *dsa* zum Eigentümer zu machen, verwenden Sie einen Befehl ähnlich dem folgenden:

```
chown -R dsa /opt/CA/eTrustDirectory
```
 4. Vergewissern Sie sich, dass der Anwender vorhanden ist, und überprüfen Sie das Stammverzeichnis und den Eigentümer von `/opt/CA/eTrustDirectory`.

Weitere Informationen:

[So installieren Sie CA EEM](#) (siehe Seite 230)

[Hinweise zu CA Workflow](#) (siehe Seite 118)

[So installieren Sie CA Workflow](#) (siehe Seite 233)

[Installieren des Standalone-Clients CA Workflow IDE](#) (siehe Seite 235)

Hinweise zu CA EEM

Bevor Sie CA EEM installieren, lesen Sie die folgenden Informationen, um eine erfolgreiche Implementierung sicherzustellen:

- **Migration:** Wenn Sie auf CA SDM r12.9 migrieren, führen Sie ein Upgrade auf CA EEM r8.4 SP4 CR05 oder höher durch, nachdem Sie CA SDM installiert haben.
- **Externer LDAP-Datenspeicher:** Wenn CA EEM zur Verwendung von externen LDAP-Datenspeichern konfiguriert ist, muss der berechtigte Anwender im LDAP-Verzeichnis erstellt werden.

Hinweis: Weitere Informationen zur Konfiguration eines externen LDAP-Servers finden Sie im *Administrationshandbuch*.

Weitere Informationen:

[So installieren Sie CA EEM](#) (siehe Seite 230)

Hinweise zu CA Workflow

Bevor Sie CA Workflow installieren, lesen Sie die folgenden Informationen, um eine erfolgreiche Implementierung sicherzustellen:

- CA Workflow wird auf den folgenden CA SDM-Servern je nach Ihrer CA SDM-Konfiguration installiert:
 - Konventionell: Primärserver oder Sekundärserver
 - Erweiterte Verfügbarkeit: Beliebiger Anwendungsserver.
- **CA MDB-Datenbankanwender oder Kennwort:** Beachten Sie die folgenden Informationen:
 - Wenn Sie nach der Erstinstallation von CA SDM entweder den CA MDB-Datenbankbenutzer oder das Kennwort ändern, dann führen Sie die Installation von CA Workflow erneut aus, damit CA Workflow die Änderungen übernimmt und mit CA SDM kommunizieren kann. Wenn Sie die Installation von CA Workflow erneut ausführen, dann legt CA SDM automatisch den neuen Benutzernamen oder das Kennwort für CA Workflow fest, und Sie können die Werte während CA Workflow-Installation *nicht* manuell ändern.

Hinweis: Oracle-Umgebungsvariablen müssen festgelegt werden, bevor CA Workflow auf UNIX- und Linux-Systemen installiert wird. Wenn die ORACLE_HOME-Variable nicht gesetzt ist, erhalten Sie beim Klicken auf die Installationsverknüpfung eine Fehlermeldung.

- Wenn Sie zu einer neuen Datenbank migrieren, führen Sie das [Dienstprogramm Workflow Migration](#) (siehe Seite 120) aus.

- **IPv6:** Ist Ihr Linux-Server für IPv6-Unterstützung konfiguriert, können Sie sich möglicherweise nicht bei der CA Workflow-IDE anmelden. Zur Behebung dieses Problems ändern Sie die Skriptdatei "ide.sh", die sich in "\$NX_ROOT\site\Workflow\Client" befindet, indem Sie die zweite Zeile von "VMARGS=" zu "VMARGS=-Djava.net.preferIPv4Stack=true" ändern. Speichern Sie anschließend die Skriptdatei, und starten Sie CA Workflow-IDE erneut.
- **Tomcat:** Beachten Sie die folgenden Informationen:
 - Wenn Sie Schwierigkeiten beim Starten von Tomcat haben und infolgedessen CA Workflow und die Web-Schnittstelle nicht verfügbar sind, vergrößern Sie den Speicherplatz für Tomcat.

Hinweis: Informationen hierzu finden Sie im Knowledge Base-Artikel TEC418959 unter <http://ca.com/support>.
 - Geben Sie während der Installation von CA Workflow, CA SDM und CA EEM eine separate Portnummer für Tomcat frei. Wenn Sie beim Installieren oder Verwenden von CA Workflow Probleme mit Tomcat haben, [halten Sie den Dienst an und starten ihn erneut](#) (siehe Seite 285).
 - Der CA Workflow-Hostname, den Sie im Optionsmanager angeben, *muss* mit der Variablen "NX_LOCAL_HOST" in der Datei "NX.env" des Servers übereinstimmen, auf dem Sie CA Workflow installiert haben. Der Hostname *muss* in Groß- und Kleinschreibung übereinstimmen.
 - Falls Sie die Installations-Standardwerte für den Tomcat-Port (8080) oder die Standardwerte für Anwendernamen und Kennwort des berechtigten Anwenders (ServiceDesk/ServiceDesk) geändert haben, müssen Sie die Standarddefinitionen/-akteure für CA Workflow folgendermaßen ändern, damit sie einwandfrei funktionieren:
 - Melden Sie sich bei Workflow IDE an.
So ändern Sie den Standard-Service Desk-Webservice-Akteur:
 - a. Klicken Sie auf die Registerkarte "Akteure".
 - b. Blenden Sie die Webservice-Baumstruktur ein.
 - c. Klicken Sie mit der rechten Maustaste auf den Akteur "Unicenter_Service_Desk_Web_Service", und wählen Sie "Eigenschaften".
 - d. Markieren Sie den WSDL-URL-Eintrag, und kopieren Sie ihn in die Zwischenablage.
 - e. Ändern Sie den Namen des Akteurs, und klicken Sie auf "OK".
 - f. Klicken Sie mit der rechten Maustaste auf die Webservice-Baumstruktur, und wählen Sie "Akteur hinzufügen" aus.
 - g. Geben Sie in das Feld "Name" Folgendes ein:
Unicenter_Service_Desk_Web_Service.
 - h. Fügen Sie den zuvor kopierten Inhalt in den WSDL URL-Eintrag ein.

- i. Ändern Sie die Portnummer in der URL so, dass sie mit der während der Tomcat-Konfiguration gewählten Portnummer übereinstimmt.
- j. Klicken Sie auf "OK".
- Nachdem Sie CA Workflow auf dem CA SDM-Server installiert haben, führen Sie folgende Schritte aus, sodass die Integration zwischen CA SDM und CA Workflow erfolgreich funktioniert:
 - Melden Sie sich bei der CA Workflow IDE an, um den standardmäßigen CA SDM-Webservice-Akteur zu ändern.
 - Wählen Sie die Registerkarte "Akteur" aus, blenden Sie die Baumstruktur "JavaScript" ein, und klicken Sie auf USD-Initialisierer.
 - Doppelklicken Sie auf "Globale Attribute abrufen".
 - Geben Sie den berechtigten Anwendernamen und das Kennwort für CA SDM in folgende Felder unter dem Skriptabschnitt ein:
`USD_Username = ""`
`USD_Password = ""`
 - Ändern Sie diese Werte in der Datei
`"$NX_ROOT\data\workflow\actors\r12_Service_Desk_Actors_en_US.xml"`.

Weitere Informationen:

[So installieren Sie CA Workflow](#) (siehe Seite 233)

Das Dienstprogramm Workflow Migration

Mit dem Tool "Workflow Data Migration" übertragen Sie Daten von einer CA Workflow-Datenbank in eine andere. Dieses Dienstprogramm kann Daten von beliebigen unterstützten Datenbanken in andere unterstützte Datenbanken verschieben, und Daten in das neueste CA Workflow-Schema übertragen.

Das Workflow Data Migration-Tool wird sowohl als Benutzeroberfläche (GUI) als auch als Bean bereitgestellt.

- **GUI:** migration.jar
- **Bean:** datamover.jar

Hinweis: Um diese Java-Befehle auszuführen, müssen zwei JAR-Dateien (datamover.jar und migration.jar) manuell entzippt und in den Java-Path extrahiert werden. Die Migration.zip-Datei finden Sie auf dem Installationsdatenträger im Verzeichnis `\winsrvr.cd1\CA_tps.nt\CAFLOW\Resources`.

Ausführen des Migrations-Dienstprogramms über die Befehlszeile

Das Migrations-Tool wird als Bean in "datamover.jar" bereitgestellt. Sie können das Migrations-Tool über die Befehlszeile ausführen.

Ausführen des Migrations-Dienstprogramms

```
java -cp <driver jar file(s)> com.ca.workflow.util.DataMover <source db driver name>  
<source db url> <source db username> <source db password> <target db driver name>  
<target db url> <target db username> <target db password> <number of entries in one  
transaction> [product keys (comma separated)]--fetchsize=15 [options]
```

Beispiel

```
java -cp iijdbc.jar;datamover.jar com.ca.workflow.util.DataMover  
ca.ingres.jdbc.IngresDriver  
jdbc:ingres://155.35.26.105:EI7/mdb;cursor=readonly;auto=multi;group=workflow_admin_group root iloveca ca.ingres.jdbc.IngresDriver  
jdbc:ingres://tadra01-w2k3-v:EI7/mdb;cursor=readonly;auto=multi;group=workflow_admin_group tadra01 ca#33333 50 wekProductKey1 --clean-target --fetchsize=15
```

driver jar file(s)

Gibt die Quell- und Zieldateien der Treiber an. Trennen Sie mehrere Treiberdateien durch Semikolon (;).

source db driver name

Gibt den Treiber der Quelldatenbank an.

source db URL

Gibt die URL der Quelldatenbank an.

source db username

Gibt den Anwender der Quelldatenbank an.

source db password

Gibt das Kennwort der Quelldatenbank an.

target db driver name

Gibt den Treiber der Zieldatenbank an.

target db URL

Gibt die URL der Zieldatenbank an.

target db username

Gibt den Anwender der Zieldatenbank an.

target db password

Gibt das Kennwort der Zieldatenbank an.

number of entries in one transaction

Gibt die Anzahl der Einträge an, die in einer Transaktion verschoben werden. Wenn diese Zahl zu groß ist, besteht die Möglichkeit eines Überlaufs im Ingres-Transaktionsprotokoll. Als Standard wird 50 empfohlen.

clean-target

Entfernt alle Daten, die sich auf den angegebenen Produktschlüssel beziehen, aus der Datenbank und überträgt anschließend die Daten. Ist kein Produktschlüssel angegeben, werden alle Daten aus der Zieldatenbank entfernt, bevor Daten übertragen werden. Diese Option dient zum Bereinigen einer Zieldatenbank, wenn zuvor eine Migration mitten in der Ausführung fehlgeschlagen ist.

fetchsize

Wenn die Befehlszeilenoption "-fetchsize" vorhanden ist, gibt sie die Anzahl der Zeilen an, die in einem scrollbaren Ergebnissatz gleichzeitig abgerufen werden können. Ist diese Option nicht angegeben, verwendet das Dienstprogramm den Standardwert von "fetchsize" aus der Quelldatenbank. Für Ingres gibt es keinen Standardwert für die Anzahl der Zeilen, die in einem scrollbaren Ergebnissatz gleichzeitig abgerufen werden können. In diesem Fall wird der Standardwert von 10 Zeilen verwendet, falls dies nicht als Befehlszeilenoption angegeben wurde.

product keys

Gibt die Produktschlüssel für die zu migrierenden Daten an. Dieser Parameter kann optional festgelegt werden. Sie können nur einen Produktschlüssel oder auch mehrere angeben. Das Trennzeichen in einer Liste von Produktschlüsseln ist das Komma. Ist dieser Parameter angegeben, werden durch das Migrations-Dienstprogramm nur solche Daten aus der Quelldatenbank migriert, die durch den Produktschlüssel eingeschränkt sind. Fehlt dieser Parameter, werden alle Workflowdaten ungeachtet des Produktschlüssels migriert.

Protokolldatei

Beim Übertragen von Daten über eine Befehlszeile wird eine Protokolldatei erstellt.

Treiberdatei

Alle Treiberdateien sollten sich im Verzeichnis des Migrations-Tools befinden. Anderenfalls müssen Sie das Verzeichnis der JAR-Treiberdatei für die Datenbank angeben.

Ausführen des Migrations-Dienstprogramms über die GUI

So führen Sie die Migration über die GUI aus:

1. Geben Sie den folgenden Befehl in der Befehlszeile ein:

```
java -cp datamover.jar;migration.jar -Dwflog="c:\wf.log" -Dtxlimit=""  
com.ca.workflow.util.WFMigration
```

Das Dialogfeld für das Workflow Data Migrations-Tool wird angezeigt.

2. Wählen Sie sowohl für die Quell- als auch für die Zieldatenbank den Datenbanktyp aus dem Dropdownmenü "Datenbanktyp" aus.

Treibernamen und URLs werden automatisch aktualisiert. Diese Werte können Sie bei Bedarf ändern.

- Für Ingres: -ijdbc.jar
- Für Oracle 10g: ojdbc14.jar
- Für Oracle 11g: ojdbc5.jar
- Für MS SQL 2000: msutil.jar, msbase.jar, mssqlserver.jar
- Für MS SQL 2005: sqljdbc.jar
- Für Sybase Adaptive Server Enterprise 12.5.4: jconn3.jar
- Für Sybase Adaptive Server Enterprise 15.0: jconn3.jar

Wichtig! Eine Liste der unterstützten Datenbanken für CA SDM finden Sie in den *Versionshinweisen*.

3. Füllen Sie die gewünschten Felder aus.
4. Klicken Sie auf „Starten“

Die Datenmigration beginnt. Unten im Dialogfenster wird während der Migration der Status laufend aktualisiert.

Planen der Integration von CA Process Automation

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

Berücksichtigen Sie bei der Planung der CA Process Automation-Integration die folgenden Gesichtspunkte:

- Planen Sie genügend Zeit zum Installieren und Konfigurieren des CA Process Automation-Produkts ein.

- Prüfen Sie, ob CA Process Automation und CA SDM auf einem einzigen Server gemeinsam ausgeführt werden können, wenn die Serverarchitektur beide Produkte unterstützt. Wenn CA Process Automation- oder CA SDM-Komponenten nicht auf dem gleichen Server ausgeführt werden können, sollten Sie die Produkte auf getrennten Servern installieren.
- Planen Sie Zeit ein, um zu prüfen, dass beide Produkte installiert sind und unabhängig voneinander funktionieren.
- Wenn CA SDM in CA Process Automation integriert wird, welches CA EEM 8.4 verwendet, müssen Sie das CA EEM 8.4 SDK-Patch auf CA SDM anwenden. Die Patchdetails finden Sie bei CA Support Online.

Hinweis: Informationen über Produktvoraussetzungen für CA SDM und CA Process Automation finden Sie in den *CA SDM Versionshinweisen*. Informationen über die von CA Process Automation unterstützten Plattformen, erforderlichen Schritte und Installationsoptionen finden Sie in der CA Process Automation-Dokumentation zur Installation und Konfiguration.

Sicherheitsempfehlungen

Zusätzlich zu den angegebenen Mindestanforderungen in den Versionshinweisen sollten Sie die folgenden Empfehlungen für die CA Process Automation-Installation in Erwägung ziehen:

- Konfigurieren Sie CA Process Automation für die Verwendung von CA EEM als Authentifizierungsserver. CA EEM löscht Användernamen und Kennwörter im Nur-Text-Format, damit sie nicht zu Authentifizierungszwecken weitergegeben werden.
- Wenn Sie mehrere Mandanten für CA Process Automation verwenden, ist die CA EEM-Installation erforderlich.

Hinweis: Informationen zur Implementierung von mehreren Mandanten für CA Process Automation finden Sie in der CA Process Automation-Installations- und Konfigurationsdokumentation.

- Wenn Sie mehrere Mandanten für CA SDM verwenden, ist die CA EEM-Installation erforderlich.

Hinweis: Wenn Sie nur einen Mandanten verwenden, ist die CA EEM-Konfiguration für CA SDM optional.

- Konfigurieren Sie CA Process Automation für die sichere Kommunikation über HTTPS. HTTPS-URLs verwenden SSL/TLS, um den Austausch im Nur-Text-Format zu löschen. So werden proprietäre und sonstige vertrauliche Daten vor einer versehentlichen oder bössartigen Freigabe geschützt.

Hinweis: Informationen zur Konfiguration von CA Process Automation für HTTPS finden Sie in der CA Process Automation-Installations- und Konfigurationsdokumentation.

Einrichten von SSL-Kommunikation mit CA Process Automation

Aus Sicherheitsgründen ziehen es manche CA Process Automation-Implementierer vor, CA Process Automation so zu installieren oder neu zu konfigurieren, dass SSL-Kommunikation angefordert wird. Wenn CA Process Automation für die Anforderung von SSL-Kommunikation konfiguriert wurde, benötigen integrierte Anwendungen wie CA SDM ein Zertifikat des CA Process Automation-Keystores für die Kommunikation.

Um SSL-Kommunikation mit CA Process Automation einzurichten, gehen Sie wie folgt vor:

1. Konfigurieren Sie die CA SDM-Optionen so, dass die CA Process Automation-HTTPS-Adresse verwendet wird.
2. Exportieren Sie das CA Process Automation-Keystore-Zertifikat in eine Datei, und kopieren Sie die Datei nach CA SDM.
3. Laden Sie die Zertifikatsdatei in CA SDM. Verwenden Sie dafür das CA SDM-Dienstprogramm "pdm_keystore_mgr".
4. Falls für Ihre CA SDM-Architektur zutreffend, aktualisieren Sie die Versionskontrolldateien, um den CA SDM Keystore an alle Sekundärserver zu senden.
5. Starten Sie CA SDM neu.

Aktivieren der Kommunikation bei SSL-fähigem CA Process Automation

Wenn CA Process Automation mit SSL kommuniziert, müssen Sie die CA SDM-Server für die Kommunikation mit CA Process Automation konfigurieren.

Führen Sie die folgenden Schritte aus, um Kommunikationen bei SSL-fähigem CA Process Automation zu aktivieren:

1. Überprüfen Sie, dass Sie CA Process Automation in einem Browser verwenden können, ohne CA SDM zu starten. Zeichnen Sie die CA Process Automation-URL auf und verwenden Sie sie als Referenz, wenn Sie die CA Process Automation-Workflow-Optionen im Optionsmanager konfigurieren.

2. Melden Sie sich bei CA SDM an und installieren oder ändern Sie die CA Process Automation-Workflow-Optionen im Optionsmanager. Verwenden Sie für jede der folgenden Optionen die Syntax "*https://server:8443*" anstelle von "*http://server:8080*" zum Erreichen der SSL-fähigen CA Process Automation-Anwendung. Wenn die CA Process Automation-Installation jedoch einen anderen Port anstelle des SSL-Ports "8443" verwendet, geben Sie die entsprechende Port-Nummer an.

- `caextwf_endpoint`
- `caextwf_processdisplay_url`
- `caextwf_worklist_url`

Hinweis: Wenn die Werte nicht den tatsächlichen CA Process Automation-Installationswerten entsprechen, kann CA SDM nicht mit CA Process Automation kommunizieren, und es tritt ein Laufzeitfehler ein. Überprüfen Sie, dass die Werte den tatsächlichen CA Process Automation-Installationswerten entsprechen, da das CA Process Automation-Installationsprogramm möglicherweise einen anderen Port als Port 8443 ausgewählt haben kann.

3. Suchen Sie auf dem CA Process Automation-Server die Einträge "KEYSTOREID" und "itpam.web.keystorealias" in der folgenden Datei:

`C:\Progra~1\ITPAM\server\c2o\.config\0asisConfig.properties`

4. Kopieren Sie "KEYSTOREID". Halten Sie den Wert "KEYSTOREID" bereit, um ihn nach der Ausgabe des Keytool-Befehls als Kennwort einzugeben.
5. Geben Sie auf dem CA Process Automation-Server den folgenden-Keytool-Befehl als eine Zeile an der Befehlszeile an:

```
C:\Progra~1\ca\sc\jre\1.6.0_00\bin\keytool.exe -keystore  
C:\Progra~1\ITPAM\server\c2o\.config\c2okeystore -export -alias  
<keystorealias> -file itpam.cer
```

Das Keytool-Dienstprogramm fordert Sie zur Eingabe eines Kennworts auf.

6. Fügen Sie den "KEYSTOREID"-Wert als Kennwort ein oder geben Sie ihn ein.

Das Keytool-Dienstprogramm verwendet den letzten Parameter ("*-file itpam.cer*") zum Erstellen einer Datei mit dem Namen "*itpam.cer*". Die Datei "*itpam.cer*" enthält die erforderlichen Zertifikatsinformationen für die Kommunikation mit CA SDM.

7. Verschieben Sie die Datei "*itpam.cer*" an einen der folgenden Speicherorte auf dem CA SDM-Server:

- (Windows) `%NX_ROOT%\bin`
- (UNIX) `$NX_ROOT/bin`

8. Importieren Sie die CA Process Automation-Zertifikatsinformationen in CA SDM, indem Sie den folgenden Befehl eingeben:
- (Windows) `pdm_perl %NX_ROOT%\bin\pdm_keystore_mgr.pl -import %NX_ROOT%\bin\itpam.cer`
- (UNIX) `pdm_perl $NX_ROOT/bin/pdm_keystore_mgr.pl -import $NX_ROOT/bin itpam.cer`

Das Skript "*pdm_keystore_mgr.pl*" generiert die Keystore-Datei an den folgenden Speicherorten:

- (Windows) `%NX_ROOT%\pdmconf\nx.keystore`
- (UNIX) `$NX_ROOT/pdmconf/nx.keystore`

9. Abhängig von der CA SDM-Konfiguration muss *nx.keystore* den folgenden CA SDM-Servern bereitgestellt werden:

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

Öffnen Sie die Datei "*server_secondary.ver*" von einem der folgenden Speicherorte aus:

- (Windows) `%NX_ROOT%\site\server_secondary.ver`
- (UNIX) `$NX_ROOT/site/server_secondary.ver`

10. Ändern Sie "*server_secondary.ver*" zur Versionskontrolle, indem Sie die folgenden Informationen hinzufügen:

```
[SSL_Keystore]
filename = "nx.keystore"
directory = "$NX_ROOT/pdmconf"
component_type = "file"
O_mode = "RW"
g_mode = "RW"
w_mode = "RW"
file_ctl
```

Hinweis: Informationen zur Verwaltung der Versionskontrolle finden Sie im *Administrationshandbuch*.

11. Starten Sie CA SDM neu.

Der CA SDM-Server kann mit der SSL-fähigen CA Process Automation-Anwendung kommunizieren.

Hinweis: Weitere Informationen zum Konfigurieren von CA Process Automation-Workflow-Optionen finden Sie in der *Online-Hilfe*.

Installationsplanung für CA Business Intelligence

Die folgenden Informationen unterstützen Sie beim Planen einer erfolgreichen CA Business Intelligence-Installation und Konfiguration. Damit suchen und erfassen Sie die richtigen Informationen.

- **Nachforschung:** Führen Sie die folgenden Schritte aus:
 - Lesen Sie die Versionshinweise, um die Voraussetzungen für CA Business Intelligence kennenzulernen.
 - Lesen Sie Ihre CA Business Intelligence-Dokumentation, einschließlich der zugehörigen Versionshinweise und optionalen Readme-Dateien (falls verfügbar).

Hinweis: Eine ausführliche Liste der unterstützten Umgebungen und Hardware-Voraussetzungen finden Sie in den Dokumenten zu den verschiedenen unterstützten Plattformen auf der CA Business Intelligence-DVD. Diese Dokumente enthalten spezifische Informationen zu Versions- und Patchvoraussetzungen für Webanwendungsserver, Webbrowser und Betriebssysteme.

- **Installationsstammverzeichnis:** Bestimmen Sie das Stammverzeichnis, in dem Sie CA Business Intelligence installieren wollen. Die Standardverzeichnisse lauten:
 - Für Rechner mit Windows 32-Bit: C:\Programme\CA\SC\CommonReporting3
 - Für x64-Computer: C:\Programme X(86)\CA\SC\CommonReporting3

Wenn dieses Verzeichnis nicht existiert, müssen Sie es vor dem Start der Installation erstellen.

- **Antivirussoftware:** Deaktivieren Sie vorübergehend alle Antivirusprogramme, die den Rechner, auf dem Sie CA Business Intelligence installieren, durchsuchen.
- **Unterstützte Anwendungsserver:** Die CA SDM-Integration mit CA Business Intelligence unterstützt nur Apache Tomcat als Anwendungsserver für CA Business Intelligence.
- **Webbrowser-Support:** CA Business Intelligence 3.2 SP5 unterstützt die folgenden Webbrowser:

Browser-Betriebssystem	Browser	JVM
Apple Mac OS X	Safari 5	Apple 1.6.0_xx
Microsoft Windows	Firefox 3.6	Sun 1.5.0._xx Sun 1.6.0_xx
	Firefox 8	Sun 1.6.0_xx
	Hinweis: Neue Firefox-Versionen werden ungefähr zwei Wochen nach der Version von Mozilla mit minimalen Tests unterstützt.	

Browser-Betriebssystem	Browser	JVM
	IE 6.0 SP3	Sun 1.5.0_xx Sun 1.6.0_02+
	IE 7.0	Sun 1.5.0_xx Sun 1.6.0_02+
	IE 8.0 Hinweis: Nur kompatibler Modus wird unterstützt.	Sun 1.6.0_xx
	IE 9.0 Hinweis: Nur kompatibler Modus wird unterstützt.	Sun 1.6.0_xx

Wichtig: Die CA Business Intelligence-Installation ist auf Windows-Plattformen nur für CA SDM r12.9 beschränkt. Sie können jedoch CA Business Intelligence auf allen unterstützten Betriebssystemen in CA SDM integrieren.

Weitere Informationen:

[Hinweise zu Berichten](#) (siehe Seite 130)

[Integrieren von CA Business Intelligence mit CA SDM](#) (siehe Seite 265)

Hinweise zu Berichten

Bevor Sie CA Business Intelligence installieren, lesen Sie die folgenden Informationen, um eine erfolgreiche Implementierung sicherzustellen.

- Eine Installation von CA Business Intelligence r3.2 (BusinessObjects Enterprise Version 3.1) ist erforderlich, um Berichte von CA SDM r12.9 anzuzeigen, die in dieser Version enthalten sind.
- CA Business Intelligence 2.1 (BusinessObjects Enterprise Version 2) wird nicht unterstützt.
- Sie können CA Business Intelligence 3.0 während des Aktualisierungsvorgangs von Version 12.1 auf Version 12.5 aufrüsten.
- Der Installationsablauf unterscheidet sich je nach ausgewähltem Installationstyp (anwenderspezifisch oder neu).
- Das BusinessObjects-Administratorkennwort muss sowohl für die Neuinstallation als auch für die anwenderspezifische Installation bekannt sein, bevor Sie das Installationsprogramm ausführen.
- Der Configuration Management Server (CMS) muss auf Port 6400 eingesetzt werden (Standard). Ansonsten scheitert die CA Business Intelligence-Konfiguration während des Setups.
- CA SDM-Anwender müssen der Administrator-Liste in CMS hinzugefügt werden, bevor sie die Berichte verwenden können.
- Wenn Sie Apache Tomcat 5.5.20 als Anwendungsserver für Business Objects installieren möchten, müssen Sie zusätzliche Konfigurationsschritte durchführen.
- SAP BusinessObjects-Anwender mit einer bestehenden Installation von BusinessObjects können entweder CA Business Intelligence installieren und konfigurieren (empfohlen) oder das installierte BusinessObjects nutzen.
- Wenn Sie auf InfoView mit Firefox zugreifen möchten, dann muss eine Firefox-Version verwendet werden, die von CA Business Intelligence 3.2 unterstützt wird.
- Die mit Business Objects bereitgestellte JRE-Version muss möglicherweise geändert und an Ihre Umgebung angepasst werden.
- Crystal Reports Explorer und Desktop Intelligence werden *nicht* unterstützt, auch wenn sie nach der CA Business Intelligence-Installation aufgerufen werden können.

Neuinstallation im Gegensatz zur benutzerdefinierten Installation (Windows)

Zwischen einer neuen Installation und einer benutzerdefinierten Installation bestehen einige Unterschiede. Die Installation unterscheidet sich je nach dem ausgewählten Installationstyp.

Neu

Installiert alle Komponenten auf einem Computer. Wählen Sie diesen Installationstyp für eine vollständige Implementierung mit allen Server- und Client-Komponenten auf einem Computer aus. Durch eine neue Installation wird Folgendes bereitgestellt:

- MySQL als Datenbank, in der Informationen von Central Management Server (CMS) gespeichert werden.
- Apache Tomcat als Anwendungsserver.

Hinweis: Für BusinessObjects Enterprise müssen Informationen zu Benutzern, Gruppen, Sicherheitsstufen, BusinessObjects Enterprise-Inhalten und Servern in einer Datenbank gespeichert werden. Die primäre Datenbank wird vom CMS verwaltet und ist als CMS-Datenbank bekannt. Während der Installation von CA Business Intelligence geben Sie den zu verwendenden CMS und die erforderlichen Parameter für die Authentifizierung ein. Weitere Informationen über CMS-Datenbankanforderungen und Vorbereitung finden Sie im *Implementierungshandbuch zu CA Business Intelligence*.

Benutzerdefiniert

Installiert die von Ihnen ausgewählten Komponenten auf dem Computer. Wählen Sie diesen Installationstyp aus, um anzugeben, welche Komponenten bei einer verteilten Implementierung installiert werden sollen oder wenn Sie Server einer bestehenden Implementierung hinzufügen wollen.

Wichtig! Wählen Sie die benutzerdefinierte Installation, wenn Sie BusinessObjects CMS für eine Microsoft SQL- oder Oracle-Datenbank installieren möchten.

Eine benutzerdefinierte Installation bietet die folgenden Optionen:

Installieren Sie MySQL, oder verwenden Sie ein bereits bestehendes CMS mit:

- Oracle
- Microsoft SQL
- Apache Tomcat — Sie können die Installation der Apache Tomcat-Instanz steuern.

Anmeldeinformationen für den BusinessObjects-Administrator

Das BusinessObjects-Administratorkennwort muss sowohl für die Neuinstallation als auch für die benutzerdefinierte Installation bekannt sein, bevor Sie das Installationsprogramm ausführen.

Dieses Kennwort muss Groß- und Kleinbuchstaben enthalten, mindestens sechs Zeichen lang sein und darf in keiner Form das Wort Administrator enthalten. Es sollte zudem mindestens zwei der folgenden Zeichentypen aufweisen:

- Großbuchstaben
- Kleinbuchstaben
- Numerisch
- Satzzeichen

Anwendungsserver von BusinessObjects Enterprise XI

BusinessObjects Enterprise benötigt einen Anwendungsserver zur Verarbeitung der Server-Skripte, aus denen Web-Anwendungen bestehen.

Während der Installation von CA Business Intelligence geben Sie den zu verwendenden Anwendungsserver an und geben die erforderlichen Konfigurationsparameter ein. CA Business Intelligence bietet die Option zum Installieren von Apache Tomcat 5.5.20. Sie können auch ihren vorhandenen Anwendungsserver nutzen.

Wenn Sie Apache Tomcat 5.5.20 zur Nutzung als Anwendungsserver für BusinessObjects installieren möchten, gehen Sie folgendermaßen vor:

- Installieren Sie die Java 2 Standard Edition JDK 1.5.
- Setzen Sie die Umgebungsvariable "\$JAVA_HOME" auf das JDK 1.5-Stammverzeichnis.
- Installieren Sie Apache Tomcat 5.5.20 und setzen Sie den Pfad für die Java Virtual Machine auf das Verzeichnis, in dem Java 2 Standard Edition JRE 1.6 auf Ihrem System installiert ist.
- Führen Sie eine anwenderspezifische Installation für CA Business Intelligence durch.
- Wählen Sie im Bildschirm "Webserverkonfiguration" "Nein", wenn Sie dazu aufgefordert werden, Tomcat für BusinessObjects XI neu zu installieren.
- Wählen Sie Tomcat aus der Liste der Anwendungsserver aus.
- Geben Sie den Speicherort des Apache Tomcat 5.5.20-Webservers im Feld "Installationsverzeichnis" ein, und führen Sie die Installation durch.
- Nachdem Sie die Installation von CA Business Intelligence abgeschlossen haben, führen Sie die CA Business Intelligence-Konfiguration aus.

Hinweis: Wenn Sie CA Business Intelligence bereits mit JDK 1.5 installiert haben (mit einem nicht standardmäßigen externen Anwendungsserver) und JRE 1.6 in einer Client-Umgebung implementieren wollen, um auf das InfoView Web Intelligence-Tool zuzugreifen, dürfen Sie bei der Aufforderung JRE 1.4.2 nicht installieren. Installieren Sie statt dessen JRE 1.6 in der Client-Umgebung. Starten Sie, falls zutreffend, Ihren Browser nach der Installation von JRE 1.6 erneut. Sie können JRE 1.6 von der Oracle-Website herunterladen.

Vorhandene Installation von BusinessObjects (SAP)

Für Benutzer von SAP BusinessObjects wird Folgendes empfohlen: Wenn BusinessObjects nicht über CA Business Intelligence installiert wurde, sollten Sie aus Gründen einer maximalen Kompatibilität und Unterstützung CA Business Intelligence installieren und konfigurieren. Wenn Sie jedoch Ihre vorhandene BusinessObjects-Installation vorziehen, können Sie die Installationsschritte für CA Business Intelligence überspringen und mit diesem Abschnitt fortfahren: Konfigurieren von CA Business Intelligence.

Hinweis: Sie müssen BusinessObjects Enterprise Version 3 verwenden und Tomcat als Anwendungsserver implementiert haben. Darüber hinaus müssen Sie eine Lizenz für Web Intelligence besitzen. Für Crystal Reports benötigen Sie mindestens eine Laufzeitlizenz.

Zugreifen auf Infoview mit Firefox

Wenn Sie beabsichtigen, auf BusinessObjects Infoview über Firefox zuzugreifen, müssen Sie Firefox 2 mit Java Virtual Machine (Java Runtime) 1.5.0_xx und 1.6.0_02+ verwenden.

Hinweis: Weitere Informationen zu unterstützten Plattformen und Versionsnummern finden Sie im *Handbuch BusinessObjects Enterprise XI für Windows*.

Best Practices bei der Berichtserstellung

Verwenden Sie die folgenden Best Practices für das Installieren, Verwalten und Verwenden von CA Business Intelligence:

- Für jedes CA-Produkt sollten Sie ein Universum installieren und verwalten. Bei Bedarf können Sie verknüpfte Universen erstellen.
- Bevor Sie Service Packs, Patches und sonstige Aktualisierungen auf Ihr benutzerdefiniertes Universum anwenden, sollten Sie alle Anpassungen sichern.
- Ändern Sie das Standard-Universum nicht. Kopieren Sie es stattdessen, und ändern Sie die Kopie. Andernfalls kann es vorkommen, dass Ihre Anpassungen gelöscht werden, wenn Sie Service Packs, Patches und sonstige Aktualisierungen anwenden.
- Erstellen Sie Ihre eigenen Ordner.
- Wenn keine Berichte mehr ausgeführt werden, überprüfen Sie, dass der Central Management Server (CMS) läuft.
- Überschreiben Sie vordefinierte Berichte nicht.
- Verwenden Sie einen vordefinierten Bericht immer als eine Grundlage zum Erstellen eines benutzerdefinierten Berichts. Dadurch wird eine einheitliche Formatierung aller Berichte sichergestellt.

Hinweis: Einzelheiten zu diesen Aufgaben finden Sie in der BusinessObjects Enterprise-Dokumentation.

Implementierungsstrategien

Berücksichtigen Sie bei der Planung Ihrer CA Service Desk-Implementierungsstrategie neben Netzwerkverfügbarkeit, nutzbare Bandbreite und Antwortzeiten auch die folgenden Informationen.

- **Zentralisierte Implementierung:** Alle Produktkomponenten werden auf einem Primärserver installiert und konfiguriert. Das ist die Standardinstallation. Sie können zwar mehrere Objektmanager und Web-Engines für Lastverteilung und Failover implementieren, doch bei zunehmendem Geschäftsvolumen reicht diese Implementierung möglicherweise nicht mehr aus.

- **Verteilte Implementierung:** Die Produktkomponenten werden auf Client-nahen Servern installiert, die den Dienst in Anspruch nehmen. In der Geschäftsstelle eines Unternehmens mit mehreren Subnetzen nutzen beispielsweise viele Analysten den Webclient. Der Einsatz eines sekundären Servers in dieser Geschäftsstelle reduziert sowohl den Netzwerkverkehr als auch die Antwortzeiten. Da der sekundäre Server auch Caching-Funktionen ausführt, entsteht zwischen der Geschäftsstelle und dem Standort des Primärservers weniger Netzwerkverkehr. Diese Art der Implementierung unterstützt den Einsatz mehrerer Objektmanager und Web-Engines für Lastverteilung und Failover.
- **Globale Implementierung:** Diese besteht aus mindestens zwei zentralisierten oder verteilten Implementierungen, die als Regionen bekannt sind. Der Primärserver einer Region repliziert einen kleinen Anteil der Informationen einer Master-Region. Auf diese Weise kann eine einzelne Region über alle erforderlichen Informationen zu allen anderen Regionen verfügen. Ein Analyst hat dadurch Zugang zu Tickets aus allen Regionen, stellt die Verbindung zu einer Region jedoch nur her, falls es erforderlich wird. Diese Implementierung ist dann nützlich, wenn die Netzwerkbandbreite für eine verteilte Implementierung nicht ausreicht. Möglicherweise liegen manche Ihrer Unternehmensstandorte in verschiedenen Ländern, zwischen denen nur eine langsame Verbindung besteht.

Hinweis: Weitere Informationen finden Sie unter [CA Service Desk-Architektur für erweiterte Verfügbarkeit](#) (siehe Seite 89).

Aktivieren der Windows-Authentifizierung in Firefox

Mit der NT LAN Manager (NTLM)-Authentifizierung werden die Anmeldeinformationen eines in der Windows-Domäne angemeldeten Windows-Benutzers automatisch an einen IIS-Webserver in derselben Domäne weitergeleitet. Standardmäßig ist die Windows-Authentifizierung in Firefox nicht aktiviert. Zur Vorbereitung Ihrer Implementierung sollten Sie die Windows-Authentifizierung in Firefox aktivieren.

So aktivieren Sie die Windows-Authentifizierung in Firefox:

1. Starten Sie Firefox.
2. Navigieren Sie zur folgenden URL:
about:config
3. Bestätigen Sie, dass Sie die erweiterten Einstellungen ändern wollen.
Die Liste der voreingestellten Namen wird angezeigt.
4. Suchen Sie den voreingestellten Namen *network.automatic-ntlm-auth.trusted-uris*, und doppelklicken Sie darauf:
Das Dialogfeld "Geben Sie einen String-Wert ein" wird angezeigt.

5. Geben Sie die Liste der vertrauenswürdigen Sites durch Eingabe der vollständigen URL (z. B. `http://web.example.com`) oder des Servernamens an (z. B. `web.example.com`)

Hinweis: Geben Sie keinen abschließenden Schrägstrich ein. Wenn Sie mehrere Server angeben möchten, trennen Sie diese durch ein Komma. Sie können alle Server in einer bestimmten Domäne angeben, die üblichen Platzhalter funktionieren jedoch nicht. Beispielsweise geben Sie *.example.com* anstelle von **.example.com* an.

6. Klicken Sie auf "OK".
7. Starten Sie Firefox erneut.

Kapitel 4: Wird installiert

Dieses Kapitel enthält folgende Themen:

- [Implementieren der Software](#) (siehe Seite 137)
- [So konfigurieren Sie CA SDM-Server](#) (siehe Seite 138)
- [So führen Sie eine Konvertierung von der konventionellen Konfiguration in eine Konfiguration für erweiterte Verfügbarkeit durch](#) (siehe Seite 146)
- [So führen Sie eine Konvertierung von der Konfiguration für erweiterte Verfügbarkeit in eine konventionelle Konfiguration durch](#) (siehe Seite 152)
- [So installieren Sie CA MDB](#) (siehe Seite 156)
- [So installieren Sie CA SDM](#) (siehe Seite 165)
- [So installieren Sie Web Screen Painter](#) (siehe Seite 181)
- [So installieren und konfigurieren Sie die CA SDM- und CA NSM-Integration](#) (siehe Seite 182)
- [So installieren Sie CA EEM](#) (siehe Seite 230)
- [So installieren Sie CA Workflow](#) (siehe Seite 233)
- [So installieren Sie CA Business Intelligence für CA SDM](#) (siehe Seite 237)
- [Überprüfen der Installation](#) (siehe Seite 241)
- [Das Installationsprotokoll](#) (siehe Seite 242)

Implementieren der Software

Die Implementierung von CA SDM erfolgt auf Basis verschiedener Faktoren, u. a. der folgenden: Handelt es sich um eine Aktualisierung einer früheren Version? Installieren Sie das Produkt zum ersten Mal? Welches Betriebssystem und welche Datenbank nutzen Sie? Welche Produkte möchten Sie integrieren? Im Allgemeinen befolgen Sie die aufgeführten Schritte, um die Software zu implementieren

1. Lesen Sie die Hinweise zur Implementierung, die in den *Versionshinweisen* dokumentiert sind.
2. Wenn Sie von einer früheren Version *aktualisieren*, gehen Sie wie im Folgenden beschrieben vor, um die Datenbank, die Konsole und CA Workflow zu aktualisieren.
3. Installieren Sie die CA MDB.

Wenn Ihre Datenbank (SQL Server oder Oracle) auf einem anderen Server als dem CA SDM-Primärserver installiert ist, sollten Sie die CA MDB auf dem Remote-Datenbankserver installieren (d. h. der Computer, auf dem SQL Server oder Oracle installiert ist). Wenn sich die CA MDB und der Primärserver auf dem selben Computer befinden, wird die CA MDB automatisch installiert.
4. Installieren Sie CA SDM auf dem primären Server oder dem optionalen sekundären Server.

Webformulare und das Schema können Sie nach der Installation anpassen, da Web Screen Painter automatisch auf dem Server installiert wird.

5. (Optional) Aktivieren Sie den CA CMDB Visualizer während der CA SDM-Konfiguration.
6. (Optional) Aktivieren Sie Support-Automatisierung während der CA SDM-Konfiguration.

Wichtig! Wenn Sie in CA Support-Automatisierung r6.0 SR1 eFix5 Bereiche zu Mandanten migrieren wollen, konvertieren Sie diese Daten vor dem Aktivieren und Konfigurieren von Support-Automatisierung in CA SDM r12.9.

7. (Optional) Aktivieren Sie während der CA SDM-Konfiguration die REST-API.
8. (Optional) Installieren Sie CA EEM für die Authentifizierung.
9. (Optional) Installieren Sie CA Workflow zum Verwalten Ihrer Geschäftsprozesse.
10. (Optional) Installieren Sie CA Business Intelligence, um Berichte mit der BusinessObjects-Technologie zu verwalten.
11. (Optional) Installieren Sie die CA NSM-Integration.

Weitere Informationen:

[So installieren Sie CA EEM](#) (siehe Seite 230)
[So installieren Sie CA Workflow](#) (siehe Seite 233)
[So installieren Sie CA MDB](#) (siehe Seite 156)
[Das Installationsprotokoll](#) (siehe Seite 242)
[So installieren Sie CA SDM](#) (siehe Seite 165)
[Überprüfen der Installation](#) (siehe Seite 241)
[Starten der Web-Schnittstelle](#) (siehe Seite 252)

So konfigurieren Sie CA SDM-Server

Als Systemadministrator konfigurieren Sie die CA SDM-Server für die erweiterte Verfügbarkeit unter folgenden Umständen:

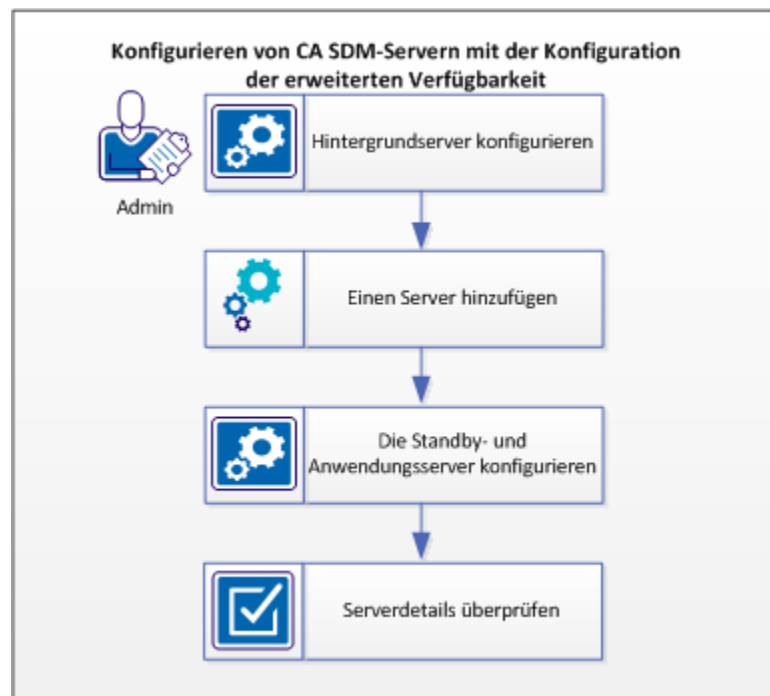
- Sie haben eine neue Installation von CA SDM durchgeführt, und Sie möchten die Konfiguration für erweiterte Verfügbarkeit oder die konventionelle Konfiguration implementieren.
- Sie haben ein Upgrade auf die neueste CA SDM-Version durchgeführt, und Sie möchten die konventionelle Konfiguration für erweiterte Verfügbarkeit implementieren.

Hinweis: Wenn Sie CA SDM mit einer bestimmten Konfiguration installiert oder aktualisiert haben (zum Beispiel konventionell), und Sie möchten die andere Konfiguration implementieren (zum Beispiel erweiterte Verfügbarkeit), finden Sie weitere Informationen in den Konvertierungsszenarien oder im *Implementierungshandbuch*.

Das folgende Diagramm zeigt, wie CA SDM-Server in konventioneller Konfiguration konfiguriert werden:



Das folgende Diagramm zeigt, wie CA SDM-Server in der Konfiguration der erweiterten Verfügbarkeit konfiguriert werden:



Gehen Sie wie folgt vor:

1. Führen Sie abhängig von Ihrer CA SDM-Konfiguration folgende Schritte durch:
 - [Konfigurieren Sie den Primärserver](#) (siehe Seite 140).
 - [Konfigurieren des Hintergrundservers](#) (siehe Seite 142)
2. [Fügen Sie einen Server hinzu](#) (siehe Seite 140), wenn Sie keinen vorhandenen Server haben.
3. Führen Sie abhängig von Ihrer CA SDM-Konfiguration folgende Schritte durch:
 - [Konfigurieren Sie den Sekundärserver](#) (siehe Seite 142).
 - [Konfigurieren der Standby-Server und Anwendungsserver](#) (siehe Seite 143)
4. [Überprüfen Sie die Serverdetails](#). (siehe Seite 145)

Konfigurieren des Primärservers

Der Primärserver muss konfiguriert werden, bevor Sie Sekundärserver konfigurieren.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei dem Server an, den Sie als Primärserver konfigurieren wollen.
2. Verwenden Sie den `pdm_configure`-Befehl, um die Konfiguration zu starten.
Das Fenster zur Auswahl der Serverkonfiguration wird geöffnet.
3. Wählen Sie "Konventionell" als Konfigurationstyp aus, und befolgen Sie die Eingabeaufforderungen, um die Konfiguration abzuschließen. Weitere Informationen zur Konfiguration finden Sie in der *Hilfe zur Serverkonfiguration*.
Der Primärserver ist jetzt konfiguriert.

Hinzufügen eines Servers

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

Gehen Sie wie folgt vor:

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

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

Erstellen von Serverfeldern

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

Hostname

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

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

Zeitzone

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

Datensatzstatus

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

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

Servertyp

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

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

Konfiguriert

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

Konfigurieren der Sekundärserver

Sie konfigurieren jeden Sekundärserver, nachdem Sie den Primärserver konfiguriert haben. Diese Konfiguration ist erforderlich, um die Kommunikation mit dem Primärserver herzustellen.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei dem Server an, den Sie als Sekundärserver konfigurieren wollen.
2. Verwenden Sie den `pdm_configure`-Befehl, um die Konfiguration zu starten.
Das Fenster zur Auswahl der Serverkonfiguration wird geöffnet.
3. Wählen Sie "Konventionell" als Konfigurationstyp aus, und befolgen Sie die Eingabeaufforderungen, um die Konfiguration abzuschließen. Weitere Informationen finden Sie in der *Hilfe zur Serverkonfiguration*.
Der Sekundärserver ist jetzt konfiguriert.
4. Wiederholen Sie die Schritte 1 bis 3 auf allen Servern, die Sie als Sekundärserver konfigurieren möchten.

Konfigurieren des Hintergrundservers

Konfigurieren Sie den Hintergrundserver, bevor Sie die Anwendungsserver oder Standby-Server konfigurieren.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei dem Server an, den Sie als der Hintergrundserver konfigurieren wollen.

2. Verwenden Sie den `pdm_configure`-Befehl, um die Konfiguration zu starten.
Das Fenster zur Auswahl der Serverkonfiguration wird geöffnet.
3. Wählen Sie "Erweiterte Verfügbarkeit" als Konfigurationstyp aus, und befolgen Sie die Eingabeaufforderungen, um die Konfiguration abzuschließen. Weitere Informationen finden Sie in der *Hilfe zur Serverkonfiguration*.
Der Hintergrundserver ist jetzt konfiguriert.

Konfigurieren der Standby-Server oder Anwendungsserver

Sie konfigurieren alle Standby-Server und Anwendungsserver, nachdem Sie den Hintergrundserver konfigurieren. Diese Konfiguration ist erforderlich, um die Kommunikation mit dem Hintergrundserver herzustellen.

Wichtig! (Empfohlen) Stellen Sie sicher, dass sowohl die Hintergrundserver als auch alle anderen Standby-Server ähnlich konfiguriert sind. Dieser Vorgang stellt sicher, dass ein Standby-Server, der während eines Failover als neuer Hintergrundserver festgelegt wird, genau wie der alte Hintergrundserver funktioniert.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei dem Server an, den Sie als Standby-Server oder Anwendungsserver konfigurieren wollen.
2. Verwenden Sie den `pdm_configure`-Befehl, um die Konfiguration zu starten.
Das Fenster zur Auswahl der Serverkonfiguration wird geöffnet.
3. Wählen Sie "Erweiterte Verfügbarkeit" als Konfigurationstyp aus, und befolgen Sie die Eingabeaufforderungen, um die Konfiguration abzuschließen. Weitere Informationen finden Sie in der *Hilfe zur Serverkonfiguration*.

4. Wiederholen Sie die Schritte 1 bis 3 auf allen Servern, die Sie als Standby-Server und Anwendungsserver konfigurieren möchten.

Sie haben die Standby-Server und Anwendungsserver konfiguriert.

5. Wenn Sie einzelne oder mehrere Anwendungsserver haben und einen Lastenausgleich verwenden möchten, um Anfragen an und von den verschiedenen Anwendungsservern zu verfolgen, konfigurieren Sie den [Lastenausgleich](#) (siehe Seite 144).

Hinweis: Um eine Lastenausgleichs-URL oder eine Anwendungsserver-URL für die Verknüpfungen in den CA SDM-Benachrichtigungen zu verwenden, führen Sie die folgenden Schritte aus:

- a. Melden Sie sich am Hintergrundserver an.
- b. Wählen Sie auf der Registerkarte "Administration" die Option "Optionsmanager", "Benachrichtigungen".
- c. Ändern Sie den Wert der web_cgi_url-Option folgendermaßen:
 - Auf den Lastenausgleich, wenn Sie mehr als einen Anwendungsserver haben.
 - Auf den Anwendungsserver, wenn Sie nur einen Anwendungsserver haben.

Konfigurieren des Lastenausgleichs

Wenn Sie einzelne oder mehrere Anwendungsserver haben, konfigurieren Sie den Lastenausgleich, um die Anwendungsserver zu überwachen.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei einem Anwendungsserver an.
2. Kopieren Sie die HealthServlet.war-Datei vom \$NX_ROOT/samples/HealthServlet-Verzeichnis zum \$NX_ROOT/bopcfg/www/CATALINA_BASE/webapps-Verzeichnis.
3. Starten Sie CA SDM-Services neu, oder starten Sie CA SDM-Tomcat neu.
4. Wiederholen Sie die Schritte 1 bis 3 für alle anderen Anwendungsserver.
5. Konfigurieren Sie den Lastenausgleich, um die folgende healthservlet-URL auf jedem Anwendungsserver zu überwachen:

`http://<Machine_name>:<Port_number>/HealthServlet/GetHealth`

- Wenn eine Stilllegungs-Antwort von der healthservlet-URL eines Anwendungsservers eingeht, muss der Lastenausgleich alle Anfragen von diesem Server an die anderen Anwendungsserver umleiten. Zum Beispiel wird die folgende Antwort bekommen, wenn der Anwendungsserver für 58677 Sekunden stillgelegt ist.

Verbleibende Stilllegungszeit :58677 Sekunden

- Wenn ein Anwendungsserver gesund ist und keine Stilllegung erforderlich ist, wird die folgende Antwort vom healthservlet des Servers bekommen:

Derzeit ist keine Stilllegungszeit festgelegt. Rückgabecode : -1

6. Konfigurieren Sie die Aufrechterhaltung der Sitzungen auf jedem Lastenausgleich. Dieser Prozess garantiert, dass eine von einem bestimmten Anwendungsserver kommende Anfrage an den gleichen Server zurückgeleitet wird.

Überprüfen der Serverdetails

Nachdem Sie alle Server konfiguriert haben, stellen Sie sicher, dass alle Server richtig konfiguriert und verfügbar sind.

(Für die Konfiguration für erweiterte Verfügbarkeit)Gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass alle Hintergrundserver, Standby-Server und Anwendungsserver ausgeführt werden.
2. Melden Sie sich an der Web-Schnittstelle des Hintergrundservers an.
3. Wählen Sie auf der Registerkarte "Administration" die Option "System", "Server" aus.

Die Seite "Server - Liste" wird geöffnet.

4. Stellen Sie sicher, dass das Feld "Konfiguriert" den Wert "Ja" für die Datensätze der Standby-Server und Anwendungsserver anzeigt.
5. Wenn "Datensatzstatus" auf "Inaktiv" festgelegt ist, bearbeiten Sie den Server, und legen Sie "Aktiv" fest. Wenn Sie den Datensatzstatus eines Servers ändern, konfigurieren Sie ihn neu.

Sie haben die Server erfolgreich für die erweiterte Verfügbarkeit konfiguriert.

Hinweis: Sie können auf eine Eingabe des lokalen Hosts auf der Seite der Serverdetails klicken, um die Details des Servers anzuzeigen.

(Für die konventionelle Konfiguration) Gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass der Primärserver und alle Sekundärserver ausgeführt werden.
2. Melden Sie sich an der Web-Schnittstelle des Primärservers an.
3. Wählen Sie auf der Registerkarte "Administration" die Option "System", "Server" aus.

Die Seite "Server - Liste" wird geöffnet.

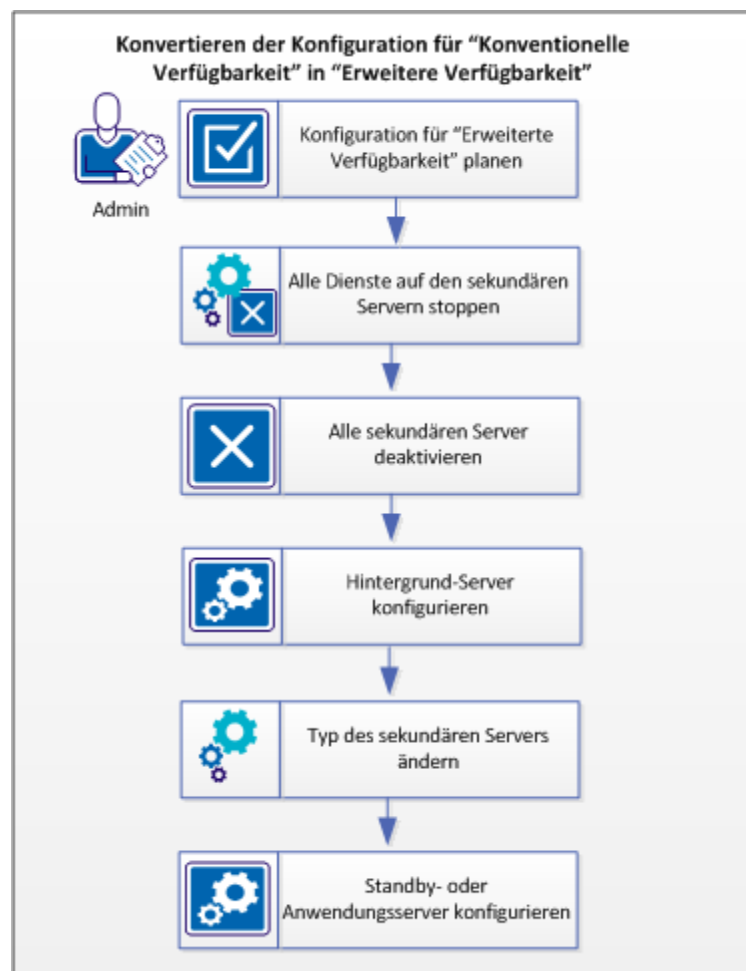
4. Wenn "Datensatzstatus" auf "Inaktiv" festgelegt ist, bearbeiten Sie den Server, und legen Sie "Aktiv" fest. Wenn Sie den Datensatzstatus ändern, stellen Sie sicher, dass Sie diesen Server neu konfigurieren.

Sie haben die Server erfolgreich konfiguriert.

So führen Sie eine Konvertierung von der konventionellen Konfiguration in eine Konfiguration für erweiterte Verfügbarkeit durch

Bevor Sie eine Konvertierung von der konventionellen Konfiguration in eine Konfiguration für erweiterte Verfügbarkeit durchführen, stellen Sie sicher, dass Sie ein Upgrade auf CA SDM r12.9 durchgeführt haben oder dass CA SDM r12.9 auf allen Servern installiert ist.

Folgendes Diagramm zeigt, wie eine Konvertierung von der konventionellen Konfiguration in eine Konfiguration für erweiterte Verfügbarkeit durchgeführt wird:



Gehen Sie wie folgt vor:

1. Planen Sie die Konfiguration für erweiterte Verfügbarkeit. Weitere Informationen finden Sie im Planungsszenario oder im *Implementierungshandbuch*.
2. Halten Sie alle Services auf den Sekundärservern an.
3. [Deaktivieren Sie alle Sekundärserver](#) (siehe Seite 147).
4. [Konfigurieren Sie den Hintergrundserver](#) (siehe Seite 148).
5. [Ändern Sie den Sekundärservertyp](#) (siehe Seite 148).
6. Konfigurieren Sie den Standby-Server oder den Anwendungsserver.
7. Überprüfen Sie die Serverdetails. (siehe Seite 150)

Deaktivieren aller Sekundärserver

Bevor Sie die Server für die Konfiguration für erweiterte Verfügbarkeit konfigurieren, stellen Sie sicher, dass Sie alle Sekundärserver deaktivieren.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei der Web-Benutzeroberfläche des Primärservers an.
2. Wählen Sie auf der Registerkarte "Administration" die Option "System", "Server" aus.

Die Seite "Server - Liste" wird geöffnet.

3. Klicken Sie auf den Hostnamen des Sekundärservers.

Die Seite "Server - Detail" wird geöffnet.

4. Klicken Sie auf "Bearbeiten".
5. Ändern Sie den Datensatzstatus in "Inaktiv".

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

6. Klicken Sie auf "Speichern".
Der Sekundärserver wird auf "Inaktiv" gesetzt.
7. Führen Sie die Schritte 3 bis 6 für alle anderen Sekundärserver aus.

Alle Sekundärserver werden auf "Inaktiv" gesetzt.

Konfigurieren des Hintergrundservers

Konfigurieren Sie den Hintergrundserver, bevor Sie die Anwendungsserver oder Standby-Server konfigurieren.

Gehen Sie wie folgt vor:

1. Melden Sie sich beim Primärserver an.
2. Verwenden Sie den `pdm_configure`-Befehl, um die Konfiguration zu starten.
Das Fenster zur Auswahl der Serverkonfiguration wird geöffnet.
3. Wählen Sie "Erweiterte Verfügbarkeit" als Konfigurationstyp aus, und befolgen Sie die Eingabeaufforderungen, um die Konfiguration abzuschließen. Weitere Informationen finden Sie in der *Hilfe zur Serverkonfiguration*.

Der Hintergrundserver ist jetzt konfiguriert.

Ändern des Sekundärservertyps

Nachdem Sie den Hintergrundserver konfiguriert haben, ändern Sie den Servertyp für alle Sekundärserver in Anwendungsserver und Standby-Server, und aktivieren Sie sie.

Gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass der Hintergrundserver ausgeführt wird.
2. Melden Sie sich bei der Web-Benutzeroberfläche des Hintergrundservers an.
3. Wählen Sie auf der Registerkarte "Administration" die Option "System", "Server" aus.

Die Seite "Server - Liste" wird geöffnet.

4. Legen Sie den Datensatzstatus für alle Sekundärserver auf "Aktiv" fest.
5. Ändern Sie den Servertyp aller Sekundärserver in Anwendungsserver oder Standby-Server, falls erforderlich.

Der Servertyp aller Sekundärserver wurde geändert.

Konfigurieren der Standby-Server und Anwendungsserver

Sie konfigurieren alle Standby-Server und Anwendungsserver, nachdem Sie den Hintergrundserver konfigurieren. Diese Konfiguration ist erforderlich, um die Kommunikation mit dem Hintergrundserver herzustellen.

Wichtig! (Empfohlen) Stellen Sie sicher, dass sowohl die Hintergrundserver als auch alle anderen Standby-Server ähnlich konfiguriert sind. Dieser Vorgang stellt sicher, dass ein Standby-Server, der während eines Failover als neuer Hintergrundserver festgelegt wird, genau wie der alte Hintergrundserver funktioniert.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei einem Sekundärserver an.
2. Verwenden Sie den `pdm_configure`-Befehl, um die Konfiguration zu starten.
Das Fenster zur Auswahl der Serverkonfiguration wird geöffnet.
3. Wählen Sie "Erweiterte Verfügbarkeit" als Konfigurationstyp aus, und befolgen Sie die Eingabeaufforderungen, um die Konfiguration abzuschließen. Weitere Informationen finden Sie in der *Hilfe zur Serverkonfiguration*.
4. Wiederholen Sie die Schritte 1 bis 3 auf allen Servern, die Sie als Standby-Server und Anwendungsserver konfigurieren möchten.

Sie haben die Standby-Server und Anwendungsserver konfiguriert.

5. Wenn Sie einzelne oder mehrere Anwendungsserver haben und einen Lastenausgleich verwenden möchten, um Anfragen an und von den verschiedenen Anwendungsservern zu verfolgen, [konfigurieren Sie den Lastenausgleich](#) (siehe Seite 144).

Hinweis: Um eine Lastenausgleichs-URL oder eine Anwendungsserver-URL für die Verknüpfungen in den CA SDM-Benachrichtigungen zu verwenden, führen Sie die folgenden Schritte aus:

- a. Melden Sie sich am Hintergrundserver an.
 - b. Wählen Sie auf der Registerkarte "Administration" die Option "Optionsmanager", "Benachrichtigungen".
 - c. Ändern Sie den Wert der `web_cgi_url`-Option folgendermaßen:
 - Auf den Lastenausgleich, wenn Sie mehr als einen Anwendungsserver haben.
 - Auf den Anwendungsserver, wenn Sie nur einen Anwendungsserver haben.
6. [Überprüfen Sie die Serverdetails](#) (siehe Seite 150)

Konfigurieren des Lastenausgleichs

Wenn Sie einzelne oder mehrere Anwendungsserver haben, konfigurieren Sie den Lastenausgleich, um die Anwendungsserver zu überwachen.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei einem Anwendungsserver an.
2. Kopieren Sie die HealthServlet.war-Datei vom
\$NX_ROOT/samples/HealthServlet-Verzeichnis zum
\$NX_ROOT/bopcfg/www/CATALINA_BASE/webapps-Verzeichnis.
3. Starten Sie CA SDM-Services neu, oder starten Sie CA SDM-Tomcat neu.
4. Wiederholen Sie die Schritte 1 bis 3 für alle anderen Anwendungsserver.
5. Konfigurieren Sie den Lastenausgleich, um die folgende healthservlet-URL auf jedem Anwendungsserver zu überwachen:

`http://<Machine_name>:<Port_number>/HealthServlet/GetHealth`

- Wenn eine Stilllegungs-Antwort von der healthservlet-URL eines Anwendungsservers eingeht, muss der Lastenausgleich alle Anfragen von diesem Server an die anderen Anwendungsserver umleiten. Zum Beispiel wird die folgende Antwort bekommen, wenn der Anwendungsserver für 58677 Sekunden stillgelegt ist.

`Verbleibende Stilllegungszeit :58677 Sekunden`

- Wenn ein Anwendungsserver gesund ist und keine Stilllegung erforderlich ist, wird die folgende Antwort vom healthservlet des Servers bekommen:

`Derzeit ist keine Stilllegungszeit festgelegt. Rückgabecode : -1`

6. Konfigurieren Sie die Aufrechterhaltung der Sitzungen auf jedem Lastenausgleich. Dieser Prozess garantiert, dass eine von einem bestimmten Anwendungsserver kommende Anfrage an den gleichen Server zurückgeleitet wird.

Überprüfen der Serverdetails

Nachdem Sie alle Server konfiguriert haben, stellen Sie sicher, dass alle Server richtig konfiguriert und verfügbar sind.

Gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass alle Hintergrundserver, Standby-Server und Anwendungsserver ausgeführt werden.
2. Melden Sie sich an der Web-Schnittstelle des Hintergrundservers an.
3. Wählen Sie auf der Registerkarte "Administration" die Option "System", "Server" aus.

Die Seite "Server - Liste" wird geöffnet.

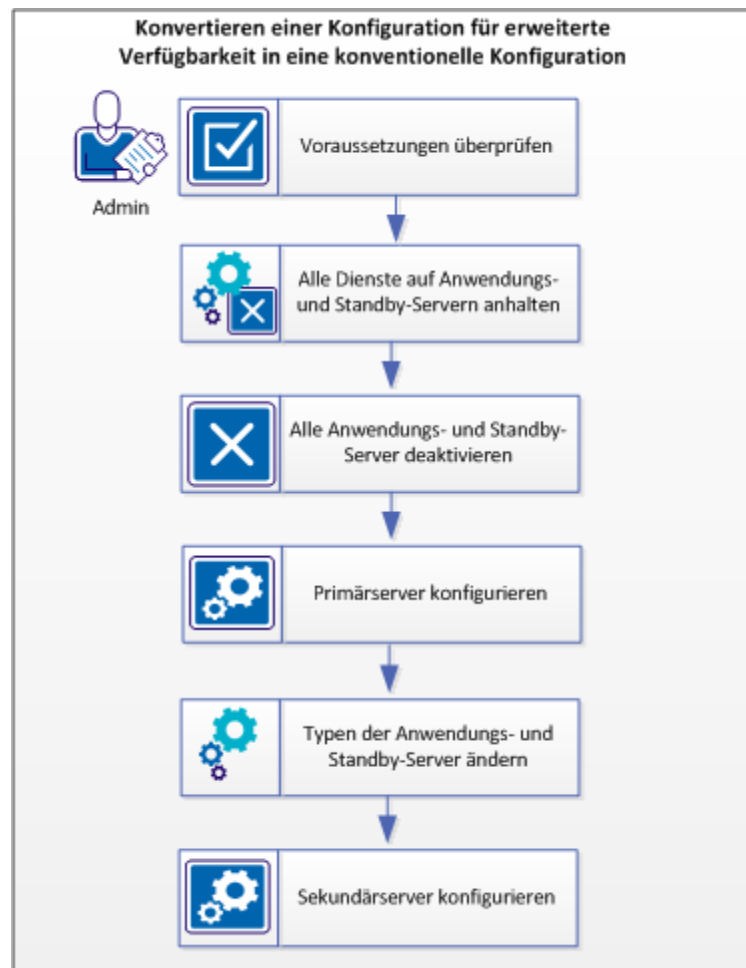
4. Stellen Sie sicher, dass das Feld "Konfiguriert" den Wert "Ja" für die Datensätze der Standby-Server und Anwendungsserver anzeigt.
5. Wenn "Datensatzstatus" auf "Inaktiv" festgelegt ist, bearbeiten Sie den Server, und legen Sie "Aktiv" fest. Wenn Sie den Datensatzstatus eines Servers ändern, konfigurieren Sie ihn neu.

Sie haben die Server erfolgreich für die erweiterte Verfügbarkeit konfiguriert.

Hinweis: Sie können auf eine Eingabe des lokalen Hosts auf der Seite der Serverdetails klicken, um die Details des Servers anzuzeigen.

So führen Sie eine Konvertierung von der Konfiguration für erweiterte Verfügbarkeit in eine konventionelle Konfiguration durch

Sie können von der Konfiguration für erweiterte Verfügbarkeit zur konventionellen Konfiguration zurückkehren. Folgendes Diagramm zeigt, wie eine Konvertierung von der Konfiguration für erweiterte Verfügbarkeit in eine konventionelle Konfiguration durchgeführt wird:



Gehen Sie wie folgt vor:

1. [Überprüfen der Voraussetzungen](#) (siehe Seite 153)
2. Halten Sie alle Dienste auf den Anwendungsserver und Standby-Servern an.
3. [Deaktivieren Sie alle Anwendungsserver und Standby-Server](#) (siehe Seite 153).
4. [Konfigurieren Sie den Primärserver](#) (siehe Seite 140).

5. [Ändern Sie den Typ der Anwendungsserver und Standby-Server](#) (siehe Seite 154).
6. [Konfigurieren Sie den Sekundärserver](#) (siehe Seite 142).
7. [Überprüfen der Serverdetails](#) (siehe Seite 155)

Überprüfen der Voraussetzungen

Überprüfen Sie folgende Voraussetzungen, bevor Sie eine Konvertierung in eine konventionelle Konfiguration durchführen:

1. Sie haben die konventionelle Konfiguration geplant. Weitere Informationen finden Sie im Planungsabschnitt des *Implementierungshandbuchs*.
2. Sie können nur den Hintergrundserver als Primärserver konfigurieren.
3. Sie können nur die Standby-Server und die Anwendungsserver als Sekundärserver konfigurieren.

Deaktivieren aller Anwendungsserver und Standby-Server

Bevor Sie die Server für die konventionelle Konfiguration konfigurieren, stellen Sie sicher, dass Sie alle Anwendungsserver und Standby-Server deaktivieren.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei der Web-Benutzeroberfläche des Hintergrundservers an.
2. Wählen Sie auf der Registerkarte "Administration" die Option "System", "Server" aus.
Die Seite "Server - Liste" wird geöffnet.
3. Klicken Sie auf den Hostnamen des Anwendungsservers.
Die Seite "Server - Detail" wird geöffnet.
4. Klicken Sie auf "Bearbeiten".
5. Ändern Sie den Datensatzstatus in "Inaktiv".

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

6. Klicken Sie auf "Speichern".
Der Anwendungsserver wird auf "Inaktiv" gesetzt.
7. Führen Sie die Schritte 3 bis 6 für alle anderen Anwendungsserver und Standby-Server aus.
Alle Anwendungsserver und Standby-Server werden auf "Inaktiv" festgelegt.

Konfigurieren des Primärservers

Der Primärserver muss konfiguriert werden, bevor Sie Sekundärserver konfigurieren.

Gehen Sie wie folgt vor:

1. Melden Sie sich an der Web-Schnittstelle des Hintergrundservers an.
2. Deaktivieren Sie den Hintergrundserver mithilfe der Web-Schnittstelle des Hintergrundservers.
3. Verwenden Sie den `pdm_configure`-Befehl, um die Konfiguration zu starten.
Das Fenster zur Auswahl der Serverkonfiguration wird geöffnet.
4. Wählen Sie "Konventionell" als Konfigurationstyp aus, und befolgen Sie die Eingabeaufforderungen, um die Konfiguration abzuschließen. Weitere Informationen zur Konfiguration finden Sie in der *Hilfe zur Serverkonfiguration*.
Der Primärserver ist jetzt konfiguriert.

Überprüfen der Serverdetails

Nachdem Sie den Primärserver konfiguriert haben, ändern Sie den Servertyp für alle Anwendungsserver und Standby-Server in Sekundärserver, und aktivieren Sie sie.

Gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass der Primärserver ausgeführt wird.
2. Melden Sie sich an der Web-Schnittstelle des Primärservers an.
3. Wählen Sie auf der Registerkarte "Administration" die Option "System", "Server" aus.
Die Seite "Server - Liste" wird geöffnet.

4. Legen Sie den Datensatzstatus für alle Anwendungsserver und Standby-Server auf "Aktiv" fest.
5. Ändern Sie den Servertyp von allen Anwendungsservern und Standby-Servern auf Sekundärserver.

Der Servertyp für alle Anwendungsserver und Standby-Server wurden geändert.

Konfigurieren der Sekundärserver

Sie konfigurieren jeden Sekundärserver, nachdem Sie den Primärserver konfiguriert haben. Diese Konfiguration ist erforderlich, um die Kommunikation mit dem Primärserver herzustellen.

Gehen Sie wie folgt vor:

1. Melden Sie sich beim Anwendungsserver oder beim Standby-Server an, den Sie als neuen Sekundärserver konfigurieren wollen.
2. Verwenden Sie den `pdm_configure`-Befehl, um die Konfiguration zu starten.

Das Fenster zur Auswahl der Serverkonfiguration wird geöffnet.

3. Wählen Sie "Konventionell" als Konfigurationstyp aus, und befolgen Sie die Eingabeaufforderungen, um die Konfiguration abzuschließen. Weitere Informationen finden Sie in der *Hilfe zur Serverkonfiguration*.

Der Sekundärserver ist jetzt konfiguriert.

4. Wiederholen Sie die Schritte 1 bis 3 auf allen Servern, die Sie als Sekundärserver konfigurieren möchten.

Überprüfen der Serverdetails

Nachdem Sie alle Server konfiguriert haben, stellen Sie sicher, dass alle Server richtig konfiguriert und verfügbar sind.

Gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass der Primärserver und alle Sekundärserver ausgeführt werden.
2. Melden Sie sich an der Web-Schnittstelle des Primärservers an.

3. Wählen Sie auf der Registerkarte "Administration" die Option "System", "Server" aus.

Die Seite "Server - Liste" wird geöffnet.

4. Wenn "Datensatzstatus" auf "Inaktiv" festgelegt ist, bearbeiten Sie den Server, und legen Sie "Aktiv" fest. Wenn Sie den Datensatzstatus ändern, stellen Sie sicher, dass Sie diesen Server neu konfigurieren.

Sie haben die Server erfolgreich konfiguriert.

So installieren Sie CA MDB

Hinweis: Bevor Sie diese Komponente installieren, stellen Sie sicher, dass Sie die [CA MDB-Installation planen](#) (siehe Seite 99).

Wichtig! Die Zuordnung des DVD-Image mit Hilfe eines UNC-Pfads wird durch das CA MDB-Installationsprogramm nicht unterstützt.

Wenn die Datenbank (SQL Server oder Oracle), die Sie mit CA SDM nutzen möchten, auf einem anderen als dem CA SDM-Primärserver installiert ist, müssen Sie die CA MDB manuell auf dem Remote-Datenbankserver installieren (d. h. der Computer, auf dem SQL Server oder Oracle installiert ist). Befinden sich die CA MDB und der Primärserver auf dem selben Computer, müssen Sie die CA MDB nicht manuell installieren. CA SDM installiert die CA MDB automatisch während der CA SDM-Installation.

Hinweis: Wenn Sie die Management-Datenbank auf dem Primärserver installieren möchten, *müssen* Sie die CA MDB-Installation auf dem Remote-Computer starten und ausführen, der den Datenbankserver hostet.

Weitere Informationen:

[Planen der CA MDB-Installation](#) (siehe Seite 99)

[Installieren unter SQL Server \(Windows\)](#) (siehe Seite 158)

[Installieren auf Oracle \(Windows\)](#) (siehe Seite 160)

[Installieren in der Oracle-Umgebung \(Linux/UNIX\)](#) (siehe Seite 163)

MDB-Installationen

Für MDB-Installationen gelten die folgenden Anforderungen:

- Wenn Sie eine MDB-Installation ausführen, um die SQL-Datenbank auf einem anderen Server zu installieren, müssen der SQL Native Client, der Client und die Verwaltungs-Tools auf dem CA CMDB-Client installiert werden.
- Für jede Oracle-Datenbankeinrichtung muss auch die Oracle Client-Software installiert werden. Sie können Oracle-Client-Software von der Oracle-Website herunterladen.

Suchen nach Informationen zur Produktintegration und Kompatibilität

Nutzen Sie die Informationen des Online-Supports von CA, um sich ein Bild von der CA MDB-Kompatibilität mit CA SDM und anderen Produkten zu machen.

- *"CA Service Accounting and CA Service Catalog Integration Guide" (CA Service Accounting- und CA Service Catalog-Integrationshandbuch)* - Beschreibt CA MDB-Versionen und wie Sie entscheiden können, ob ein CA MDB-Kompatibilitätspatch installiert werden muss, um andere Produkte mit CA MDB zu integrieren.
- *"CA Management Database Mixed Version Installation" (CA-Management-Datenbank - Installation von Mischversionen)* - Beschreibt-CA MDB-Kompatibilität.

So finden Sie Integrationen zur Integration mit CA MDB

1. Öffnen Sie einen Browser, und gehen Sie zu <http://support.ca.com>.
Der CA Support Online-Seite wird angezeigt.
2. Melden Sie sich bei CA Support Online an.
3. Klicken Sie im linken Fenster auf die Verknüpfung "Documentation" (Dokumentation).
Die Dokumentationsseite wird angezeigt.

4. Wählen Sie "CA Service Catalog, r12", und "Englisch (US)" aus den Dropdown-Listen aus. Klicken Sie auf "Starten".

Die CA Service Catalog-Dokumentationsliste wird angezeigt.

5. Klicken Sie auf die PDF-Verknüpfung für das Integrationshandbuch J02775-1E.

Das "CA Service Accounting and CA Service Catalog Integration Guide" wird angezeigt.

6. Klicken Sie auf das Lesezeichen "Enabling Integration with CA Products that Use an Earlier Version of the MDB" (Ermöglichen der Integration mit CA-Produkten, die eine frühere Version der MDB verwenden).

Sie können die Informationen zur Unterstützung der Integration von Produkten mit CA MDB verwenden.

So finden Sie Kompatibilitätsinformationen

1. Öffnen Sie einen Browser, und gehen Sie zu <http://support.ca.com>.

Der CA Support Online-Seite wird angezeigt.

2. Melden Sie sich bei CA Support Online an.

3. Klicken Sie im Fenster "Support" auf "Knowledge Base Search" (Knowledge Base-Suche).

Die Seite "Knowledge Base Search" wird angezeigt.

4. Geben Sie im Suchfeld "**MDB104 Compatibility**" ein. Klicken Sie auf "Suche".

Knowledge-Base-Suchergebnisse werden angezeigt.

5. Klicken Sie auf den Link "CA Management Database Mixed Version Installation" (CA-Management-Datenbank - Installation von Mischversionen).

Das Dokument "CA Management Database Mixed Version Installation" wird angezeigt.

Installieren unter SQL Server (Windows)

Wenn Sie die Konfiguration für erweiterte Verfügbarkeit verwenden und die CA MDB, die Sie verwenden, auf einem anderen Computer installiert ist als der CA SDM-Server, dann müssen Sie die CA MDB auf dem Remote-Datenbankserver installieren (der Computer, auf dem SQL Server installiert ist).

Gehen Sie wie folgt vor:

1. Legen Sie den Installationsdatenträger in Ihr Laufwerk ein.

Wichtig! Wenn Ihr Computer nicht über ein geeignetes Laufwerk für den Installationsdatenträger verfügt, kopieren Sie die Inhalte des Datenträgers auf den Computer, auf dem Sie CA SDM installieren wollen. Starten Sie die Installation dann erneut. Für eine Remote-Installation über das Netzwerk können Sie ein Laufwerk oder einen Ordner auf dem Netzwerk freigeben und dann eine Verbindung über das Netzwerk herstellen, um die Installation zu starten.

2. Wählen Sie die gewünschte Sprache aus der Liste aus, und klicken Sie auf "Sprache auswählen".

Das Installationsmenü wird angezeigt.

Hinweis: Wenn das Installationsmenü nicht automatisch angezeigt wird, starten Sie die Installation durch einen Doppelklick auf die Datei "setup.exe", die sich im Stammverzeichnis des Installationsdatenträgers befindet.

3. Klicken Sie die Registerkarte "Produktinstallationen".
4. Klicken Sie auf CA MDB.
5. Befolgen Sie für die Installation die Anweisungen auf dem Bildschirm.
6. Wenn Sie dazu aufgefordert werden, wählen Sie SQL Server als Datenbanktyp aus und geben die entsprechenden Informationen für SQL Server ein.

Hinweis: Informationen zu den erforderlichen Eingaben zu SQL Server finden Sie in der *Online-Hilfe zur Serverkonfiguration*.

7. Folgen Sie den Anweisungen auf dem Bildschirm, um die CA MDB-Installation abzuschließen.

Die CA MDB ist nun in der SQL Server-Umgebung installiert.

Weitere Informationen:

[Das Installationsprotokoll](#) (siehe Seite 242)

Installieren auf Oracle (Windows)

Wenn Sie die Konfiguration für erweiterte Verfügbarkeit verwenden und die CA MDB, die Sie verwenden, auf einem anderen Computer installiert ist als der CA SDM-Server, dann müssen Sie die CA MDB auf dem Remote-Datenbankserver installieren (der Computer, auf dem SQL Server installiert ist).

Gehen Sie wie folgt vor:

1. Legen Sie den Installationsdatenträger in Ihr Laufwerk ein.

Wichtig! Wenn Ihr Computer nicht über ein geeignetes Laufwerk für den Installationsdatenträger verfügt, kopieren Sie die Inhalte des Datenträgers auf den Computer, auf dem Sie CA SDM installieren wollen. Starten Sie die Installation dann erneut. Für eine Remote-Installation über das Netzwerk können Sie ein Laufwerk oder einen Ordner auf dem Netzwerk freigeben und dann eine Verbindung über das Netzwerk herstellen, um die Installation zu starten.

Das Installationsmenü wird angezeigt.

Hinweis: Wenn das Installationsmenü nicht automatisch angezeigt wird, starten Sie die Installation durch einen Doppelklick auf die Datei "setup.exe", die sich im Stammverzeichnis des Installationsdatenträgers befindet.

2. Klicken Sie auf die Registerkarte "Produktinstallationen".
3. Klicken Sie auf CA MDB.
4. Befolgen Sie für die Installation die Anweisungen auf dem Bildschirm.
5. Wenn Sie dazu aufgefordert werden, wählen Sie Oracle als Datenbanktyp aus und geben die entsprechenden Informationen für Oracle ein.

Hinweis: Informationen zu den erforderlichen Eingaben für Oracle finden Sie in der *Online-Hilfe zur Serverkonfiguration*.

6. Geben Sie die Informationen für die Konfiguration der Oracle-Datenbank ein bzw. wählen Sie die Informationen aus.

CA SDM erfordert einen Netzdienstnamen, der die Oracle-Datenbank angibt, auf der sich die MDB befindet. CA SDM erfordert außerdem eine System-ID (SID) für die Datenbank. Diese Namen können unterschiedlich sein, obwohl sie dieselbe MDB-Datenbank angeben. Es sind zwei Namenwerte erforderlich, da CA SDM sowohl mit der Oracle-Client-Technologie als auch der JDBC-Technologie auf die Datenbank zugreift.

Hinweis: Informationen zu Dienstnamen und SIDs finden Sie in der Oracle-Dokumentation.

Standarddaten laden

Gibt an, ob die standardmäßigen CA SDM-Daten in die Oracle-Datenbank geladen werden sollen.

Wenn dieses Kontrollkästchen aktiviert ist, lädt das System die CA SDM-Standardssystemdaten in die Oracle-Datenbank. Wenn Sie Systemstandardwerte geändert haben, ersetzt diese Option die Werte. Aktivieren Sie dieses Kontrollkästchen für Erstinstallationen. Diese Option ersetzt existierende Daten, wenn es sich nicht um eine Erstinstallation handelt. Wenn dieses Kontrollkästchen nicht aktiviert ist, werden keine Standarddaten geladen.

Remote-Datenbank

Gibt an, dass eine Oracle-Datenbank auf einem anderen Server als dem CA SDM-Primärserver installiert ist. Installieren Sie die CA MDB manuell auf dem Remote-Datenbankserver (also auf dem Computer, auf dem Oracle installiert ist), bevor Sie die Installation von CA SDM ausführen.

Wenn es sich um einen lokalen Oracle-Server handelt (nicht ausgewählt), dann erstellt CA SDM die MDB, falls nicht bereits erstellt.

Tablespaces erstellen

Gibt an, ob Tablespaces für die MDB-Datenbank erstellt werden müssen oder bereits vorhandene Tablespaces verwendet werden können.

- Deaktivieren Sie dieses Kontrollkästchen, wenn Sie Tablespaces bereits manuell erstellt haben. Geben Sie die Namen der existierenden Tablespaces an. Das Feld für den Pfad zum Tablespace wird im Produkt gesperrt und die Felder "Name des Daten-Tablespace" und "Name des Index-Tablespace" werden aktiviert.
- Aktivieren Sie dieses Kontrollkästchen, um Tablespaces mit den Standardnamen MDB_DATA und MDB_INDEX zu erstellen. Geben Sie einen Tablespace-Pfad an. Die Tablespace-Namensfelder "Daten" und "Index" sind deaktiviert.

Hinweis: Wenn Sie den Automated Storage Manager (ASM) von Oracle verwenden, dann erstellen Sie manuell einen Oracle-Tablespace, bevor Sie die Installation von CA SDM ausführen. Wenn Oracle installiert und für ASM konfiguriert wird, können Sie keinen Oracle-Tablespace während der MDB-Installation erstellen. ASM verwendet virtuelle Speicherung, während Sie ein physisches Verzeichnis benötigen. Daher können Sie mit dieser Konfiguration keinen Tablespace erstellen.

Netzdienstname

Identifiziert den Netzdienstnamen der Oracle-Datenbank, in der sich die MDB befindet. Wenn es sich um eine Remotedatenbank handelt, wird hier der Netzdienstname verwendet, der im Oracle-Client auf dem lokalen Computer definiert ist. Der Grund dafür ist, dass CA SDM über eine lokale Installation des Oracle-Clients auf die Datenbank zugreift, wobei möglicherweise ein Netzdienstname angegeben wird, der sich vom Dienstnamen auf dem Oracle-Server unterscheidet.

mdbadmin-Anwenderkennwort

Gibt das mdbadmin-Anwenderkennwort an. Geben Sie das bestehende Kennwort ein, oder geben Sie ein neues Kennwort ein, wenn CA SDM den Anwender erstellt.

DBA-Anwendername

Der Name eines Oracle-Anwenders mit DBA-Zugang (normalerweise SYS). Dieses Feld wird nur verwendet, wenn der Oracle-Server auf dem lokalen Computer ausgeführt wird.

DBA-Kennwort

Gibt das Kennwort für den DBA-Anwender an. Dieses Feld wird nur verwendet, wenn der Oracle-Server auf dem lokalen Computer ausgeführt wird.

Name des Daten-Tablespace

Erstellt den Datentablespace Namen, der angegeben wird, wenn das Kontrollkästchen "Tablespaces erstellen" aktiviert ist. Dieses Feld wird nur verwendet, wenn der Oracle-Server auf dem lokalen Computer ausgeführt wird.

Name des Index-Tablespace

Erstellt den Namen des Index-Tablespace, der angegeben wird, wenn das Kontrollkästchen "Tablespaces erstellen" aktiviert ist. Dieses Feld wird nur verwendet, wenn der Oracle-Server auf dem lokalen Computer ausgeführt wird.

Pfad zum Tablespace

Gibt den Verzeichnispfad zum physischen Tablespace-Speicherort an, der erstellt wird, wenn der zuvor erwähnte Tablespace noch nicht vorhanden ist. Dieses Feld wird nur verwendet, wenn der Oracle-Server auf dem lokalen Computer ausgeführt wird.

Oracle-Home-Pfad

Gibt den Verzeichnispfad zum Oracle-Stammverzeichnis an.

JDBC-Konnektivität

Gibt an, ob JDBC-Konnektivität verwendet wird. Mehrere CA SDM-Komponenten greifen mit Hilfe der JDBC-Technologie auf den Datenbankserver zu und erfordern spezifische Informationen über den Oracle-Server.

Identifizieren Sie den Datenbank-Hostnamen, SID, und den Empfangsport, die Sie zuvor konfiguriert haben.

Die CA MDB ist nun in der Oracle-Umgebung installiert.

Weitere Informationen:

[Das Installationsprotokoll](#) (siehe Seite 242)

Installieren in der Oracle-Umgebung (Linux/UNIX)

Wenn Sie die Konfiguration für erweiterte Verfügbarkeit verwenden und die CA MDB, die Sie verwenden, auf einem anderen Computer installiert ist als der CA SDM-Server, dann müssen Sie die CA MDB auf dem Remote-Datenbankserver installieren (der Computer, auf dem SQL Server installiert ist).

Hinweis: Vergewissern Sie sich, dass Ihre Oracle-Umgebung korrekt eingerichtet und zugänglich ist.

Gehen Sie wie folgt vor:

1. Legen Sie den Installationsdatenträger in das Laufwerk ein.

Wichtig! Wenn Ihr Computer nicht über ein geeignetes Laufwerk für den Installationsdatenträger verfügt, kopieren Sie die Inhalte des Datenträgers auf den Computer, auf dem Sie CA SDM installieren wollen. Starten Sie die Installation dann erneut. Für eine Remote-Installation über das Netzwerk können Sie ein Laufwerk oder einen Ordner auf dem Netzwerk freigeben und dann eine Verbindung über das Netzwerk herstellen, um die Installation zu starten.

2. Navigieren Sie zum Stammverzeichnis des Installationsdatenträgers, und starten Sie den Installationsvorgang mit folgendem Befehl:

```
sh ./setup.sh
```

3. Wählen Sie die gewünschte Sprache aus der Liste aus, und klicken Sie auf "Sprache auswählen".

Das Installationsmenü wird angezeigt.

4. Klicken auf Sie die Registerkarte "Produktinstallationen".
5. Klicken Sie auf CA MDB.
6. Befolgen Sie für die Installation die Anweisungen auf dem Bildschirm.

7. Wenn Sie dazu aufgefordert werden, wählen Sie Oracle als Datenbanktyp aus und geben die entsprechenden Informationen für Oracle ein.

Hinweis: Informationen zu den erforderlichen Eingaben für Oracle finden Sie in der *Online-Hilfe zur Serverkonfiguration*.

8. Folgen Sie den Anweisungen auf dem Bildschirm, um die CA MDB-Installation abzuschließen.

Die CA MDB ist nun in der Oracle-Umgebung installiert.

Weitere Informationen:

[Das Installationsprotokoll](#) (siehe Seite 242)

Installieren einer Remote-MDB unter HP-UX

Sie können eine Remote-MDB unter HP-UX installieren.

Gehen Sie wie folgt vor:

1. Laden Sie das CA MDB-Installationsprogramm für HP-UX vom CA Support-Portal herunter oder wenden Sie sich an den technischen Support von CA.
2. Entpacken Sie den Datenträger in einen Speicherort Ihrer Wahl.
3. Überprüfen Sie, ob der CA MDB-Ordner über volle Berechtigungen für alle Anwender verfügt.

Zum Beispiel "chmod -R 777 mdb".

4. Navigieren Sie zum Oracle-Ordner, und führen Sie folgenden Befehl aus:

```
./setupmdb.sh -DBVENDOR=oracle -DBHOST=<DBHOST_NAME> -DBNAME=<ORACLE_SID>  
-DBUSER=<DB_User_SYS_name> -DBPASSWORD=<DB_User_SYS_password>  
-MDB_ADMIN_PSWD=<MDB_ADMIN_PASSWORD>  
-ORA_TBLSPACE_PATH=<Oracle_Table_Space_path> -MANIFEST=Service_Desk  
-WORKSPACE=Service_Desk -JRE_DIR=<JRE_PATH> -MDB_COMMON_DIR=<mdb_Common_DIR>
```

5. Zum Beispiel führen Sie folgenden Befehl aus:

```
./setupmdb.sh -DBVENDOR=oracle -DBHOST=hostname -DBNAME=mdb -DBUSER=SYS  
-DBPASSWORD=mdbpassword -MDB_ADMIN_PSWD=mdbpassword  
-ORA_TBLSPACE_PATH=/sdhome/oracle/oracle/product/10.2.0/db_1/oradata/mdb  
-MANIFEST=Service_Desk -WORKSPACE=Service_Desk  
-JRE_DIR=/sdhome/opt/Sharedcomponents/JRE/1.6.0_00  
-MDB_COMMON_DIR=/sdhome/opt/Sharedcomponents/Mdb
```

Die CA MDB-Installation wird abgeschlossen, und eine Meldung wird angezeigt, die auf eine erfolgreiche Installation hinweist.

So installieren Sie CA SDM

Hinweis: Bevor Sie diese Komponente installieren, stellen Sie sicher, dass Sie die [CA SDM-Installation planen](#) (siehe Seite 102). Bei Installationen unter Linux und UNIX werden einige Popup-Meldungen nicht deutlich angezeigt, falls die Farbeigenschaften Weiß auf Weiß eingestellt sind.

Wenn Sie CA SDM auf einem Server starten und installieren, werden folgende Dateien, Komponenten und Funktionen für das Produkt installiert:

- Serverfunktionen, die auf Ihrer Konfiguration des Produkts nach der Installation basieren.
- Die SQL Server- oder Oracle-Schnittstelle
- Die ODBC-Schnittstelle

Wichtig! Die Installation der ODBC-Schnittstelle dient nur dem Zugriff auf den ODBC-Treiber für die Berichterstellung durch Business Objects in CA SDM mit CA Business Intelligence. Die Verwendung des ODBC-Treibers durch andere Anwendungen wird nicht direkt unterstützt, ist nicht zertifiziert, nicht durch eine Garantie von CA Technologies abgedeckt und erfolgt auf eigenes Risiko.

- Die Web-Schnittstelle
- CA CMDB

Wichtig! Wenn Sie von einer CA CMDB-Standalone-Version nach CA SDM migrieren, erscheint während der Konfiguration ein Kontrollkästchen mit der Option "Nur CMDB konfigurieren". Wenn Sie das Kontrollkästchen "Nur CMDB konfigurieren" deaktivieren und Sie auf "Weiter" klicken, können Sie CA CMDB nicht noch einmal konfigurieren. Auch wenn Sie auf "Zurück" klicken, ist das Kontrollkästchen "Nur CMDB konfigurieren" nicht mehr verfügbar. Eine Meldung im Konfigurationsdialog warnt Sie davor. Wenn Sie die Konfiguration vor der Fertigstellung abbrechen und sie dann wiederholen, ist das Kontrollkästchen "Nur CMDB konfigurieren" verfügbar.

Über das Kontrollkästchen "Nur CMDB konfigurieren" steuern Sie den Wert der CA SDM-Umgebungsvariable NX_CMDB. Die Umgebungsvariable kontrolliert, ob die Support-Automatisierung-Funktion konfiguriert wird. Wenn das Kontrollkästchen deaktiviert ist, kann Support-Automatisierung konfiguriert werden, andernfalls ist eine Konfiguration nicht möglich. Die Umgebungsvariable wirkt sich auf das Verhalten einiger Webformulare aus.

- Visualizer
- Support-Automatisierung

Die Option *supportautomation_url* installieren Sie nach der Support-Automatisierung-Konfiguration während der CA SDM-Konfiguration. Weitere Informationen hierzu finden Sie in der *Online-Hilfe*.

Wichtig! Wenn Sie CA SDM deinstallieren, wird CA Workflow auch deinstalliert.

Weitere Informationen:

[Planen der CA SDM-Installation](#) (siehe Seite 102)

[Installieren unter SQL Server \(Windows\)](#) (siehe Seite 166)

[Installieren auf Oracle \(Windows\)](#) (siehe Seite 168)

[Installieren in der Oracle-Umgebung \(Linux/UNIX\)](#) (siehe Seite 173)

Variablen der Oracle-Umgebung

Legen Sie die Oracle-Umgebungsvariablen folgendermaßen fest, bevor Sie CA SDM installieren oder migrieren:

- Überprüfen Sie, ob die Umgebungsvariable "ORACLE_HOME" korrekt festgelegt ist.
Wichtig! Sie müssen die Variable "TWO_TASK" exportieren, wenn die Oracle-32-Bit-Client-Variablen in eine Nicht-Windows-Umgebung exportiert werden.
- Schließen Sie die 32-Bit Oracle-Bibliotheken (normalerweise "\$ORACLE_HOME/lib32" für 64-Bit-Oracle) in der Bibliothekspfadvariablen "LD_LIBRARY_PATH" ("LIBPATH" unter AIX) ein.

Installieren unter SQL Server (Windows)

Wenn Sie CA SDM auf einem Server starten und installieren, werden folgende Komponenten und Funktionen installiert:

- Serverfunktionen, die auf Ihrer Konfiguration des Produkts nach der Installation basieren.
- Die SQL Server-Schnittstelle
- Die Web-Schnittstelle
- Die ODBC-Schnittstelle

Wichtig! Die Installation der ODBC-Schnittstelle dient nur dem Zugriff auf den ODBC-Treiber für die Berichterstellung durch Business Objects in CA SDM mit CA Business Intelligence. Die Verwendung des ODBC-Treibers durch andere Anwendungen wird nicht direkt unterstützt, ist nicht zertifiziert, nicht durch eine Garantie von CA Technologies abgedeckt und erfolgt auf eigenes Risiko.

Gehen Sie wie folgt vor:

1. Legen Sie den Installationsdatenträger in Ihr Laufwerk ein.

Wichtig! Wenn Ihr Computer nicht über ein geeignetes Laufwerk für den Installationsdatenträger verfügt, kopieren Sie die Inhalte des Datenträgers auf den Computer, auf dem Sie CA SDM installieren wollen. Starten Sie die Installation dann erneut. Für eine Remote-Installation über das Netzwerk können Sie ein Laufwerk oder einen Ordner auf dem Netzwerk freigeben und dann eine Verbindung über das Netzwerk herstellen, um die Installation zu starten.

2. Wählen Sie die gewünschte Sprache aus der Liste aus, und klicken Sie auf "Sprache auswählen".

Das Installationsmenü wird angezeigt.

Hinweis: Wenn das Installationsmenü nicht automatisch angezeigt wird, starten Sie die Installation durch einen Doppelklick auf die Datei "setup.exe", die sich im Stammverzeichnis des Installationsdatenträgers befindet.

3. Klicken Sie die Registerkarte "Produktinstallationen".
4. Klicken Sie auf CA SDM.
5. Um die Installation fortzusetzen, folgen Sie den Anweisungen auf dem Bildschirm.

Der Konfigurationsassistent wird angezeigt.

Hinweis: Wenn Hosts mit Internet Protocol Version 4 (IPv4) und Internet Protocol Version 6 (IPv6) gleichzeitig im Netzwerk vorhanden sind, sollten Sie sicherstellen, dass die entsprechenden Übergangsstrategien, Tools und Mechanismen zur Unterstützung beider Technologien eingerichtet sind, bevor Sie mit der Konfiguration beginnen. Informationen zur Konfiguration von Servern finden Sie im *Administrationshandbuch*.

6. Geben Sie die entsprechenden Informationen ein, und wählen Sie die gewünschten Optionen, um das Produkt zu konfigurieren.

Hinweis: Weitere Informationen über die im Assistenten angezeigten Felder finden Sie in der *Online-Hilfe*.

7. Folgen Sie den Anweisungen auf dem Bildschirm, um die Installation fertig zu stellen.

CA SDM ist nun in der SQL Server-Umgebung installiert.

8. Nachdem Sie die Installation konfiguriert haben, gibt der Assistent Anweisungen an, wie "pslist.exe" heruntergeladen und ausgeführt wird. Führen Sie diese Schritte aus, und klicken Sie auf "Weiter".
9. Nachdem Sie CA SDM installiert (oder von einem CA CMDB Standalone-System nach CA SDM migriert) haben, führen Sie das Dienstprogramm *cmdb_update_ambiguity* aus. Mit dem Befehl -h können Sie die obligatorischen Optionen anzeigen. Weitere Informationen zum Berechnen des Mehrdeutigkeitsindex finden Sie im *Administrationshandbuch*.

Hinweis: Wenn die Konfiguration während der Validierung der Erweiterungstabellen fehlschlägt, können Probleme bei der Datenbankverbindung auftreten. Führen Sie die Konfiguration erneut aus, und überprüfen Sie, ob Sie die richtigen Datenbankkonnektivitätsdaten eingegeben haben.

Weitere Informationen:

[Das Installationsprotokoll](#) (siehe Seite 242)

[Überprüfen der Installation](#) (siehe Seite 241)

[Starten der Web-Schnittstelle](#) (siehe Seite 252)

Installieren auf Oracle (Windows)

Wenn Sie CA SDM auf einem Server starten und installieren, werden folgende Komponenten und Funktionen installiert:

- Serverfunktionen, die auf Ihrer Konfiguration des Produkts nach der Installation basieren.
- Die Oracle-Schnittstelle
- Die Web-Schnittstelle
- Die ODBC-Schnittstelle

Sie können CA MDB oder CA SDM nur als Administrator installieren.

Wichtig! Die Installation der ODBC-Schnittstelle dient nur dem Zugriff auf den ODBC-Treiber für die Berichterstellung durch Business Objects in CA SDM mit CA Business Intelligence. Die Verwendung des ODBC-Treibers durch andere Anwendungen wird nicht direkt unterstützt, ist nicht zertifiziert, nicht durch eine Garantie von CA Technologies abgedeckt und erfolgt auf eigenes Risiko.

Gehen Sie wie folgt vor:

1. Legen Sie den Installationsdatenträger in Ihr Laufwerk ein.

Wichtig! Wenn Ihr Computer nicht über ein geeignetes Laufwerk für den Installationsdatenträger verfügt, kopieren Sie die Inhalte des Datenträgers auf den Computer, auf dem Sie CA SDM installieren wollen. Starten Sie die Installation dann erneut. Für eine Remote-Installation über das Netzwerk können Sie ein Laufwerk oder einen Ordner auf dem Netzwerk freigeben und dann eine Verbindung über das Netzwerk herstellen, um die Installation zu starten.

2. Wählen Sie die gewünschte Sprache aus der Liste aus, und klicken Sie auf "Sprache auswählen".

Das Installationsmenü wird angezeigt.

Hinweis: Wenn das Installationsmenü nicht automatisch angezeigt wird, starten Sie die Installation durch einen Doppelklick auf die Datei "setup.exe", die sich im Stammverzeichnis des Installationsdatenträgers befindet.

3. Klicken Sie auf die Registerkarte "Produktinstallationen".
4. Klicken Sie auf CA SDM.
5. Um die Installation fortzusetzen, folgen Sie den Anweisungen auf dem Bildschirm.

Der Konfigurationsassistent wird angezeigt.

Hinweis: Wenn Hosts mit Internet Protocol Version 4 (IPv4) und Internet Protocol Version 6 (IPv6) gleichzeitig im Netzwerk vorhanden sind, sollten Sie sicherstellen, dass die entsprechenden Übergangsstrategien, Tools und Mechanismen zur Unterstützung beider Technologien eingerichtet sind, bevor Sie mit der Konfiguration beginnen. Informationen zur Konfiguration von Servern finden Sie im *Administrationshandbuch*.

6. Geben Sie die Informationen für die Konfiguration der Oracle-Datenbank ein bzw. wählen Sie die Informationen aus.

CA SDM erfordert einen Netzdienstnamen, der die Oracle-Datenbank angibt, auf der sich die MDB befindet. CA SDM erfordert außerdem eine System-ID (SID) für die Datenbank. Diese Namen können unterschiedlich sein, obwohl sie dieselbe MDB-Datenbank angeben. Es sind zwei Namenwerte erforderlich, da CA SDM sowohl mit der Oracle-Client-Technologie als auch der JDBC-Technologie auf die Datenbank zugreift.

Hinweis: Informationen zu Dienstnamen und SIDs finden Sie in der Oracle-Dokumentation.

Standarddaten laden

Gibt an, ob die standardmäßigen CA SDM-Daten in die Oracle-Datenbank geladen werden sollen.

Wenn dieses Kontrollkästchen aktiviert ist, lädt das System die CA SDM-Standardssystemdaten in die Oracle-Datenbank. Wenn Sie Systemstandardwerte geändert haben, ersetzt diese Option die Werte. Aktivieren Sie dieses Kontrollkästchen für Erstinstallationen. Diese Option ersetzt existierende Daten, wenn es sich nicht um eine Erstinstallation handelt. Wenn dieses Kontrollkästchen nicht aktiviert ist, werden keine Standarddaten geladen.

Remote-Datenbank

Zeigt an, dass eine Oracle-Datenbank auf einem Remote-Server installiert ist. Installieren Sie die CA MDB manuell auf dem Remote-Datenbankserver (also auf dem Computer, auf dem Oracle installiert ist), bevor Sie die Installation von CA SDM ausführen.

Wenn es sich um einen lokalen Oracle-Server handelt (nicht ausgewählt), dann erstellt CA SDM die MDB, falls nicht bereits erstellt.

Tablespaces erstellen

Gibt an, ob Tablespaces für die MDB-Datenbank erstellt werden müssen oder bereits vorhandene Tablespaces verwendet werden können.

- Deaktivieren Sie dieses Kontrollkästchen, wenn Sie Tablespaces bereits manuell erstellt haben. Geben Sie die Namen der existierenden Tablespaces an. Das Feld für den Pfad zum Tablespace wird im Produkt gesperrt und die Felder "Name des Daten-Tablespace" und "Name des Index-Tablespace" werden aktiviert.
- Aktivieren Sie dieses Kontrollkästchen, um Tablespaces mit den Standardnamen MDB_DATA und MDB_INDEX zu erstellen. Geben Sie einen Tablespace-Pfad an. Die Tablespace-Namensfelder "Daten" und "Index" sind deaktiviert.

Hinweis: Wenn Sie den Automated Storage Manager (ASM) von Oracle verwenden, dann erstellen Sie manuell einen Oracle-Tablespace, bevor Sie die Installation von CA SDM ausführen. Wenn Oracle installiert und für ASM konfiguriert wird, können Sie keinen Oracle-Tablespace während der MDB-Installation erstellen. ASM verwendet virtuelle Speicherung, während Sie ein physisches Verzeichnis benötigen. Daher können Sie mit dieser Konfiguration keinen Tablespace erstellen.

Netzdienstname

Identifiziert den Netzdienstnamen der Oracle-Datenbank, in der sich die MDB befindet. Wenn es sich um eine Remotedatenbank handelt, wird hier der Netzdienstname verwendet, der im Oracle-Client auf dem lokalen Computer definiert ist. Der Grund dafür ist, dass CA SDM über eine lokale Installation des Oracle-Clients auf die Datenbank zugreift, wobei möglicherweise ein Netzdienstname angegeben wird, der sich vom Dienstnamen auf dem Oracle-Server unterscheidet.

mdbadmin-Anwenderkennwort

Gibt das mdbadmin-Anwenderkennwort an. Geben Sie das bestehende Kennwort ein, oder geben Sie ein neues Kennwort ein, wenn CA SDM den Anwender erstellt.

DBA-Anwendername

Der Name eines Oracle-Anwenders mit DBA-Zugang (normalerweise SYS). Dieses Feld wird nur verwendet, wenn der Oracle-Server auf dem lokalen Computer ausgeführt wird.

DBA-Kennwort

Gibt das Kennwort für den DBA-Anwender an. Dieses Feld wird nur verwendet, wenn der Oracle-Server auf dem lokalen Computer ausgeführt wird.

Name des Daten-Tablespace

Erstellt den Datentablespace Namen, der angegeben wird, wenn das Kontrollkästchen "Tablespaces erstellen" aktiviert ist. Dieses Feld wird nur verwendet, wenn der Oracle-Server auf dem lokalen Computer ausgeführt wird.

Name des Index-Tablespace

Erstellt den Namen des Index-Tablespace, der angegeben wird, wenn das Kontrollkästchen "Tablespaces erstellen" aktiviert ist. Dieses Feld wird nur verwendet, wenn der Oracle-Server auf dem lokalen Computer ausgeführt wird.

Pfad zum Tablespace

Gibt den Verzeichnispfad zum physischen Tablespace-Speicherort an, der erstellt wird, wenn der zuvor erwähnte Tablespace noch nicht vorhanden ist. Dieses Feld wird nur verwendet, wenn der Oracle-Server auf dem lokalen Computer ausgeführt wird.

Oracle-Home-Pfad

Gibt den Verzeichnispfad zum Oracle-Stammverzeichnis an.

JDBC-Konnektivität

Gibt an, ob JDBC-Konnektivität verwendet wird. Mehrere CA SDM-Komponenten greifen mit Hilfe der JDBC-Technologie auf den Datenbankserver zu und erfordern spezifische Informationen über den Oracle-Server.

Identifizieren Sie den Datenbank-Hostnamen, SID, und den Empfangsport, die Sie zuvor konfiguriert haben.

7. Folgen Sie den Anweisungen auf dem Bildschirm, um die Installation fertig zu stellen.

CA SDM ist auf Oracle installiert.
8. Nachdem Sie die Installation konfiguriert haben, gibt der Assistent Anweisungen an, wie "pslist.exe" heruntergeladen und ausgeführt wird. Führen Sie diese Schritte aus, und klicken Sie auf "Weiter".
9. Nachdem Sie CA SDM installiert (oder von einem CA CMDB Standalone-System nach CA SDM migriert) haben, führen Sie das Dienstprogramm *cmdb_update_ambiguity* aus. Mit dem Befehl -h können Sie die obligatorischen Optionen anzeigen. Weitere Informationen zum Berechnen des Mehrdeutigkeitsindex finden Sie im *Administrationshandbuch*.

Weitere Informationen:

[Das Installationsprotokoll](#) (siehe Seite 242)

[Überprüfen der Installation](#) (siehe Seite 241)

[Starten der Web-Schnittstelle](#) (siehe Seite 252)

Installieren in der Oracle-Umgebung (Linux/UNIX)

Wenn Sie CA SDM auf einem Server starten und installieren, werden folgende Komponenten und Funktionen installiert:

- Serverfunktionen, die auf Ihrer Konfiguration des Produkts nach der Installation basieren.
- Die Oracle-Schnittstelle
- Die Web-Schnittstelle
- Die ODBC-Schnittstelle

Wichtig! Die Installation der ODBC-Schnittstelle dient nur dem Zugriff auf den ODBC-Treiber für die Berichterstellung durch Business Objects in CA SDM mit CA Business Intelligence. Die Verwendung des ODBC-Treibers durch andere Anwendungen wird nicht direkt unterstützt, ist nicht zertifiziert, nicht durch eine Garantie von CA Technologies abgedeckt und erfolgt auf eigenes Risiko.

Hinweis: Vergewissern Sie sich, dass Ihre Oracle-Umgebung korrekt eingerichtet und zugänglich ist.

Gehen Sie wie folgt vor:

1. Legen Sie den Installationsdatenträger in das Laufwerk ein.

Wichtig! Wenn Ihr Computer nicht über ein geeignetes Laufwerk für den Installationsdatenträger verfügt, kopieren Sie die Inhalte des Datenträgers auf den Computer, auf dem Sie CA SDM installieren wollen. Starten Sie die Installation dann erneut. Für eine Remote-Installation über das Netzwerk können Sie ein Laufwerk oder einen Ordner auf dem Netzwerk freigeben und dann eine Verbindung über das Netzwerk herstellen, um die Installation zu starten.

2. Navigieren Sie zum Stammverzeichnis des Installationsdatenträgers, und starten Sie den Installationsvorgang mit folgendem Befehl:

```
sh ./setup.sh
```

3. Wählen Sie die gewünschte Sprache aus der Liste aus, und klicken Sie auf "Sprache auswählen".

Das Installationsmenü wird angezeigt.

Hinweis: Bei Installationen unter Linux und UNIX können Sie möglicherweise einige Popup-Meldungen nicht deutlich anzeigen, wenn die Farbeigenschaften Weiß auf Weiß sind.

4. Klicken Sie auf die Registerkarte "Produktinstallationen".

5. Klicken Sie auf CA SDM.
6. Um die Installation fortzusetzen, folgen Sie den Anweisungen auf dem Bildschirm.
Der Konfigurationsassistent wird angezeigt.

Hinweis: Wenn Hosts mit Internet Protocol Version 4 (IPv4) und Internet Protocol Version 6 (IPv6) gleichzeitig im Netzwerk vorhanden sind, sollten Sie sicherstellen, dass die entsprechenden Übergangsstrategien, Tools und Mechanismen zur Unterstützung beider Technologien eingerichtet sind, bevor Sie mit der Konfiguration beginnen. Informationen zur Konfiguration von Servern finden Sie im Administrationshandbuch.

7. Geben Sie die entsprechenden Informationen ein, und wählen Sie die gewünschten Optionen, um das Produkt zu konfigurieren.

Hinweis: Weitere Informationen über die im Assistenten angezeigten Felder finden Sie in der *Online-Hilfe*.

8. Folgen Sie den Anweisungen auf dem Bildschirm, um die Installation fertig zu stellen.

CA SDM ist auf Oracle installiert.

9. Nachdem Sie CA SDM installiert (oder von einem CA CMDB Standalone-System nach CA SDM migriert) haben, führen Sie das Dienstprogramm `cmdb_update_ambiguity` aus. Mit dem Befehl `-h` können Sie die obligatorischen Optionen anzeigen. Die Option `-d` ist in einer Linux/Unix-Umgebung nicht erforderlich, da standardmäßig Oracle eingestellt ist.

Hinweis: Weitere Informationen über die Berechnung des Mehrdeutigkeitsindex finden Sie im *Administrationshandbuch*.

Weitere Informationen:

[Das Installationsprotokoll](#) (siehe Seite 242)

[Überprüfen der Installation](#) (siehe Seite 241)

[Starten der Web-Schnittstelle](#) (siehe Seite 252)

Visualizer-Konfiguration

Sie können während der CA SDM-Installation Visualizer konfigurieren. Wenn Sie das Kontrollkästchen "Visualizer konfigurieren" aktivieren, werden die Bereiche für die Visualizer-Konfiguration angezeigt.

Klicken Sie im Assistenten auf die Schaltfläche "Weiter", um die Konfigurationsinformationen zu validieren. Nach einer erfolgreichen Validierung werden die validierten Visualizer-Konfigurationsinformationen von der Visualizer-Konfigurationsaufgabe verwendet.

Konfigurieren von Visualizer auf einem Sekundärserver

Sie können Visualizer auf einem CA SDM-Sekundärserver konfigurieren, um Webservices zu verwenden. Sie starten und konfigurieren Visualizer auf einem Sekundärserver während der CA SDM-Konfiguration. Dabei wird das Hilfsprogramm *"pdm_edit"* verwendet.

Hinweis: Wählen Sie bei der Konfiguration von sekundären Webservices auf einer Sekundärinstallation von CA CMDB Visualizer den Servernamen aus dem Dropdown-Menü aus. Die Standardauswahl ist der Primärserver.

Gehen Sie wie folgt vor:

1. Wählen Sie im Konfigurations-Assistenten für Visualizer die Option "Visualizer konfigurieren".
2. Wählen Sie den CA SDM-Sekundärserver als Webhost aus und geben Sie den Webhost-Port an.

Wenn die Konfiguration auf einem CA SDM-Sekundärserver ausgeführt wird, können Sie aus dem Dropdown-Menü für verfügbare Webservice-Hosts die Eigenschaftswerte *"general.primary_server_node"* und *"general.local_host"* auswählen.

3. Geben Sie die CA SDM-Port-Nummer für den Visualizer-Sekundärserver ein.
4. Folgen Sie den Anweisungen auf dem Bildschirm, um die Installation fertig zu stellen.

Visualizer wird installiert und auf einem CA SDM-Sekundärserver konfiguriert.

5. Öffnen Sie eine Eingabeaufforderung und navigieren Sie zum Ordner *"\$NX_ROOT\samples\pdmconf"*. Führen Sie folgenden Befehl aus:

```
pdm_perl pdm_edit.pl
```

Ein Kontextmenü wird angezeigt.

6. Wählen Sie "Z" aus, um die Visualizer-Tomcat-Server zu bearbeiten. Geben Sie "A" ein, um einen neuen Visualizer-Tomcat-Server hinzuzufügen.

Sie werden aufgefordert, einen Hostnamen einzugeben.

7. Geben Sie den sekundären Hostnamen ein.

Der Name des sekundären Hosts wird gespeichert und eine Liste mit Vorlagen angezeigt.

8. Befolgen Sie die Anweisungen im Hilfsprogramm *"pdm_edit.pl"*.

Die sekundäre Visualizer-Tomcat-Konfiguration ist abgeschlossen.

Konfiguration von Support-Automatisierung-Komponenten

CA SDM installiert und konfiguriert die folgenden-Support-Automatisierung-Komponenten:

- Endanwender-Client
- Analystenschnittstelle von Support-Automatisierung
- Server

Die folgenden Komponenten werden getrennt installiert und konfiguriert:

- Endanwender-Agent
- Editor für automatisierte Aufgaben - IDE

Wichtig! Zusätzlich zur Konfiguration von Support-Automatisierung während der CA SDM-Konfiguration *müssen* Sie die Option "*supportautomation_url*" nach der Installation von CA SDM installieren. Weitere Informationen zur Option "*supportautomation_url*" finden Sie in der *Online-Hilfe*.

Konfigurieren von Support-Automatisierung-Server-Modi

Während der Installation können Sie die folgenden-Support-Automatisierung-Servermodi konfigurieren:

- **Hauptserver-**Wenn Sie den Konfigurationstyp "Hauptserver" auswählen, wird als Hostnamen oder im IP-Feld standardmäßig der lokale Hostname angegeben. Alle Parameter müssen für den Hauptserver angegeben werden; Ausnahmen sind der Abschnitt zum internen Port und der Abschnitt zum Binden an die IP im Socket-Server; diese sind optional.

Hinweis: Konfigurieren Sie den Hauptserver auf dem folgenden CA SDM-Server gemäß dem CA SDM-Konfigurationstyp:

- Konventionell: Primärserver oder Sekundärserver.
- Erweiterte Verfügbarkeit: Hintergrundserver.

Wichtig! Wenn Sie die *Option* "*supportautomation_url*" festlegen, muss diese URL die URL des Hauptservers von Support-Automatisierung verwenden. Sie darf nicht auf den Proxy-Server oder den Lastausgleichsserver verweisen. Dies gilt nur für das konventionelle Modell. In der Konfiguration für erweiterte Verfügbarkeit kann die URL auf einen Lastenausgleich, Hauptserver oder Proxy-Server verweisen.

Hinweis: Wenn Sie die Option "Hauptserver" wählen und die Konfiguration von einem oder mehreren Socket-Proxy-Servern planen, *müssen* Sie den Hostnamen des Socket-Servers und den externen Port auf den Socket-Proxy-Host und den externen Port setzen. Bei mehreren Socket-Proxys setzen Sie den Socket-Server auf den Host und externen Port des Servers für den Lastausgleich.

- **Socket-Proxy-Server:** Sie können abhängig von der CA SDM-Konfiguration den Konfigurationstyp des Socket-Proxy-Servers auf folgenden Servern auswählen:

- Konventionell: Sekundärserver
- Erweiterte Verfügbarkeit: Anwendungsserver.

Die Standardwerte für Felder werden angezeigt. Für den Socket-Proxy-Server müssen alle Parameter außer dem optionalen Feld "An IP binden" im Abschnitt "Socket-Konfiguration" angegeben werden.

- **Nachrichtenroutingserver:** Sie können abhängig von der CA SDM-Konfiguration den Konfigurationstyp des Nachrichtenroutingservers auf folgenden Servern auswählen:

- Konventionell: Sekundärserver
- Erweiterte Verfügbarkeit: Anwendungsserver.

Die Standardwerte für Felder werden angezeigt. Für den Nachrichtenroutingserver müssen alle Parameter außer dem optionalen Feld "An IP binden" im Abschnitt "Socket-Konfiguration" angegeben werden.

Konfigurieren von Support-Automatisierung auf einem Sekundärserver

Sie können Support-Automatisierung auf einem CA SDM-Sekundärserver konfigurieren.

Gehen Sie wie folgt vor:

1. Wählen Sie Support-Automatisierung im Konfigurations-Assistenten aus.
2. Geben Sie die entsprechenden Informationen für Ihre Konfigurationstypen auf dem Sekundärserver ein, wie den Hostnamen und den Port auf einem Socket-Server.

Wichtig! Wenn ein Support-Automatisierung-Server definiert wurde, kann seine Rolle als Primär- oder Sekundärserver nicht mehr geändert werden.

3. Folgen Sie den Anweisungen auf dem Bildschirm, um die Installation fertig zu stellen.

Support-Automatisierung wird installiert und auf einem CA SDM-Sekundärserver konfiguriert.

4. Öffnen Sie auf dem Primärserver eine Eingabeaufforderung, und navigieren Sie zum Ordner "\$NX_ROOT\samples\pdmconf".

5. Führen Sie folgenden Befehl aus:

```
pdm_perl pdm_edit.pl
```

Ein Kontextmenü wird angezeigt.

6. Geben Sie "M" ein, um die Support-Automatisierung-Tomcat-Server zu bearbeiten. Geben Sie "A" ein, um einen neuen Support-Automatisierung-Tomcat-Server hinzuzufügen.

Sie werden aufgefordert, einen Hostnamen und Servertyp einzugeben.

7. Geben Sie den sekundären Hostnamen und Servertyp ein.

Der Name des sekundären Hosts wird gespeichert und eine Liste mit Vorlagen angezeigt.

8. Befolgen Sie die Anweisungen im Hilfsprogramm "pdm_edit.pl".

Die sekundäre Support-Automatisierung-Tomcat-Konfiguration ist abgeschlossen.

Konfigurieren von Support-Automatisierung auf dem Hintergrundserver

Sie können Support-Automatisierung auf dem Hintergrundserver konfigurieren, wenn Sie die Konfiguration für erweiterte Verfügbarkeit ausgewählt haben. Für die Konfiguration für erweiterte Verfügbarkeit konfigurieren Sie den Hauptserver auf dem Hintergrundserver.

Gehen Sie wie folgt vor:

1. Wählen Sie Support-Automatisierung im Konfigurations-Assistenten aus.
2. Wählen Sie auf der Seite "Konfig. auswählen" die Option "Erweiterte Verfügbarkeit" aus der Dropdown-Liste "Serverkonfiguration". Weitere Informationen finden Sie in der Online-Hilfe.
3. Wählen Sie auf der Seite "Allgemeine Einstellungen" die Option "Hintergrundserver" bzw. "Standby-Server" aus der Dropdown-Liste "Konfigurationstyp" aus.
4. Wählen Sie auf der Seite "Support-Automatisierung" die Option "Hauptserver" aus.
5. Geben Sie die Details der Socket-Konfiguration und Tomcat-Konfiguration ein.
6. Folgen Sie den Anweisungen, um den Assistenten abzuschließen.

Sie haben Support-Automatisierung auf dem Hintergrundserver konfiguriert.

Konfigurieren von Support-Automatisierung auf dem Anwendungsserver

Sie können Support-Automatisierung auf dem Anwendungsserver konfigurieren, wenn Sie die Konfiguration für erweiterte Verfügbarkeit ausgewählt haben. Der Socket-Proxy-Server oder der Nachrichtenroutingserver sind die gültigen Support-Automatisierung-Servermodi auf dem Anwendungsserver.

Gehen Sie wie folgt vor:

1. Wählen Sie Support-Automatisierung im Konfigurations-Assistenten aus.
2. Wählen Sie auf der Seite "Konfig. auswählen" die Option "Erweiterte Verfügbarkeit" aus der Dropdown-Liste "Serverkonfiguration". Weitere Informationen finden Sie in der Online-Hilfe.
3. Wählen Sie auf der Seite "Allgemeine Einstellungen" die Option "Anwendungsserver" aus der Dropdown-Liste "Konfigurationstyp" aus.
4. Wählen Sie auf der Seite "Support-Automatisierung" die Option "Nachrichtenroutingserver" oder "Socket-Proxy-Server" aus.
5. Geben Sie die Details der Socket-Konfiguration und Tomcat-Konfiguration ein.
6. Folgen Sie den Anweisungen, um den Assistenten abzuschließen.
Sie haben Support-Automatisierung auf dem Anwendungsserver konfiguriert.

Konfigurieren automatischer Aufgaben

Sie installieren und konfigurieren den automatischen Aufgaben-Editor, um automatische Aufgaben zu verwalten, mit deren Hilfe Support-Automatisierung-Analysten Endanwender unterstützen. Der Endanwender kann eine automatische Aufgabe in einem Knowledge-Dokument und der Self-Service-Schnittstelle öffnen, oder ein Analyst führt während einer Unterstützungssitzung eine automatische Aufgabe aus. Automatisierte Aufgaben bieten Analysten detaillierte Informationen über den Computer des Endanwenders. Sie erstellen automatische Self-Service-Aufgaben, die mit dem Endanwender interagieren und die Eingabe des Endanwenders bearbeiten. Diese Aufgaben können das Dateisystem und die Registrierung ändern, Installationssoftware herunterladen und so weiter. Sie konfigurieren automatische Aufgaben folgendermaßen:

1. Installieren Sie den automatischen Aufgaben-Editor.

Sie öffnen das Installationsprogramm vom folgenden Standort auf den Installationsdatenträgern:

`casd.nt\SAScriptWriter`

Hinweis: Sie können auch das Installationsprogramm kopieren und es den entsprechenden Anwendern in Ihrer Unterstützungsumgebung bereitstellen.

Der automatische Aufgaben-Editor wird installiert.

2. Öffnen Sie den automatischen Aufgaben-Editor.

Bei der Installation des automatischen Aufgaben-Editors wird eine Verknüpfung auf Ihrem Desktop erstellt.

3. Legen Sie die folgenden Verbindungsparameter fest:

- a. Klicken Sie auf Werkzeuge, Server.

Das Dialogfeld Serverkonfiguration wird angezeigt.

- b. Geben Sie Hostnamen und Port an.

Standard-Port: 8070

- c. Geben Sie den Användernamen und das Kennwort eines Anwenders mit Lese-/Schreibzugriff auf den automatischen Aufgaben-Editor an, z. B. die Anmeldedaten eines Support-Automatisierung-Analysten.

- d. Klicken Sie auf Test.

- e. Klicken Sie auf OK.

4. Erstellen Sie automatische Aufgaben, und laden Sie sie auf Ihren Server.

Sie können öffentliche Aufgaben exportieren oder sie bestimmten Mandanten und Untermantanten zuweisen.

Wichtig! Nur Rollen des 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.

So installieren Sie Web Screen Painter

Installieren Sie Web Screen Painter, um das Schema und die Web-Schnittstelle anzupassen.

Gehen Sie wie folgt vor:

1. Melden Sie sich abhängig von Ihrer CA SDM-Konfiguration bei folgendem Server an, auf dem Sie Web Screen Painter installieren möchten:

- Konventionell: Primärserver oder Sekundärserver oder ein beliebiger Remote-Computer
- Erweiterte Verfügbarkeit: Hintergrundserver

Wichtig! WSP kann nur auf dem Hintergrundserver ausgeführt werden. WSP kann über das Installationsprogramm auf anderen Servern installiert werden, jedoch kann WSP nicht auf eigenständigen Servern oder auf dem Standby-Server und Anwendungsserver ausgeführt werden. Zum Beispiel haben Sie WSP auf einem Server installiert, der nicht der Hintergrundserver ist. Die WSP-Verknüpfungen werden im Startmenü angezeigt. Wenn Sie auf die Verknüpfung klicken, wird eine Fehlermeldung angezeigt.

2. Legen Sie den Installationsdatenträger in Ihr Laufwerk ein.

Wichtig! Wenn Ihr Computer nicht über ein geeignetes Laufwerk für den Installationsdatenträger verfügt, kopieren Sie die Inhalte des Datenträgers auf den Computer, auf dem Sie CA SDM installieren wollen. Starten Sie die Installation dann erneut. Für eine Remote-Installation über das Netzwerk können Sie ein Laufwerk oder einen Ordner auf dem Netzwerk freigeben und dann eine Verbindung über das Netzwerk herstellen, um die Installation zu starten.

3. Wählen Sie die gewünschte Sprache aus der Liste aus, und klicken Sie auf "Sprache auswählen".

Das Installationsmenü wird angezeigt.

Hinweis: Wenn das Installationsmenü nicht automatisch angezeigt wird, starten Sie die Installation durch einen Doppelklick auf die Datei "setup.exe", die sich im Stammverzeichnis des Installationsdatenträgers befindet.

4. Klicken Sie auf die Registerkarte "Produktinstallationen".
5. Klicken Sie auf "Web Screen Painter".
6. Wählen Sie Ihre Sprache aus, und klicken Sie auf "OK".
7. Folgen Sie weiterhin den Anweisungen auf dem Bildschirm, um die Web Screen Painter-Installation fertig zu stellen.

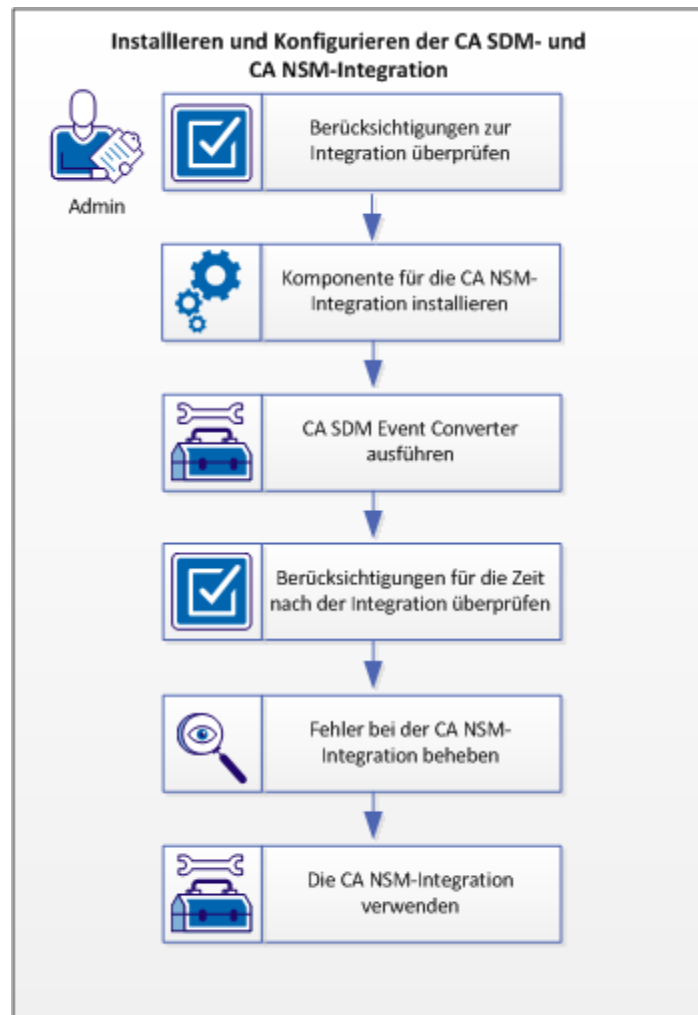
Web Screen Painter ist installiert.

So installieren und konfigurieren Sie die CA SDM- und CA NSM-Integration

Die CA NSM-Integration dient zum Durchführen folgender Aufgaben:

- Automatische Steuerung von Netzwerkverwaltungsproblemen, die von CA NSM Event and Alert Management erkannt werden
- Automatische Koordination kritischer Verwaltungsereignisse, die von CA NSM im Incident Management erkannt werden
- Bestimmen der Auswirkungen durch Ihren Netzwerkadministrator und Service Desk-Mitarbeiter
- Vermeiden starker Häufungen von Anfragen oder Incidents
- Automatisches Aktualisieren von Anfragen oder Incidents
- Implementieren von Geschäftsregeln als Best Practices für die Verwaltung von Netzwerk- und Service-Support
- Automatisches Senden von neuen Anfragen oder Incidents
- Automatisieren der Interaktion mit CA SDM, um manuelle Aufgaben für Kunden-Support-Mitarbeiter und somit auch deren Arbeitslast zu reduzieren
- Reduzieren der Anzahl Anfragen und Incidents, die von Anwendern erstellt werden müssen, da diese bei Auftreten eines Problems im Unternehmen automatisch erstellt werden.

Folgendes Diagramm zeigt, wie die CA SDM- und CA NSM-Integration installiert und konfiguriert wird:



Gehen Sie wie folgt vor:

1. [Überprüfen Sie die Hinweise zur Integration](#) (siehe Seite 184).
2. [Installieren der CA NSM-Integrationskomponente](#) (siehe Seite 185).
3. [Führen Sie den CA SDM-Event Converter aus](#) (siehe Seite 188).
4. [Überprüfen Sie die Hinweise zur Post-Integration](#) (siehe Seite 189).
5. [Beheben Sie die durch die CA NSM-Integration aufgetretenen Fehler](#) (siehe Seite 190), falls erforderlich.
6. [Verwenden Sie die CA NSM-Integration](#) (siehe Seite 222).

Weitere Informationen:

[Erstellen von Anlagen, die Eigentümern zugeordnet sind](#) (siehe Seite 190)

[Überwachen von Meldungen der Event-Konsole](#) (siehe Seite 192)

[Hinweise zu Filterregeln](#) (siehe Seite 193)

[Fehlerbehebung bei der CA NSM-Integration](#) (siehe Seite 216)

Überprüfen der Hinweise zur Integration

Überprüfen Sie folgende Hinweise, bevor Sie mit der Integration beginnen:

- Stellen Sie sicher, dass Sie CA SDM und CA NSM r11.2 SP2 cum1 mit dem WSDL-Fix installiert und konfiguriert haben.
- Wenn Sie bei der Integration von CA SDM mit CA NSM Änderungen an den Standardeinstellungen vornehmen, kann dies zu unerwarteten Ergebnissen führen. Um während der Integration eine sofortige Erstellung von Tausenden von CA SDM-Requests zu vermeiden, stellen Sie sicher, dass die folgenden Parameter in der Datei "NX.env", die sich in "\$NX_ROOT" (UNIX) oder im Installationsverzeichnis (Windows) befinden, auf NEIN festgelegt sind:

@NX_TNG_OBJECT_UPDATED_SUBSCRIBE=NO

@NX_TNG_OBJECT_ADDED_SUBSCRIBE=NO

@NX_TNG_OBJECT_DELETED_SUBSCRIBE=NO

@NX_TNG_OBJECT_STATUS_UPDATED_SUBSCRIBE=NO

- Sie können abhängig von Ihrer CA SDM-Konfiguration die CA NSM-Integration auf den folgenden Servern installieren:
 - Konventionell: Primärserver oder Sekundärserver oder ein anderer eigenständiger Server.
 - Erweiterte Verfügbarkeit: Ein beliebiger Anwendungsserver oder ein anderer eigenständiger Server.

Wichtig! Um die CA NSM-Integration auf einem eigenständigen Server zu installieren, [installieren Sie die CA NSM-Integrationskomponente](#) (siehe Seite 185) auf dem eigenständigen Server. Für die Konfiguration für erweiterte Verfügbarkeit verweisen Sie die Komponente auf einen Anwendungsserver.

- Wenn Sie planen, CA SDM und CA NSM auf dem gleichen Computer zu installieren, müssen Sie die CA NSM-Integration nicht installieren. Diese Integration ist automatisch aktiviert.
- (Windows) Wenn Sie planen, CA SDM und CA NSM auf verschiedenen Computern zu installieren, führen Sie abhängig von Ihrer CA SDM-Konfiguration eine der folgenden Aktionen durch:
 - Konventionell: Installieren und konfigurieren Sie den Sekundärserver auf dem CA NSM-Server, oder [installieren Sie die CA NSM-Integrationskomponente](#) (siehe Seite 185) auf dem CA NSM-Server.
 - Erweiterte Verfügbarkeit: Installieren und konfigurieren Sie einen der Anwendungsserver auf dem CA NSM-Server, oder [installieren Sie die CA NSM-Integrationskomponente](#) (siehe Seite 185) auf dem CA NSM-Server, und verweisen Sie auf einen der Anwendungsserver.
- (UNIX) Wenn Sie planen, CA SDM und CA NSM auf verschiedenen Computern zu installieren, führen Sie abhängig von Ihrer CA SDM-Konfiguration eine der folgenden Aktionen durch:
 - Konventionell: Installieren Sie den Sekundärserver auf dem CA NSM-Server.
 - Erweiterte Verfügbarkeit: Installieren Sie den Anwendungsserver auf dem CA NSM-Server.

Installieren der CA NSM-Integrationskomponente

Sie müssen die CA NSM-Integrationskomponente (oder Event Converter) installieren, wenn CA SDM und CA NSM nicht auf dem gleichen Computer installiert sind oder wenn Sie die CA NSM-Integration auf einem eigenständigen Server installieren möchten. Diese Komponente kann nur auf einem Windows-Computer ausgeführt werden.

Gehen Sie wie folgt vor:

1. Melden Sie sich beim CA NSM-Server oder beim eigenständigen Server an.
2. Legen Sie den Installationsdatenträger in Ihr Laufwerk ein.

Wichtig! Wenn Ihr Computer nicht über ein geeignetes Laufwerk für den Installationsdatenträger verfügt, kopieren Sie die Inhalte des Datenträgers auf den Computer, auf dem Sie CA SDM installieren wollen. Starten Sie die Installation dann erneut. Für eine Remote-Installation über das Netzwerk können Sie ein Laufwerk oder einen Ordner auf dem Netzwerk freigeben und dann eine Verbindung über das Netzwerk herstellen, um die Installation zu starten.

3. Wählen Sie die gewünschte Sprache aus der Liste aus, und klicken Sie auf "Sprache auswählen".

Das Installationsmenü wird geöffnet.

Hinweis: Wenn das Installationsmenü nicht automatisch angezeigt wird, starten Sie die Installation durch einen Doppelklick auf die Datei "setup.exe", die sich im Stammverzeichnis des Installationsdatenträgers befindet.

4. Klicken Sie die Registerkarte "Produktinstallationen".
5. Klicken Sie auf "CA NSM-Integration".
6. Folgen Sie den Anweisungen auf dem Bildschirm, und geben Sie die folgenden Informationen ein, wenn Sie dazu aufgefordert werden:

- Slump-Hostname
- Slump-Host-IP-Adresse
- Slump-Port-ID
- NSM-Repository

Das Installationsprogramm erstellt die Datei "NX.env" und einen Windows-Dienst zum Starten und Anhalten des Event Converter.

7. Melden Sie sich abhängig von Ihrer CA SDM-Konfiguration bei folgendem Server an:
 - Konventionell: Primärserver oder Sekundärserver
 - Erweiterte Verfügbarkeit: Einer der Anwendungsserver.
8. Navigieren Sie in das folgende Verzeichnis, und öffnen Sie die Datei "topology.cfgf":

\$NX_ROOT/site/eh

9. Stellen Sie sicher, dass die Datei folgende Informationen enthält:

```
# <remote_node>:uniconv uniconvert IP_ADDR_tngfilter:tngfilter uni
IP_ADDR_tngcnv:tngcnv tngcnv <IP_ADDR_tngfilter>:tngfilter tng
IP_ADDR_tngfilter:tngfilter filter_nxd <IP_ADDR_tngwriter>:tngwriter -
IP_ADDR_tngwriter:tngwriter ehwriter - -
```

IP_ADDR_tngcnv

Gibt die IP-Adresse des Servers an, auf dem der CA NSM-Event Converter-Prozess ausgeführt wird.

IP_ADDR_tngfilter

Gibt die IP-Adresse des Servers an, auf dem CA SDM ausgeführt wird.

IP_ADDR_tngwriter

Gibt die IP-Adresse des Servers an, auf dem CA SDM ausgeführt wird.

10. Speichern Sie die Datei.

Die CA NSM-Integrationskomponente ist installiert.

11. [\(Nur Unix\) Konfigurieren Sie den Event Converter](#) (siehe Seite 187).

Der Event Converter ist konfiguriert.

(Nur UNIX) Konfigurieren des Event Converter

Nachdem Sie CA SDM und CA NSM integriert haben, müssen Sie auch den Converter konfigurieren.

Gehen Sie wie folgt vor:

1. Melden Sie sich in der Web-Benutzeroberfläche aus folgenden Servern an, abhängig von Ihrer CA SDM-Konfiguration:

- Konventionell: Primärserver oder Sekundärserver
- Erweiterte Verfügbarkeit: Anwendungsserver oder Hintergrundserver

2. Wählen Sie auf der Registerkarte "Administration" die Option "System", "Konfigurationen" aus.

Die Seite "Konfiguration - Liste" wird geöffnet.

3. Wählen Sie die Konfiguration für den Server aus, auf dem der Event Converter installiert ist.

Die Seite "Konfigurationsdetail" wird geöffnet.

4. Klicken Sie auf "Zusätzliche Prozesse".

"Zusätzlicher Prozess - Liste" wird angezeigt.

5. Klicken Sie auf "Prozess hinzufügen".

Das Fenster "Neuen Prozess erstellen" wird geöffnet.

6. Wählen Sie "UNI-Konverter" als Prozess aus.

7. Geben Sie die IP-Adresse des Servers ein, auf dem der Event Converter installiert ist.

8. Klicken Sie auf "Speichern".

9. Führen Sie abhängig von Ihrer CA SDM-Konfiguration "pdm_configure" auf folgendem Server aus:

- Konventionell: Primärserver.
- Erweiterte Verfügbarkeit: Anwendungsserver.

10. Dadurch werden die neuen Konfigurationseinstellungen beim Neustart des Servers wirksam.

Wichtig! Reinitialisieren Sie die Datenbank nicht während der Neukonfiguration.

11. Führen Sie als berechtigter Anwender "pdm_proctor_init" auf dem CA NSM-Server aus, um den CA SDM-Proctor zu starten.
12. Starten Sie die CA SDM-Dienste als berechtigter Anwender neu, um die CA SDM-Daemons zu starten. Geben Sie "pdm_status" ein, um den Status der Daemons anzuzeigen.

Der Event Converter ist konfiguriert.

CA SDM-Event Converter

Diese Informationen beziehen sich nur auf die CA NSM-Integration in eine Windows-Betriebsumgebung. Der CA SDM-Event Converter wird auf zwei unterschiedliche Arten installiert, wenn Sie die CA SDM-Konfiguration auf einem Windows-Server ausführen:

- Als Windows-Dienst
- Wird als Teil des CA SDM-Daemon-Servers installiert, von wo aus Sie den Konverter starten und anhalten können

Obwohl Sie beide Methoden verwenden können, um den Converter auf der CA SDM-Serverinstallation zu starten (abhängig von Ihrer CA SDM-Konfiguration), kann er auf Clients nur als Windows-Dienst gestartet werden.

Hinweis: Wenn CA SDM aus einem beliebigen Grund heruntergefahren wird, ist es ratsam, den Event Converter aktiv zu lassen, damit Nachrichten weiterhin von NSM empfangen werden können. Wenn Nachrichten von NSM empfangen werden, während CA SDM heruntergefahren ist, werden diese Nachrichten in die Warteschlange gestellt und nach dem Neustart von CA SDM verarbeitet.

Löschen von Event Converter (Windows-Dienst)

Wenn Sie den Daemon-Manager zum Starten und Stoppen des Event Converters verwenden möchten, löschen Sie mithilfe des folgenden Befehls den Event Converter aus dem Windows-Dienst:

```
tngcnv -u
```

Sie können den Event Converter als einen Windows-Dienst durch den folgenden Befehl erneut installieren:

```
tngcnv -i
```

Löschen des Event Converters (Daemon-Manager)

Der Daemon-Manager startet und stoppt den Converter nicht nur, sondern er startet den Converter auch neu, falls dieser versehentlich gestoppt wird. Sie können *"pdm_status"* verwenden, um festzustellen, ob der Converter läuft oder nicht, und um zu bestimmen, ob er auf dem lokalen oder auf einem Remote-(Sekundär-)Server ausgeführt wird.

Wenn Sie möchten, dass der Windows-Dienste-Manager den Converter startet und stoppt, löschen Sie den Event Converter aus der Startkonfiguration des Daemon-Managers.

Um die *"tngcnv"*-Zeile zu aktivieren oder zu deaktivieren, melden Sie sich abhängig von Ihrer CA SDM-Konfiguration bei folgenden Servern an, und navigieren Sie über die CA SDM-Web-Benutzeroberfläche zu *"System"*, *"Konfigurationen"*:

- Konventionell: Primärserver oder Sekundärserver.
- Erweiterte Verfügbarkeit: Anwendungsserver.

Wichtig! Diese Änderung wird rückgängig gemacht, wenn Sie die CA SDM-Konfiguration erneut ausführen. Wenn Sie die Änderung nach Ausführen der Konfiguration beibehalten wollen, ändern Sie *"pdm_startup.tpl"*.

Überprüfen der Hinweise zur Post-Integration

Beachten Sie bei der Auswahl während des Integrationsprozess folgende Informationen:

- Bevor der Prozess zum Empfangen eines CA NSM-Ereignisses und Erstellen einer Anfrage in CA SDM funktionieren kann, müssen Sie alle Komponenten installieren, konfigurieren und sicherstellen, dass sie aktiv sind.
- Ein Ereignis geht nur dann verloren, wenn der Event Converter-Dienst beendet worden ist. Der Event Converter-Dienst fügt CA NSM-Ereignisse in eine Warteschlange ein, wenn das CA SDM-System angehalten (d. h. in Microsoft Windows unter *"Dienste"* angehalten und nicht beendet) wurde. Nach dem erneuten Start von CA SDM werden die in der Warteschlange befindlichen Ereignisse verarbeitet.

- DerCA NSM-Event Converter-Dienst fügt die Ereignisse bis zu der Maximalanzahl in die Warteschlange ein, die in der Umgebungsvariablen "NX_TNGCNV_QUEUE_SIZE" angegeben ist.
- Wenn das CA NSM-Repository nach der Integration mit CA SDM neu erstellt wird, gehen die CA SDM-Menüeinträge verloren. Um diese wiederherzustellen, müssen Sie die Integration auf dem CA NSM-Windows-Rechner erneut ausführen. Dazu müssen sie die Datei "integAHD.exe located" im Verzeichnis "installation-directory\bin" ausführen.
- Wenn der CA NSM-Event Converter während der Erzeugung von CA NSM-Ereignissen startet, gehen diejenigen Ereignisse verloren, die vor der vollständigen Initialisierung des Converters aufgetreten sind.

Überprüfen der CA NSM-Integration

Stellen Sie folgende Aktionen fertig, um die CA NSM-Integration zu überprüfen:

- [Erstellen von Anlagen, die Eigentümern zugeordnet sind](#) (siehe Seite 190)
- [Überwachen von Meldungen der Event-Konsole](#) (siehe Seite 192)
- [Hinweise zu Filterregeln](#) (siehe Seite 193)

Erstellen von Anlagen, die Eigentümern zugeordnet sind

Durch viele CA Technologies-Produkte werden in der CA MDB Assets erstellt. Diese stehen CA SDM jedoch nicht automatisch zur Verfügung. Üblicherweise erfasst und verfolgt eine CA SDM-Organisation nur solche Assets, deren Eigentümer sie ist, und die durch einen formalen Prozess erworben wurden. Einige Geräte, die durch andere CA Technologies-Produkte im Netzwerk ermittelt wurden, sollen möglicherweise nicht automatisch für CA SDM verfügbar sein. Zum Beispiel ist der Laptop eines Beraters, der das Unternehmen besucht, für die CA SDM-Organisation wahrscheinlich nicht interessant.

Um ein in der CA MDB ermitteltes Asset für CA SDM verfügbar zu machen, verwenden Sie das Auswahldialogfeld "Ermittelte Assets" in den Formularen "Asset-Suche" oder "Neues Asset erstellen" der Web-Schnittstelle für Analysten.

Hinweis: Das Auswahldialogfeld "Ermittelte Assets" ist nur auf dem Webclient verfügbar.

Im integrierten WorldView können ermittelte Assets mit dem Befehlszeilendienstprogramm "pdm_nsmimp" für CA SDM verfügbar gemacht werden. Mit Hilfe der CA NSM 2D/3D-Zuordnung und Unicenter Explorer können Sie Anfragen erstellen und auf diese zugreifen. Dazu klicken Sie mit der rechten Maustaste auf ein verwaltetes Objekt, um die beiden Menüoptionen "Anfrage erstellen" und "Anfrageliste" anzuzeigen. Diese Menüoptionen werden CA NSM bei der Integration in CA SDM hinzugefügt.

Registrieren von ermittelten Assets

Das Dienstprogramm "pdm_discimp" wird für die Stapelverarbeitung bei der Registrierung von nicht von CA SDM ermittelten Assets verwendet. Dieses Dienstprogramm kann verwendet werden, um die CA MDB nach Assets zu durchsuchen, die von anderen Softwareprodukten registriert wurden und diese als CA SDM-Assets zu registrieren, so dass sie in CA SDM verwendet werden können. Dabei handelt es sich um einen interaktiven Stapelverarbeitungsprozess.

Die Logik ähnelt dem Dialogfeld "Ermittelte Assets", das vom Web-Formular "Asset-Suche/Asset-Liste" gestartet werden kann. Dieses Programm durchsucht mit Hilfe verschiedener Parameter die Tabellen "ca_logical_asset", "ca_asset" und "ca_logical_asset_property" und registriert anhand der gefundenen Werte neue CA SDM-Assets.

Hinweis: Wenn die Verarbeitung eine leere Asset-Beschriftung ergibt, wird der gefundene Wert für den Host- oder DNS-Namen als Asset-Beschriftung verwendet. Anlagen müssen zumindest eine Benennung und eine Anlagenklasse aufweisen, um für die Verwendung in CA SDM registriert zu werden.

Um die entsprechenden Datensätze für die Verarbeitung auszuwählen, werden aufgrund der Struktur der CA MDB und der CA SDM-Architektur die folgenden Abfragen durchgeführt.

1. Eine Abfrage ruft die Zeilen aus einer Verbindung der Tabellen "ca_logical_asset" und "ca_asset" ab, bei denen Beschriftung, Seriennummer, Kennung und Hostname verglichen werden.
2. Anschließend wird für jede resultierende Zeile eine Abfrage für "ca_logical_asset_property" durchgeführt, um "dns_name" und "mac_address" zu vergleichen.

Das Asset aus der ersten Abfrage wird für die Registrierung ausgewählt, wenn bei der zweiten Abfrage Zeilen zurückgegeben werden.

Hinweis: Dieser Prozess kann die Leistung beeinträchtigen.

Überwachen von Meldungen der Event-Konsole

Die CA SDM-Basisinstallation überwacht automatisch Statusänderungen überwachter Objekte und die Hinzufügung neuer verwalteter Objekte. Sie können Ihre Umgebung so einrichten, dass die Datei "AHD.DLL" verwendet wird, um unter Windows die Konsolenmeldungen zu überwachen und Event-Meldungen an den CA SDM-Server zu senden.

Es wird empfohlen, AHD.DLL zum Senden von Events an CA SDM zu verwenden. Es stehen jedoch auch andere Methoden zur Verfügung, wenn die Event-Konsole auf einem UNIX-System läuft.

Mit dem Event Management in CA NSM können Sie Events identifizieren, auf die Sie reagieren möchten und eine oder mehrere Aktionen angeben, die automatisch eingeleitet werden sollen. Nachdem Sie eine Nachricht und eine zugeordnete Aktion definiert haben, wird die Aktion automatisch durchgeführt, wenn das Event eintritt.

Wenn die Event-Meldung nach der Integration mit CA SDM angezeigt wird, können Sie für folgende Aktionen generische Event-Daten an CA SDM senden:

- Requests erstellen oder vorhandene Requests aktualisieren
- Ankündigungen erstellen und diese an das CA SDM-Scoreboard übertragen

Hinweis: Weitere Informationen über das Erstellen von Requests und Ankündigungen finden Sie in der *Online-Hilfe*.

So beginnen Sie die Integration:

1. Erstellen Sie mit AHD.DLL einen "msg_action"-Datensatz für CA NSM.
2. Leiten Sie diesen Meldungsdatensatz mit dem Befehl "cawto" an die Event-Konsole.

Hinweis: Verwenden Sie den Standardfilter und die mit CA SDM bereitgestellten Regeln, bis Sie sicher sind, dass Ihr System integriert ist. Ändern oder löschen Sie keine Standardregeln, bis Sie sich davon überzeugt haben, dass durch CA NSM-Events Requests erstellt werden. Vermeiden Sie es, die Zeichenkombination "Leerzeichen, Doppelpunkt, Doppelpunkt, Leerzeichen" (::) zu verwenden, wenn Sie Zeichenfolgen für CA NSM-Meldungen erstellen. Anderenfalls kann ein Analysefehler auftreten, wenn das Produkt die Meldung verarbeitet.

Allgemeine Event-Daten senden (nur UNIX)

Um allgemeine Event-Daten zum Filtern der Daemons in CA SDM zu senden, verwenden Sie den Uniconv-Daemon in einer Meldungsaktion in CA NSM Event Management.

Allgemeine Event-Daten können dann dazu verwendet werden, um Requests automatisch in derselben Weise zu generieren wie dies durch die Verwendung von "AHD.DLL" unter Windows geschieht. Dies ist die bevorzugte Methode unter UNIX.

Ankündigungen automatisch schicken

Wenn Sie CA SDM und CA NSM integriert haben, können Sie von CA NSM aus Ankündigungen erstellen und auf dem CA SDM-Scoreboard bereitstellen.

Hinweise zu Filterregeln

Nachdem Sie die Integration korrekt eingerichtet haben und Requests wie festgelegt durch Events erstellt oder aktualisiert werden, können Sie Filterregeln ändern, um unerwünschte Events herauszufiltern.

In der folgenden Tabelle sind einige Tipps für die Codierung von Filterregeln enthalten.

- Starten Sie CA SDM neu, nachdem Sie eine Filterregel geändert haben.
- Verwenden Sie beim Testen Ihrer Filterregeln die Standard-Erstellerregeln.
- Beim Codieren der Parameter *node_ID*, *user_ID* oder *event_ID* in der Filterregel, müssen Sie Groß-/Kleinschreibung eines eingehenden Event anpassen. Um sicherzugehen, dass Sie die Zeichen korrekt angegeben haben, erstellen Sie in CA NSM ein Event für den Parameter, den Sie testen möchten. Dadurch wird ein Request mit den Informationen erstellt, die Sie benötigen. Passen Sie den Request und Ihre Filterregel aneinander an. Zu dieser Regel gehören auch eingehende Konsolenmeldungen.
- Vermeiden Sie es, die Zeichenkombination "Leerzeichen, Doppelpunkt, Doppelpunkt, Leerzeichen" (::) zu verwenden, wenn Sie Zeichenfolgen für CA NSM-Meldungen erstellen. Anderenfalls kann ein Analysefehler auftreten, wenn das Produkt die Meldung verarbeitet.
- Wenn Sie eine Filterregel für ein bestimmtes Event codieren, kann der eingehende Text zu dem Event das folgende Format haben: "Object_Status_Updated minor." Codieren Sie die Filterregel, um nach dem folgenden Text zu suchen:

```
tng::*::*::*::Object_Status_Updated.*minor.*:::(0,1)
```
- Leerzeichen im Event können auch nicht darstellbare Zeichen sein. Codieren Sie den Filter so, dass er ein oder mehrere Zeichen mit einem Punkt und Sternchen (.*) anstelle des Leerzeichens (' ') enthält. Geben Sie am Ende des Events ebenfalls einen Punkt und ein Sternchen (.*) als Platzhalter für alle nicht darstellbaren Zeichen am Ende des Event-Textes an.
- Wenn Sie mehr als einen Parameter in einem Filter kombinieren, wie z. B. *node_ID*, *user_ID* und *event_ID*, dann codieren Sie einen Filter und überprüfen Sie, ob er funktioniert. Fügen Sie dann den nächsten Parameter hinzu, und prüfen Sie, ob er zusammen mit dem ersten funktioniert. Fahren Sie auf diese Weise fort, bis Sie alle Parameter codiert haben.
- Zur Erleichterung beim Debuggen ordnen Sie Ihre Filterregeln von der spezifischsten Regel am Anfang der Datei bis zur allgemeinsten am Ende der Datei an.

Die Event-Erstellerregeln folgen denselben Regeln für das Debuggen wie die Filterregeln. Wenn Sie die Aktion "CR_CREATE" zusammen mit einer Vorlage verwenden, müssen Sie sich vergewissern, dass die Vorlage existiert.

Automatisches Filtern von Ereignissen

Sie können CA SDM so konfigurieren, dass für Fehler- und Ereignismeldungen, die von Netzwerkgeräten oder anderen Ereignisquellen generiert werden, die entsprechenden Anfragen automatisch erstellt werden. Die Definition der Art und Weise, wie Ereignisse gefiltert werden, ermöglicht Ihnen, automatisch festzustellen, wann ein Ereignis auftritt und die Aktionen einzuleiten, die zur Behandlung des Ereignisses angegeben sind. Mit dieser Methode können insgesamt die Effizienz des Betriebs verbessert und das Fehlerpotenzial verringert werden.

Sie können CA SDM für folgende Aktionen konfigurieren:

- Ereignisse anhand von Host, Inhalt, Typ und anderen Informationen aus CA NSM filtern
- automatisch Anfragen für Fehler- und Ereignismeldungen zu erstellen, die von Netzwerkgeräten generiert werden
- Befehle automatisch als Reaktion auf ein Ereignis durchführen

Um Ereignisse automatisch zu filtern, führen Sie die folgenden Schritte aus:

- Filterregeln zur Erkennung der Ereignisse definieren, die eine spezielle Behandlung erfordern
- Ereigniserstellerregeln definieren, mit deren Hilfe die Aktionen benannt werden, die bei Feststellung dieser Ereignisse automatisch durchgeführt werden.

In den Erstellerregeln für Filter und Ereignisse wird eine allgemeine Ereignisdaten-Struktur für das Empfangen und Senden von Daten verwendet. Sie werden mithilfe eines Texteditors definiert und nur im CA SDM-Server gespeichert und bearbeitet.

Alle Ereignisse können durch die Erstellerregeln für Filter und Ereignisse verarbeitet werden. Einige Beispiele für Ereignisse, die Sie filtern und von den Erstellerregeln für Ereignisse verarbeiten lassen können, sind nachfolgend angegeben:

- Hardwarefehler
- Fehler geplanter Batch-Vorgänge
- Übermäßige CPU-Auslastung
- Hohe Geschwindigkeit bei Seitenwechseln

- Ungewöhnliche Dateiaktivität
- Ungewöhnliche Sicherheitszustände

Sie können auf verschiedenen Rechnern eine beliebige Anzahl von Filterdaemons, Ereigniserstellerdaemons und Ereignisquellen konfigurieren. Die Orte und Beziehungen dieser Elemente sind in der Topologiedatei auf dem CA SDM-Server gespeichert.

Hinweis: Nach der Integration in CA NSM können Sie den "uniconv"-Daemon zum automatischen Generieren von Anfragen verwenden (dies ist die bevorzugte Methode für UNIX). "uniconv" wird in einer Meldungsaktion in CA NSM Event Management verwendet

Allgemeine Ereignisdaten

Informationen über Ereignisse werden mithilfe einer *allgemeinen Ereignisdatenstruktur* übertragen. Die allgemeine Ereignisdatenstruktur besteht aus den folgenden Datenelementen:

Source Type

Bezeichnet das Format für das restliche Ereignis.

Node ID

Bezeichnet den Gerätenamen oder die ID.

Benutzer-ID

Bezeichnet den Benutzernamen oder die ID (falls zutreffend).

Major Source

Bezeichnet die Quellenanwendungs-ID.

Minor Source

Bezeichnet den Agenten des Ereignisses oder die weitere Beschreibung.

Datum/Uhrzeit

Bezeichnet Datum und Zeit des Ereignisses

Event ID

Bezeichnet die Zeichenfolge des Quellereignisses, das das Ereignis ausgelöst hat.

Event Data

Bezeichnet die zugeordneten Ereignisdaten.

Relevanz

Bezeichnet den Bedeutungsgrad des Ereignisses.

Kennung

Bezeichnet die vom Daemon gelieferte Zeichenfolge, die sich aus den Regeln ergibt.

Handle Source

Bezeichnet das Daemonkennzeichen, das die Kennung zugewiesen hat.

Handle Status

Bezeichnet den Status als Erstellen, Aktualisieren oder Beenden.

Status Count

Bezeichnet die Anzahl der Aktualisierungen.

Einrichten der Filterregel

Filter empfangen Informationen von Ereignisquellen, die dann an Ereignisersteller weitergegeben werden können. Da Netzwerkgeräte Hunderte von Ereignismeldungen generieren, können Sie Filterregeln verwenden, um die Meldungen zu isolieren, die zur Erstellung von Anfragen verwendet werden können. Filterregeln ermöglichen Folgendes:

- bestimmen, welche Netzwerkereignisse oder Traps gemeldet und wie sie gemeldet werden sollen.
- steuern, was bei Meldung der einzelnen Typen von Ereignissen oder Traps geschehen soll. Zu den gültigen Aktionen gehören „Ignorieren“, „Berichten über“ und „Markieren“.

Wenn die Filterung in CA NSM integriert ist, können Sie mit deren Hilfe Ereignisse von allen Systemen verwalten, die durch CA NSM verwaltet werden, darunter auch SNA- und TCP/IP-Netzwerke.

Durch Filtern von Ereignissen können Sie bestimmte Informationen über einen bestimmten Knoten, Benutzer oder eine Workstation abrufen und diese Informationen dann an Ereignisersteller weitergeben. Sie können Ereignisfilterregeln definieren, um entsprechend Ihren Bedürfnissen nach speziellen Informationen zu suchen und auf diese Weise verdächtige Ereignisse zu erkennen und sie korrigieren, bevor sie Probleme verursachen.

Hinweis: Beim Schreiben von Filterregeln ist es von Vorteil, wenn Sie mit den regulären UNIX-Ausdrücken vertraut sind. Sie können reguläre UNIX-Ausdrücke auch unter Windows benutzen.

Definitionen der Filterregel

In Filterregeln wird die Übereinstimmung mit regulären UNIX-Ausdrücken verwendet, um zu bestimmen, ob es eine zu einem Ereignis passende Filterregel gibt sowie, um Ereignisse zu blockieren, die den Filterregeln nicht entsprechen. Ein besonderer Filter (ID=5) leitet das eingehende allgemeine Ereignis unverändert zum Ereignisersteller weiter. Der Filter übergibt nur gefilterte Ereignisse und weist die Kennungsquelle "*Filter*" und den Kennungsstatus "*Erstellen*", "*Aktualisieren*" oder "*Beenden*" zu.

In CA SDM werde die Hauptquelle, Ereignis-ID, Knoten-ID und die Felder „Benutzer-ID“ aus der allgemeinen Ereignisdatenstruktur verwendet, um eine passende Filterregel zu finden.

Wichtig! Filterregeln geben an Informationen aus Ereignissen an einen anderen Daemon weiter, der Ereignis- Erstellerregeln verwendet, die automatisch Anforderungen erstellen können.

Die Datei mit den Standardfilterregeln "tngfilter_rule.dat" befindet sich auf dem CA SDM-Server in "\$NX_ROOT/site/eh/IP" (UNIX) oder in "*installation-directory*\site\eh\IP" (Windows). "\$NX_ROOT" oder "*installation-directory*" ist das Verzeichnis, in dem Sie CA SDM installiert haben, und "IP" ist die IP-Adresse des Rechners, auf dem der Filter gespeichert ist. In der Regel ist dies der CA SDM-Server.

Diese Datei enthält auch viele Kommentarzeilen, aus denen Sie entnehmen können, wie die verschiedenen Filterregeln aufgestellt werden. Kommentarzeilen beginnen mit dem Rautesymbol (#).

Verwenden Sie einen Texteditor, um die Datei mit den Filterregeln anzuzeigen, zu aktualisieren und zu speichern. Verwenden Sie keinen Editor, der zusätzliche Formatierungszeichen in die Datei einfügt. Zu empfehlen sind WordPad für Windows-Benutzer und vi für UNIX-Benutzer.

Syntax (Filterregeln)

Die Syntax für Filterregeln ist folgende:

```
source_type:::node_ID:::user_ID:::event_ID:::filter
```

Dabei gilt:

Felder in der Regel durch drei Doppelpunkte (:::) getrennt werden. Sie können ein Sternchen (*) als Platzhalterzeichen verwenden, d. h. der Wert des Parameters wird bei der Bestimmung von Übereinstimmungen mit der Ereigniserstellerregel ignoriert.

Hinweis: Die ersten vier Parameter in der Filterregel beschreiben ein Muster, das mit eingehenden Ereignissen verglichen wird. Dieses Muster wird verwendet, um festzulegen, ob der im letzten Parameter der Regel angegebene Filter das eingehende Ereignis verarbeiten soll.

Parameter (Filterregeln)

source_type

Gibt die Arte der Quelle an, die Ereignisse zum Filter leitet. Das Hauptquellfeld des eingehenden Ereignisses wird mit dem Wert in diesem Parameter verglichen. Der Typ des Konverters, der dem Filter Ereignisse sendet, bestimmt im Allgemeinen den Wert dieses Parameters. Gültige Werte sind:

uni

Kennzeichnet den Konverter bei CA NSM unter UNIX.

tng

Kennzeichnet den Konverter bei CA NSM unter Windows.

Wenn ein ankommendes Ereignis mehreren Regeln entspricht, nachdem Quelltypen und Ereignis-IDs bewertet wurden, werden die Knoten-IDs verglichen.

node_ID

Gibt die Knoten-ID an, von der das Ereignis stammt. Dieser Parameter muss exakt der Knoten-ID des eingehenden Ereignisses entsprechen oder diese Filterregel wird nicht verwendet. Ein Sternchen (*) zeigt an, dass die Knoten-ID bei der Bestimmung ignoriert wird, wenn ein ankommendes Ereignis diesem Filterregelmuster entspricht.

Regeln, die der Knoten-ID des eingehenden Ereignisses entsprechen, haben Vorrang vor Regeln, bei denen das Sternchen (*) für die Knoten-ID angegeben ist.

Wenn ein ankommendes Ereignis mehreren Regeln entspricht, nachdem Quelltypen, Ereignis-IDs und Knoten-IDs, bewertet wurden, werden die Anwender-IDs verglichen.

user_ID

Identifiziert einen mit dem Ereignis verknüpften Anwender. Verwenden Sie diesen Parameter, um eine besondere Aktion für Ereignisse eines bestimmten Anwenders auszuführen. Vielen Ereignissen sind keine bestimmten Anwender zugeordnet. Dieser Parameter darf keinen regulären UNIX-Ausdruck enthalten. Geben Sie eine genaue Anwender-ID oder ein Sternchen (*) ein. Ein Sternchen (*) ist der Standardwert, der anzeigt, dass der Anwender bei der Auswahl der Regel ignoriert wird.

Regeln, die der Anwender-ID entsprechen, die dem Ereignis zugeordnet ist, haben Vorrang vor Regeln, bei denen das Sternchen (*) für die Anwender-ID angegeben ist.

event_ID

Gibt das Ereigniskennzeichen an. Sie können einen regulären UNIX-Ausdruck verwenden. Ein Punkt und ein Sternchen (.*) steht für einen beliebigen Ereignisnamen. Geben Sie beispielsweise [Aa].* ein, um ein beliebiges Ereignis zu finden, das mit einem Großbuchstaben oder Kleinbuchstaben „a“ beginnt.

Wenn der Parameter *event_ID* einfachen Text enthält (und keinen regulären Ausdruck), muss er genau mit der Ereignis-ID des generischen Ereignisses übereinstimmen. Teilübereinstimmungen werden nicht berücksichtigt. Wenn es sich bei der *event_ID* um einen regulären Ausdruck handelt, wird die Länge des Gegenstücks zum regulären Ausdruck verwendet, um zu bestimmen, wie gut die *event_ID* der Ereigniserstellerregel der *event_ID* des allgemeinen Ereignisses entspricht.

Wenn ein ankommendes Ereignis mehreren Regeln entspricht, nachdem Quelltypen und Ereignis-IDs bewertet wurden, werden die Knoten-IDs verglichen.

filter

Legt fest, welcher Filter für die Verarbeitung des eingehenden Ereignisses zu verwenden ist, sowie die Parameter, die der Filter benutzt. Das Format ist folgendes:

(filter_id, filter_parameter1, filter_parameter2, ...)

Gültige Werte für *filter_id* sind:

Value=0

Alle Ereignisse melden

Value=2

Selten auftretende Ereignisse ignorieren

Value=3

Ausfälle ignorieren, die kürzer als die in *filter_parameter1* angegebene Länge sind

Value=4

Bursts ignorieren, die kürzer als die in *filter_parameter1* angegebene Länge sind

Value=5

Alle Ereignisse ohne Änderung weiterleiten

Die Anzahl von Filterparametern ändert sich bei jeder *filter_id* gemäß der folgenden Tabelle:

filter_ID	filter_parameter1	filter_parameter2	filter_parameter3
0	0 = Nein, 1 = Ja Zeigt an, ob Ereignisse immer als separate Probleme gemeldet werden sollen.	Keine	Keine
2	Anzahl des Auftretens Gibt an, wie oft ein Ereignis in einem Zeitraum auftreten muss, um als wichtig betrachtet zu werden.	Intervall Gibt die verstrichene Zeit in Sekunden an, in der ein Ereignis stattfinden muss, damit es als wichtig erachtet wird.	0 = Nein, 1 = Ja Zeigt an, ob Ereignisse immer als separate Probleme gemeldet werden sollen.
3	Intervall Gibt die verstrichene Zeit in Sekunden an, in der ein Ereignis stattfinden muss, damit es als wichtig erachtet wird.	0 = Nein, 1 = Ja Zeigt an, ob Ereignisse immer als separate Probleme gemeldet werden sollen.	Keine
4	Intervall Gibt die verstrichene Zeit in Sekunden an, in der ein Ereignis stattfinden muss, damit es als wichtig erachtet wird.	0 = Nein, 1 = Ja Zeigt an, ob Ereignisse immer als separate Probleme gemeldet werden sollen.	Keine
5	Keine	Keine	Keine

Hinweis: Die ersten vier Parameter in der Filterregel beschreiben ein Muster, das mit eingehenden Ereignissen verglichen wird. Dieses Muster wird verwendet, um festzulegen, ob der im letzten Parameter der Regel angegebene Filter das eingehende Ereignis verarbeiten soll.

Ereignisersteller

Ereignisersteller legen fest, was CA SDM tun soll, wenn die Software ein wichtiges Ereignis im Netzwerk feststellt. Der Ereignisersteller verwendet konvertierte Ereignisse (Ereignisse, die eine allgemeine Ereignisdatenstruktur verwenden) von einer Ereignisquelle und Ereignissen, die einen Filter passiert haben, um Anfragen zu erstellen.

Mit Ereigniserstellern können Sie folgende Funktionen ausführen:

- den Typ eines Ereignis kennzeichnen, das von einer Ereignisquelle empfangen wurde
- die Aktion festlegen, die durchgeführt werden soll, wenn der Ereignisersteller Ereignisse dieses Typs empfängt. Zu den gültigen Aktionen gehören:
 - Erstellen von Anfragen
 - Aktualisieren vorhandener Anfragen
 - Ausführen eines Befehls
- Anzeigen, ob eine Protokollierung angelegt wird

Regeldefinitionen von Ereigniserstellern

Wenn CA SDM installiert ist, läuft eine Standardkonfiguration auf dem CA SDM-Server. Mit dieser Standardkonfiguration wird eine Ereignisquelle, ein Filter und ein Ersteller eingerichtet, und sie enthält eine Filterregel, die alle Ereignisse zum Ersteller weiterleitet. Die Standard-Erstellerregel erstellt Anfragen für alle Ereignisse, die sie empfängt.

Die Datei mit den Standard-Erstellerregeln "tngfilter_rule.dat" befindet sich auf dem CA SDM-Server in "\$NX_ROOT/site/eh/IP" (UNIX) oder in "*installation-directory*\site\eh\IP" (Windows). "\$NX_ROOT" bzw. "*installation-directory*" ist das Verzeichnis, in dem CA SDM installiert ist, und "IP" ist die IP-Adresse des CA SDM-Servers.

Sie können den Inhalt dieser Datei mit den Definitionen der Standard-Erstellerregel und den Kommentaren zum Format der Erstellerregeln anzeigen. Die Kommentare befinden sich am Anfang der Datei und die Erstellerregeln am Ende. Kommentarzeilen beginnen mit dem Rautesymbol (#).

Verwenden Sie einen Texteditor, um die Datei mit den Erstellerregeln anzuzeigen, zu aktualisieren und zu speichern. Verwenden Sie keinen Editor, der zusätzliche Formatierungszeichen in die Datei einfügt. Zu empfehlen sind WordPad für Windows-Benutzer und vi für UNIX-Benutzer.

Syntax (Ereigniserstellerregeln)

Die Syntax für Ereigniserstellerregeln lautet:

```
event_ID:::device:::user_ID:::majorSrc:::minorSrc:::action:::template:::  
command:::logging:::event_token:::user_parms
```

Dabei gilt:

Felder in der Regel durch drei Doppelpunkte (:::) getrennt werden. Sie können ein Sternchen (*) als Platzhalterzeichen verwenden, d. h. der Wert des Parameter wird bei der Bestimmung von Übereinstimmungen mit der Ereigniserstellerregel ignoriert.

Parameter (Ereigniserstellerregeln)

event_ID

Legt das Ereigniskennzeichen fest, auf das die Ereigniserstellerregel zutrifft. Sie können einen regulären UNIX-Ausdruck verwenden. Ein Punkt und ein Sternchen (.*) steht für einen beliebigen Ereignisnamen. Geben Sie beispielsweise [Aa].* ein, um ein beliebiges Ereignis zu finden, das mit einem Großbuchstaben oder Kleinbuchstaben „a“ beginnt.

Wenn der Parameter *event_ID* einfachen Text enthält (und keinen regulären Ausdruck), muss er genau mit der Ereignis-ID des generischen Ereignisses übereinstimmen. Teilübereinstimmungen werden nicht berücksichtigt. Wenn es sich bei der *event_ID* um einen regulären Ausdruck handelt, wird die Länge des Gegenstücks zum regulären Ausdruck verwendet, um zu bestimmen, wie gut die *event_ID* der Ereigniserstellerregel der *event_ID* des allgemeinen Ereignisses entspricht.

device

Gibt den Namen des Objekts an, das in der Regel ein Gerät oder Host ist, das bzw. der diesem Ereignis zugeordnet ist. Ein Punkt und ein Sternchen (*) ist der Standardwert und zeigt an, dass das Quellobjekt beim Markieren der Regel ignoriert wird.

Wenn ein ankommendes Ereignis mehreren Regeln entspricht, nachdem Quelltypen und Ereignis-IDs bewertet wurden, werden die Geräte verglichen. Regeln, die dem Gerät des eingehenden Ereignisses entsprechen, haben Vorrang vor Regeln, bei denen das Sternchen (*) für *Gerät* angegeben ist.

Wenn Sie Regeln für die Zuweisung von Gerätenamen definiert haben, kann dieser Parameter nützlich sein. Wenn Sie z. B. Geräte, die sich in den Vereinigten Staaten befinden, mit USxx benennen, können Sie „US.*“ in diesem Parameter angeben, um eine bestimmte Erstelleraktion für Ereignisse von Geräten in den Vereinigten Staaten durchzuführen.

user_ID

Identifiziert einen mit dem Ereignis verknüpften Benutzer. Verwenden Sie diesen Parameter, um eine besondere Aktion für Ereignisse eines bestimmten Benutzers auszuführen. Vielen Ereignissen sind keine bestimmten Benutzer zugeordnet. Dieser Parameter darf keinen regulären UNIX-Ausdruck enthalten. Geben Sie eine genaue Benutzer-ID oder ein Sternchen (*) ein. Ein Sternchen (*) ist der Standardwert, der anzeigt, dass der Benutzer bei der Auswahl der Regel ignoriert wird.

Wenn ein ankommendes Ereignis mehreren Regeln entspricht, nachdem Quelltypen, Ereignis-IDs und Geräte bewertet wurden, werden Benutzer-IDs verglichen. Die Regeln, die der Benutzer-ID entsprechen, die dem Ereignis zugeordnet ist, haben Vorrang vor Regeln, bei denen das Sternchen (*) für die *user_ID* angegeben ist.

majorSrc

Zeigt automatisch die wichtigste Quelle (Typ) an, die Ereignisse an den Ereignisersteller leitet. Dieser Parameter ist erforderlich. Sein Wert wird durch die Ereignisquelle bestimmt. Bei Ereignissen aus CA NSM unter Windows muss der Wert "tng" lauten. Bei Ereignissen aus CA NSM unter UNIX muss der Wert "uni" lauten.

minorSrc

Zeigt automatisch die unbedeutendste Quelle (Typ) an, die Ereignisse an den Ereignisersteller leitet. Bei Ereignissen aus CA NSM enthält dieser Parameter den Ereignistyp. Verwenden Sie ein Sternchen (*), um alle Ereignisse zu akzeptieren.

action

Legt die Aktion fest, die mit einem der folgenden Werte stattfindet, wenn der Ereignisersteller diese Art von Ereignis empfängt:

CR_CREATE

Schreiben einer neuen Anforderung für jedes Ereignis.

CR_UPDATE

Aktualisieren einer vorhandenen Anfrage oder vorhandener Anfragen (falls zutreffen) oder Erstellen einer neuen Anfrage, wenn keine Anfragen gefunden wurden. Standardmäßig werden Datensätze durch Vergleichen der Attribute *log_agent* und *affected_resource* gesucht. Der Benutzer kann die Standardwerte durch Angabe einer Liste von Anforderungsattributen überschreiben

CR_UPDATE_ONLY

Wie "CR_UPDATE", mit der Ausnahme, dass keine neue Anfrage erstellt wird, wenn keine passenden Anfrage gefunden werden.

COMMAND

Ausführen des Befehls, der im Parameter *Command* angegeben ist.

Hinweis: Wenn CA SDM nicht auf eine Anfrage oder einen Change zugreifen kann, versucht die Software nach einem festgelegten Zeitraum erneut eine Aktualisierung.

Vorlage

Gibt den Namen einer Anforderungsvorlage an, die für die Erstellung einer Anforderung zu verwenden ist. Dieser Parameter ist nicht erforderlich und wird ignoriert, wenn die Aktion nicht CR_CREATE ist.

Hinweis: Die Anfragevorlage muss erstellt werden, bevor die Regel definiert wird.

Befehl

Legt den Befehl fest, der ausgeführt werden soll, wenn der Wert des Parameters *Aktion* „COMMAND“ lautet. In dem Befehl können Ersetzungsargumente verwendet werden, die in der folgenden Tabelle aufgeführt sind. Die Argumente werden bei der Ausführung des Befehls durch ihre Echtzeitwerte ersetzt.

&node

Gerätename oder Knotenkennzeichen

&user

Benutzername oder ID

&date

Ereignisdatum

&time

Ereigniszeit

&event-id

Die Zeichenfolge des Quellereignisses, das das Ereignis auslöst hat.

&data

Die zugeordneten Ereignisdaten.

&sev

Ein Maß für die Bedeutung des Ereignisses

&major-src

Die Quellenanwendungs-ID.

&minor-src

Der Name des Agenten oder die weitere Beschreibung des Ereignisses

&handle

Die vom Daemon gelieferte Zeichenfolge, die sich aus den Regeln ergibt.

&src-handle

Das Daemonkennzeichen, das die Kennung zugewiesen hat.

&status-handle

Der Status der Kennung (gültige Werte sind „create“, „update“ oder „terminate“)

Protokollierung

Legt fest, ob die Protokollierung stattfindet, wobei einer der folgenden Werte verwendet wird:

NONE

Keine Protokollierung außer der normalen Fehlerprotokollierung. „NONE“ ist der Standardwert.

PDM

Protokollierung findet im CA SDM-Protokoll (stdlog.0) in dessen internem allgemeinen Ereignisformat statt.

SYS

Protokollierung findet im UNIX-syslog statt, das zur Unicenter Konsole weitergeleitet werden kann. Dem Ereignis wird eine Meldungs-ID ("CAPD 13") zugewiesen, um die Ereignisverarbeitung von der Unicenter Konsole zu ermöglichen

BOTH

Protokollierung findet im CA SDM-Protokoll (stdlog.0) und im UNIX-syslog statt.

event_token

Ein benutzerdefinierter Tag mit 30 Zeichen zur Kennzeichnung einer bestimmten Anfrage, die einer *event_id* (tng-Ereignismeldung) oder allen Meldungen wie *event_id* (z. B. einer *event_id* mit Platzhaltern) zugeordnet ist. *event_token* ist ein Anfrageattribut, das in jeder von der CA NSM-Schnittstelle generierten Anfrage gespeichert wird. Wenn kein *event_token* in der Erstellerregel angegeben ist, wird die Zeichenfolge „tng_generated“ verwendet. Dadurch kann der Benutzer alle Anfragen aktualisieren, die dem Attribut *event_token* entsprechen. Zum Beispiel können zwei verschiedene Meldungen für dieselbe Anlage eindeutige Anforderungen aktualisieren.

Jede CR_UPDATE-Erstellerregel gibt die eindeutigen Meldungsteile und ein eindeutiges *event_token* an. Das *event_token* wird für die Suche und Aktualisierung der entsprechenden Anfrage verwendet. Standardmäßig wird ein Aktivitätsprotokoll, das die Meldung enthält, zur entsprechenden Anforderung hinzugefügt. In einem weiteren Beispiel kann der Benutzer in einer vorhandenen Anfrage das Statusattribut aktualisieren (z. B. status=CL (geschlossen)), indem er dasselbe *event_token* in der Erstellerregel "CR_UPDATE" angibt, die verwendet wurde, als die Anfrage mit Hilfe der Erstellerregel "CR_CREATE" erstellt wurde.

Zum Beispiel bewirkt die erste der nachfolgenden Erstellerregeln, dass der Erstellerprozess (tngwriter) eine Anrufanforderung mit einem „event_token“ erstellt, das der Bedingung „SystemCritical bei Empfang eines NSM-Ereignisses, das durch die Zeichenfolge 'Event1' gekennzeichnet ist“ entspricht. Die zweite Erstellerregel bewirkt, dass der Erstellerprozess bei allen Anrufanforderungen den Statuswert auf „CL“ aktualisiert, bei denen „event_token“ der Bedingung „SystemCritical bei Empfang eines NSM-Ereignisses, das durch die Zeichenfolge 'Event2' gekennzeichnet ist“ entspricht.

```
Event1:...*::*:tng:...*:::CR_CREATE:::::NONE:::SystemCritical:::  
Event2:...*::*:tng:...*:::CR_UPDATE:::::NONE:::SystemCritical:::%SEARCH  
=EVENT_TOKEN;%STATUS=CL
```

user_parms

Enthält die folgenden Informationen:

Anforderungsattributwerte

Anfrageattributwerte werden anhand der folgenden Syntax angegeben: "*%ATTRIBUTE=value*", wobei "*ATTRIBUTE*" ein in "text_api.cfg" identifizierter Attributname ist, der auf eine CA SDM Majic-Aufruf-Anfrageattribut verweist. Diese Datei befindet sich in "\$NX_ROOT/site (UNIX)" bzw. "*installation-directory\site*" (Windows).

Hinweis: Wenn Sie mehrere Schlüsselwort/Wert-Paare verwenden, trennen Sie jedes durch ein Semikolon (";").

Zum Beispiel bewirkt die nachfolgende Erstellerregel, dass der Erstellerprozess ("tngwriter") eine Aufrufanforderung mit einem Zuständigen "mccda04" und einem Kunden "nsm" erstellt, sobald der Prozess ein CA NSM-Ereignis empfängt, das durch die Zeichenfolge "Event4" gekennzeichnet ist.

```
Event4:...*::*:tng:...*:::CR_CREATE:::::NONE:::::%ASSIGNEE=mccda04  
;CUSTOMER=nsm
```

Liste der Anforderungsattribute, für die beim Aktualisieren vorhandener Anforderungsdatensätze eine Übereinstimmung vorliegen muss

Die Syntax für die Liste der Attribute ist nachfolgend angegeben:

%SEARCH=Attribut1[, Attribut2...], wobei "SEARCH" ein feststehendes Schlüsselwort ist und "Attribut1", "Attribut2" usw. die in der Datei text_api.cfg angegebenen Attributnamen sind.

Die Standardsuchliste der Attribute ist „asset_name“ (DEVICE oder UUID) und „LOG_AGENT“. Das Schlüsselwort „SEARCH“ fügt Attribute (für die Suche nach Übereinstimmungen) zur Standardsuchliste hinzu. Das Schlüsselwort „SEARCH_EXPLICIT“ überschreibt die Standardsuchliste vollständig. Für die Suche nach einer Anrufanforderung werden nur die Attribute verwendet, die nach dem Schlüsselwort „SEARCH_EXPLICIT“ folgen.

Zum Beispiel bewirkt die folgende Erstellerregel, dass der Erstellerprozess ("tngwriter") bei allen Aufrufanforderungen mit dem Zuständigen "mccda04" den Statuswert auf "CL" aktualisiert, sobald der Prozess ein CA NSM-Ereignis empfängt, das durch die Zeichenfolge "Event2" gekennzeichnet ist.

```
Event2::.*::.*::tng::.*::CR_UPDATE:::::NONE::SystemCritical::%SEARCH=ASSIGNEE;%STATUS=CL;%ASSIGNEE=mccda04
```

Ein Attribut in der Liste der Attributwerte wird zur weiteren Suche verwendet, wenn das Attribut in der Liste „SEARCH“ oder in „SEARCH_EXPLICIT“ enthalten ist. Wenn es nicht in der Suchliste nicht enthalten ist, wird es zur Festlegung oder zur Aktualisierung des Attributwertes in der Anrufanforderung verwendet. Es kann in derselben Erstellerregel nicht für beides verwendet werden.

Hinweis: Weitere Informationen zu "text_api.cfg" und die Verwendung in CA SDM finden Sie im *Administrationshandbuch*.

Besondere Parameternamen, die durch ihre entsprechenden Werte aus der CA NSM-Ereignisstruktur ersetzt werden

Sie können die folgenden speziellen Parameternamen an beliebiger Stelle in der Zeichenfolge *user_parms* verwenden.

&message

Der CA NSM-Meldung zugeordnete Meldungstext.

&parm>

Parameterfeld der Datei "AHD. DLL" auf dem CA NSM-Bildschirm für die Meldungsaktionen.

&uuid

Eindeutiges Kennzeichen aus CA NSM.

&device

Das Gerät, z. B. Hostname, das die CA NSM-Meldung generiert hat.

&majorsrc

Die wichtigste Quelle (Typ), die Ereignisse an den Ereignisersteller leitet. Bei Ereignissen aus CA NSM unter Windows ist der Wert "tng". Bei Ereignissen aus CA NSM unter UNIX ist der Wert "uni".

&minorsrc

Die unbedeutendste Quelle (Typ), die Ereignisse an den Ereignisersteller leitet.

&node

Das Gerät, z. B. Hostname, das die CA NSM-Meldung generiert hat.

&addr

Die IP-Adresse des Hosts, der die CA NSM-Meldung generiert hat.

&username

Der Benutzername auf dem Host, der die CA NSM-Meldung generiert hat.

&date

Eine Ganzzahl, die darstellt, um wie viele Jahre später als 1970 die CA NSM-Meldung generiert wurde.

&time

Datum und Uhrzeit der CA NSM-Meldung (z. B. Di 4. Jul 10:23:37 2000).

&severity

Der Schweregrad der CA NSM-Meldung.

&tag

Der CA NSM-Meldung zugeordnete Tagdaten.

Zum Beispiel bewirkt die nachstehende Erstellerregel, dass der Erstellerprozess (tngwriter), eine Anrufanforderung mit einem Kunden erstellt, dessen Name dem Benutzernamen („&username“) der Ereignismeldung entspricht, wenn der Erstellerprozess ein NSM-Ereignis empfängt, das durch die Zeichenfolge „Event2“ gekennzeichnet ist.

```
Event2::.*::.*::tng::.*::CR_CREATE:::::NONE:::::%CUSTOMER=&username
```

Mit Hilfe von *event_token* und *user_parms* können Sie Anfangs- oder Aktualisierungswerte für alle Attribute der Anfrage einstellen und angeben, welche Felder übereinstimmen müssen, wenn Sie nach Datensätzen suchen, die aktualisiert werden sollen. Die einzige Einschränkung besteht darin, dass das Beschreibungsattribut in einem vorhandenen Datensatz einer Anrufanforderung keinesfalls aktualisiert wird. Wenn bei einer Datensatzaktualisierung das Beschreibungsfeld angegeben wurde, wird zu dem vorhandenen Datensatz ein Aktivitätsprotokoll hinzugefügt, das den Text der Beschreibung enthält.

CA NSM-Meldungsaktionsdatensatz: ahd.dll AHD_Call <parms...>

Sie können für den "AHD_Call" im Datensatz der CA NSM-Meldungsaktion auch Daten angeben ("**<parms...>**"), die zur Ersetzung des Parameters "&Parm" verwendet werden können, den Sie im Parameter "user_parms" in Ihrer Erstellerregel angegeben haben. Um die Daten, die Sie für "AHD_Call" angegeben haben, auf diese Weise zu verarbeiten, müssen die Daten ("**<parms...>**") durch ein "%" -Zeichen eingeleitet werden, und der Sonderparameter "&Parm" muss im Feld "user_parms" der Erstellerregel an beliebiger Stelle vorhanden sein.

Nachfolgend sind eine CA NSM-Meldungsaktion und eine Erstellerregel angegeben, die zusammen bewirken, dass der Erstellerprozess Anforderungen mit dem Zuständigen "mccda04" erstellt, wenn der Erstellerprozess ein NSM-Ereignis empfängt, das durch die Zeichenfolge "Event3" gekennzeichnet ist.

Ahd.dll AHD_Call %ASSIGNEE=mccda04

Event3:::.*:::.*:::tnng:::.*:::CR_CREATE:::.*:::NONE:::.*:::&Parm

CA SDM-Kunden, die von AHD4.5 oder einer früheren Version aktualisieren, können das Feld "<parms...>" bereits verwenden. Zum Beispiel können Sie diese Daten verwenden, um Übereinstimmungen mit den Erstellerregeln festzustellen. Sie können dies weiterhin tun. Wenn Sie sowohl „alte“ und „neue“ Parameter verwenden möchten, müssen Sie Ihre „alten“ <parms..>-Daten mit einem „&“-Zeichen versehen und daran die „neuen“ Daten anfügen.

Beispiel:

Ahd.dll AHD_Call alte Daten

Ahd.dll AHD_Call% neue user_parms

Ahd.dll AHD_Call alte Daten% neue user_parms

Daten vor dem ersten "%" -Zeichen werden mit der CA NSM-Ereignismeldung verkettet, die im Beschreibungsfeld der Aufrufanforderung abgelegt wird. So funktionierte CA SDM in der Vergangenheit. Daten nach dem ersten „%“-Zeichen werden zur Ersetzung des Parameters „&Parm“ verwendet, gleichgültig, wo Sie ihn im Parameter „user_parms“ Ihrer Erstellerregel angegeben haben.

Syntax des CA SDM-Protokolls (stdlog.0)

Die Syntax der Einträge in der Datei "stdlog.0" lautet:

```
genDate genTime genNode genProc PID level codefile linenum msgID  
:::msgDomain\msgNode::: ::: :::msgGenDomain\msgGenUser:::domainID  
:::msgDate msgTime:::eventID arg tag::: :::IPAddr:filter:filterNum  
:::majorSrc::: :::msgSrc:::msgType:::msgSrcNum::: :::platform
```

Dabei gilt:

Felder in der Regel durch drei Doppelpunkte (:::) getrennt werden.

genDate

Gibt Monat und Tag (der Systemzeit) an, an dem der Protokollvorfall generiert wurde.

genTime

Gibt die Zeit (der Systemzeit) an, zu welcher der Protokollvorfall generiert wurde.

genNode

Gibt den Knotennamen an, der den Protokollvorfall generiert hat. Der Wert besteht in der Regel aus den ersten acht Zeichen des DNS-Namens Knotens, der den Protokollvorfall generiert hat. Dieser Wert ist stets derselbe, da "stdlog.0" nur Einträge von Prozessen enthält, die auf demselben Knoten laufen.

genProc

Gibt den Namen des Prozesses an (z. B. „ehwriter“) der den Protokollvorfall generiert hat. Der Name des Prozesses hängt von der Betriebssystemumgebung ab, muss jedoch dem Namen in der Prozessliste des Task-Managers (Windows) oder in der Ausgabe des Befehles „ps“ (UNIX) entsprechen.

PID

Gibt die numerische Prozesskennung aus der Prozessliste des Task-Managers (Windows) oder aus der Ausgabe des Befehles „ps“ (UNIX) an. Die PID ist dann wichtig, wenn mehrere laufende Prozesse denselben Namen tragen. Zum Beispiel laufen in der Regel mehrere Datenbankagenten gleichzeitig mit demselben Prozessnamen.

level

Gibt die Einschätzung des Programmierers über die Bedeutung der Meldung an. Zu den möglichen Werten gehören: FATAL, EXIT, RESTART, SIGNIFICANT, SEVERE, ERROR, MINIMUM, WARNING, INFORMATION, MILESTONE, TRACE und VERBOSE.

codefile

Gibt den Namen der Code-Quelldatei an, aus der die Meldung generiert wurde.

linenum

Gibt die Zeilennummer in der Code-Quelldatei an, an der die Meldung generiert wurde.

msgID

Gibt die einem TNG-Ereignis zugewiesene ID an.

msgDomain

Gibt den Namen der Domäne an, aus der die Meldung stammt.

msgNode

Gibt den Namen des Knotens an, aus dem die Meldung stammt.

msgGenDomain

Gibt die Domäne an, aus welcher der durch den Wert in „msgGenUser“ gekennzeichnete Benutzer die TNG-Meldung generiert hat.

msgGenUser

Gibt die Benutzer-ID des Benutzers an, der die TNG-Meldung generiert hat.

domainID

Gibt die ID der Domäne an, aus der die TNG-Meldung generiert wurde.

msgDate

Gibt Monat und Tag (der Systemzeit) an, an dem die TNG-Meldung generiert wurde.

msgTime

Gibt die Zeit (der Systemzeit) an, zu welcher die TNG-Meldung generiert wurde.

eventID

Gibt die Zeichenfolge des Quellereignisses oder den regulären Hexadezimal-Ausdruck an, die das Ereignis ausgelöst haben.

arg

Gibt eine Variable an, die in die Textzeichenfolge einer Meldungsaktion eingegeben wird. Wenn Sie z. B. in das Textfeld einer Meldungsaktion den Wert „Ahd. Dll AHD_Call help me“ eingeben, wird das Argument in „stdout.0“ als „args=help me“ wiedergegeben.

tag

Gibt die Tagdaten an, die der TNG_meldung zugeordnet sind.

IPAddr

Gibt die IP-Adresse des Hosts an, der die TNG-Meldung generiert hat.

filter

Gibt den Prozessnamen für die Filterregeldatei an.

filterNum

Gibt die Nummer der Filterregeldatei an.

majorSrc

Gibt die Hauptquelle (oder den Konvertertyp) an. Dies ist eine Zeichenfolge zur Kennzeichnung der Quellenanwendungs-ID. Das heißt, ob Ereignisse von Unicenter TNG für Windows (wodurch der Wert „tng“ lautet), von Unicenter für UNIX (wodurch der Wert „uni“ lautet) oder von einem internen Daemon (wodurch der Wert „-“ lautet) kommen.

msgScr

Gibt die Quelle der Meldung an. Mögliche Werte sind „CNV“ (Konverter), „FLT“ (Filter), „NOS“ (keine Quelle) und „WRT“ (Ersteller).

msgType

Gibt die Art der Meldung an. Mögliche Werte sind „CRT“ (Erstellung), „DSC“ (Erkennung), „TRM“ (Beendigung), and „UPD“ (Aktualisierung)

msgSrcNum

Gibt die Nummer der Meldungsquelle an.

platform

Gibt die Betriebssystemumgebung an, aus der die Meldung stammt. Mögliche Werte sind: AIX, AS400, DECOSF1, DGUX, DYNIX, HPUX, IRIX, MISERVER, MPRAS, MVS, NETWARE, SINIX, SOLARIS, SVR4MP, TANDEM, UNIXWARE, WNT (Windows) oder ein durch UNIX-Agenten definierter Wert.

Laden von Regeln der Ereignisersteller

Wenn Sie Erstellerregeln ändern oder definieren, können Sie diese laden, ohne den CA SDM-Server oder einen der Supportprozesse wie CA NSM Converter oder die Filter- oder Erstellerdemons neu zu starten. Sie können dieses Dienstprogramm verwenden, um vorhandene Erstellerregeln in eine Datei zu schreiben.

Verwenden Sie das Dienstprogramm "wrtrule", um Regeln der Ereignisersteller zu laden.

Syntax (Laden von Ereigniserstellerregeln)

Die Syntax für das Laden von Ereigniserstellerregeln lautet:

```
wrtrule [-v] -c addr [-r rule_file] [-d dump_file]
```

Parameter (Laden von Ereigniserstellerregeln)

-v

Legt den Verbose-Modus fest, sodass während der Ausführung des Dienstprogramms Rückmeldungen angezeigt werden.

"-C addr"

Der Name des Ereigniserstellers gemäß der Anzeige durch „slstat“.

-r rule_file

Der Name der Textdatei, welche die Ereignisse enthält, die geladen werden sollen.

-d dump_file

Der Name der Datei, in die Sie die aktuellen Ereigniserstellerregeln schreiben möchten. Die folgenden Informationen werden in die Datei geschrieben:

- Ausstehende Ereignismeldungen
- Informationen über Netzwerkressourcen im Abrufprozess
- Ereigniserstellerregeln

Hinweis: Obwohl es sich bei "-r rule_file" und "-d dump_file" um optionale Werte handelt, müssen Sie einen der beiden Werte angeben. Sie können beide angeben, wodurch neue Regeln zuerst geladen werden.

Hinweis: Wenn der Ereignisersteller bei Empfang einer Anforderung zum Laden neuer Erstellerregeln eine oder mehrere CA NSM-Ereignismeldungen behandelt, wird der Ladevorgang verzögert, bis der Ersteller die aktuellen Meldungen abgearbeitet hat. Zum Beispiel verarbeitet der Ersteller ein Ereignis, wobei er auf eine Information über eine Netzwerkressource (Anlage) wartet. In diesem Fall wird die Lademeldung verzögert, bis diese Informationen abgerufen wurden und die Anfrage auf eine CA SDM-Anrufanfrage generiert wurde.

Jedoch wird eine Anfrage zum Schreiben der aktuellen Ereignisregeln in eine Datei ohne Verzögerung ausgeführt.

Verwaltung gefilterter Ereignisse

Die Beziehungen zwischen Filter- und Ereigniserstellerdaemons und Ereignisquellen auf verschiedenen Rechnern werden in der Topologiedatei "topology.cfg" im Verzeichnis "\$NX_ROOT/site/eh" (UNIX) oder im Verzeichnis "installation-directory\site\eh" (Windows) auf dem CA SDM-Server verwaltet. Mithilfe der Topologiedatei können Sie von einer Stelle aus das gesamte Ereignis-Behandlungssystem definieren und verwalten. Sie können Dateien an einem einzigen Ort bearbeiten und die Topologie des gesamten Ereignis-Behandlungssystem festlegen, anstatt dies auf mehreren Clients zu tun.

Hinweis: Das Verzeichnis "\$NX_ROOT/site/eh" (UNIX) oder "installation-directory\site\eh" (Windows) auf dem CA SDM-Server enthält auch die Filter- und Ereigniserstellerregeln.

Verwenden Sie einen Texteditor, um die Datei "topology.cfg" anzuzeigen, zu aktualisieren und zu speichern. Zu empfehlen sind WordPad für Windows-Benutzer und vi für UNIX-Benutzer. Benutzen Sie keinen Texteditor, der Formatierungszeichen in einer Datei hinterlässt.

Die Topologiedatei hat folgendes Format:

```
name cmd [dest-name] [converter-type]
```

Dabei gilt:

Name

Gibt den Hostnamen und den eindeutigen Namen des Ereignisbehandlungs-Daemons im Format "*hostname:daemon-name*" an (z. B. "ws2:uconv"). Der *daemon-name* wird in *sstat* angezeigt.

cmd

Gibt den Namen der ausführbaren Datei im Verzeichnis "\$NX_ROOT/bin" (UNIX) oder im Verzeichnis "*installation-directory*\bin" (Windows) an, wie z. B. "tngcnv", "uniconvert", "filter_nxd", oder "ehwriter" an.

dest-Name

gibt den Daemon an, der die allgemeinen Ereignisse von diesem Daemon empfängt (z. B. „ws2:filter1“ und „ws3:wrtr“). Ereigniserstellerdaemons weisen keine Ziel-Daemons auf. Für alle Daemons muss in der Topologiedatei ein Datensatz vorhanden sein.

converter-type

Gibt an, ob Ereignisse von CA NSM für Windows ("tng"), CA NSM für UNIX ("uni"), oder von einem internen Daemon ("-") stammen.

Eine Beispiel-Topologiedatei könnte folgenden Inhalt aufweisen:

```
# maple:uconv    uniconvert  maple:tngfilter  uni
maple:tngcnv    tngcnv      maple:tngfilter  tng
maple:tngfilter filter_nxd  maple:tngwriter  -
maple:tngwriter ehwriter   -                -
```

Beispiel

Es folgt ein Beispiel, in dem eine Organisation gefilterte Ereignisse in einer integrierten Installation von CA SDM und CA NSM implementiert hat.

Um Anfragen automatisch zu erstellen, wenn ein kritischer Status auf der Karte von <NMS> WorldView angezeigt wird, muss der CA SDM-Administrator (Ken) eine Ereignisfilterregel erstellen, um die Ereignisse zu kennzeichnen, auf die eine Reaktion erfolgen soll. Er muss außerdem eine Ereigniserstellerregel erstellen, um die Aktion anzugeben, die auszuführen ist, wenn Ereignisse dieses Typs empfangen werden.

Ken entscheidet sich, zunächst nur eine einfache Filterregel zu verwenden. Wenn er im Laufe der Zeit mit dem System besser vertraut ist, verwendet er einen komplizierteren Satz von Regeln. Er entscheidet, jedes kritische Ereignis von US-Servern zu erfassen. Sein System verwendet die Konvention, der zufolge die Namen aller Server im zusammenhängenden Staatsgebiet der Vereinigten Staaten in einfacher Weise mit „usaxxx“ bezeichnet werden.

Ken bearbeitet zuerst die Filterregeldatei "tngfilter_rule.dat" im Verzeichnis "\$NX_ROOT/site/eh/IP" auf dem CA SDM-Server, wobei IP die IP-Adresse des CA SDM-Servers ist. Er verwendet den UNIX-Editor „vi“, obwohl er jeden anderen Texteditor ebenfalls verwenden könnte, der keine fremden Steuerzeichen hinzufügt (Windows-Anwendern wird WordPad empfohlen, um Dateien zu bearbeiten).

In der Datei "tngfilter_rule.dat" wird die Raute (#) als Kommentarzeichen verwendet. Alle Zeichen nach der Raute werden beim Lesen der Regeln ignoriert. Die meisten Zeilen in Kens Datei "tngfilter_rule.dat" sind auskommentiert, jedoch bemerkt er die folgenden Zeilen:

```
# Alle Ereignisse melden (separat)
uni::*:*:*:*:*:*:(0,1)
tng::*:*:*:*:*:*:(0,1)
```

Diese Zeilen bilden einen offenen Filter, d. h., einen Filter, der alle Ereignisse zum Ereignisersteller weiterleitet.

Ken ändert diese Zeilen in:

```
# Alle Ereignisse melden (separat)
# uni::*:*:*:*:*:*:(0,1)
tng::*:*:*:*:*:*:Object_Status_Updated.*Critical.*:(0,1)
```

Ken kommentiert die "uni"-Zeile aus, weil er momentan nur an Windows CA NSM-Ereignissen interessiert ist. Er gibt „Object_Status_Updated.*Critical.*“ in das Feld event_ID der tng-Zeile ein, weil er möchte, dass nur „Object_Status_Updated.*Critical.*“-Ereignisse den Filter passieren sollen. CA NSM generiert "Object_Status_Updated.*Critical.*"-Ereignisse, wenn der Status eines Objekts kritisch wird.

Nach dem Speichern der Filterregeldatei bearbeitet Ken die Erstellerregeldatei "tngwriter_rule.dat" im Verzeichnis "\$NX_ROOT/site/eh/IP" des CA SDM-Servers, wobei IP die IP-Adresse des CA SDM-Servers ist.

Bei den meisten Zeilen handelt es sich um Kommentarzeilen. In den letzten beiden Zeilen der Datei stehen die Definitionen für die Standard-Erstellerregel. Ken richtet seine Aufmerksamkeit nur auf Ereignisse von CA NSM unter Windows und kommentiert deshalb die erste der beiden Zeilen aus.

Ken formatiert die zweite Zeile anhand der folgenden Schritte:

1. Er hat den Filter bereits so definiert, dass nur kritische Ereignisse den Filter passieren und lässt deshalb die Ereignis-ID mithilfe von „.*“ offen.
2. Er konzentriert sich auf Ereignisse nur von Servern aus den USA und trägt deshalb usa* in das Gerätefeld ein.
3. Er will Ereignisse von allen Anwendern erhalten; daher bleibt das Sternchen (*) im Anwenderfeld erhalten.
4. Er will bei jedem kritischen Ereignis eine neue Anforderung schreiben und belässt daher den Wert „CR_CREATE“ im Aktionsfeld.
5. Er hat bereits eine geeignete Anforderungsvorlage in das System eingegeben und gibt daher deren Namen „CriticalTemplate“ in das Vorlagenfeld ein.
6. Er möchte keine Protokollierung; deshalb bleibt das Protokollfeld auf „NONE“:

Nachfolgend finden Sie die Ergebnisse von Kens Bearbeitung:

```
# .*...*...*...:uni:...*...:CR_CREATE:...:NONE
.*...:usa.*...*...:tng:...*...:CR_CREATE::CriticalTemplate:...:NONE
```

Ken speichert die Erstellerregeldatei und startet den CA SDM-Server neu. Er kann jetzt Ereignisse zu empfangen, und Anfragen automatisch zu schreiben.

Fehlerbehebung bei der CA NSM-Integration

Bei Verwendung von CA NSM mit CA SDM können während der Integration und Konfiguration Fehler auftreten. Lesen Sie die folgenden Informationen, um diese Fehler zu beheben:

- [Fehlermeldungen bei der 2D/3D-Zuordnung \(nur Windows\)](#) (siehe Seite 216)
- [Überprüfung der Serverkonfiguration](#) (siehe Seite 218)
- [Filtern von Fehlermeldungen](#) (siehe Seite 219)
- [Prüfen der Slump-Verbindung](#) (siehe Seite 220)
- [Einschalten der Protokollierung](#) (siehe Seite 221)

Fehlermeldungen bei der 2D/3D-Zuordnung (nur Windows)

Die integrierte 2D/3D-Zuordnung und Unicenter Explorer können CA NSM-Fehler verursachen.

TNGWV object create failure= x

Grund:

Dieser Fehler tritt in der Regel dann auf, wenn das Integrationsskript mehrfach ausgeführt wurde, ohne zuvor die Deintegration auszuführen ("x" steht für eine Zahl).

Aktion:

Führen Sie die folgenden Schritte aus, um CA SDM mit der CA NSM 2D/3D-Zuordnung und Unicenter Explorer zu deintegrieren und anschließend wieder zu integrieren:

1. Geben Sie in der Befehlszeile Folgendes ein:
`installation-directory\bin\deintahd.exe.`
2. Öffnen Sie den CA NSM-Objektbrowser. Klicken Sie auf „Methode“, um eine Liste der Methoden anzuzeigen.
3. Wenn eine AHD-Methode in der Namensspalte aufgeführt ist, markieren Sie „Löschen“ im Objekt-Menü, um diese zu löschen.
4. Klicken Sie auf „Popup_Menü“, um eine Liste der Menüs anzuzeigen.
5. Wenn ein von AHD verwaltetes Objekt (AHDManagedObject) in der Namensspalte vorhanden ist, markieren Sie „Löschen“ im Objekt-Menü, um dieses zu löschen.
6. Bei immer noch geöffnetem Popup-Menü gehen Sie nach unten, bis „Verwaltete Objekte“ (ManagedObjects) in der Namensspalte angezeigt wird.
7. Suchen Sie ein ManagedObject, das einen Methodennamen mit „AHD“ enthält. Ist ein derartiges Objekt vorhanden, markieren Sie „Löschen“ im Objekt-Menü, um dieses zu löschen.
8. Klicken Sie auf „Jasmine_Menu_Action“, um eine Liste von Unicenter Explorer-Methoden anzuzeigen. Wenn eine AHD-Methode in der Namensspalte aufgeführt ist, markieren Sie „Löschen“ im Objekt-Menü, um diese zu löschen.
9. Klicken Sie auf „Jasmine_Menu_Action“, um eine Liste von Unicenter Explorer-Methoden anzuzeigen. Wenn eine AHD-Methode in der Namensspalte aufgeführt ist, markieren Sie „Löschen“ im Objekt-Menü, um diese zu löschen.
10. Beenden Sie den Objektbrowser.
11. Geben Sie in der Befehlszeile Folgendes ein:
`installation-directory\bin\integAHD.exe.`

Ihre Integration in die 2D/3D-Zuordnung und in Unicenter Explorer ist jetzt erfolgreich abgeschlossen. Klicken Sie mit der rechten Maustaste auf ein verwaltetes Objekt der 2D-/3D-Zuordnung oder des Unicenter Explorer, und überprüfen Sie, dass alle CA SDM-Menüoptionen angezeigt werden.

CAE0232E-Repository-Fehlercode 22

Grund:

Diese Meldung zeigt an, dass der Pfad zum ausführbaren Teil der Methode falsch ist.

Aktion:

Fügen Sie den Pfad "installation-directory\bin" Ihrer Pfad-Variablen hinzu oder ändern das Feld "exe_name" in der Methodenliste so, dass der vollständige Pfadverweis darin enthalten ist.

Überprüfung der Serverkonfiguration

Wenn der CA SDM-Server auf einem UNIX- oder Windows-Rechner installiert ist und CA NSM sich auf einem anderen Windows-Rechner befindet, muss der CA SDM-Server gestartet sein und ausgeführt werden. Starten Sie den NSM Event Converter-Service auf dem CA NSM-Rechner. Um sicherzustellen, dass der Converter ausgeführt wird, prüfen Sie die Prozesse im Task-Manager. Wenn "tngcnv" nicht als ausgeführter Prozess angezeigt wird, nachdem der Event Converter-Dienst gestartet wurde, überprüfen Sie die neuesten Versionen der Dateien "tngcnv.n" oder "stdlog.n" (im Verzeichnis "*installation-directory\log*"). Diese Dateien liefern Ihnen Informationen darüber, warum der Event Converter nicht läuft.

Wenn sich der CA SDM-Server und der <NSM-Server auf demselben Windows-Rechner befinden, muss der CA SDM-Dienst gestartet sein und ausgeführt werden. Starten Sie den CA NSM Event Converter-Service auf dem Rechner. Um sicherzustellen, dass der Converter ausgeführt wird, prüfen Sie die Prozesse im Task-Manager. Wenn „tngcnv“ nicht als ausgeführter Prozess angezeigt wird, nachdem der CA SDM-Dienst gestartet wurde, überprüfen Sie Folgendes:

1. Bearbeiten Sie mit Hilfe von WordPad die Datei "pdm_startup" in "*installation-directory\pdmconf*". In dieser Datei sehen Sie einen ähnlichen Text wie den folgenden:

```
[ procset MAIN_PROCKET]
pdm_info
sw_ver_ctl
bpnotify_nxd
PDMBASE
PDMBOP
FILTERING
```

Wurde „FILTERING“ mit einem Semikolon (;) auskommentiert, entfernen Sie das Semikolon.

2. Wenn Sie sich rückwärts bis zum Dateianfang bewegen müssen Sie folgenden Text sehen können:

```
[ procset FILTERING ]
tngfilter
tngwriter
ehc
; UNICNV_REPLACE
; tngcnv:NT_ONLY
```

Wurde eine der oben aufgeführten Optionen mit einem Semikolon (;) auskommentiert, entfernen Sie das Semikolon.

3. Wenn Sie Änderungen an dieser Datei vorgenommen haben, speichern Sie die Änderungen und starten den CA SDM-Server neu

Wenn der Event Converter noch immer nicht als ausgeführter Prozess angezeigt wird, prüfen Sie die neueste Dateiversion von "tngcnv.n" (im Verzeichnis "*installation-directory*\log"). Diese Datei liefert Ihnen Informationen darüber, warum der Event Converter nicht läuft.

Filtern von Fehlermeldungen

Wenn Ihr Event Converter ("tngcnv") nicht startet oder Ihr Konverter läuft, aber es werden keine Anfragen erstellt, enthalten Ihre Protokolldateien eventuell einen Fehler, der darauf hinweist, warum dieser nicht starten oder Ereignisse melden konnte. Eventuell finden Sie eine oder mehrere der folgenden Fehlermeldungen:

Kann Hostnamen nicht in eine IP-Adresse auflösen

Grund:

Diese Meldung zeigt an, dass auf Ihrem CA SDM-Rechner, auf Ihrem CA NSM-Rechner oder auf beiden Host-Einträge fehlen.

Dieser Fehler weist eventuell auch darauf hin, dass der DNS nicht funktioniert oder nicht die korrekte IP-Adresse zurückgibt.

Aktion:

Überprüfen Sie die Datei "%SystemRoot%/system32/drivers/etc/hosts". Ihre Hostdatei muss einen Eintrag für den CA SDM- und den CA NSM-Rechner enthalten. Nach dem Hinzufügen des Hostnamens starten Sie den Konverter (oder den CA SDM-Dienst) wieder. Beispiel:

```
127.0.0.1      localhost      # Local host loop back
141.202.211.11 usbegp11      # This is the NSM client box
141.202.211.12 usbegp12 ahdhost # This is the Service Desk host
                                     # (bei mehreren Einträgen)
```

Kann Repository-Datei nicht finden

Grund:

Diese Meldung zeigt an, dass der Parameter "@NX_REPOSITORY" in der Datei "NX.env" (im Verzeichnis "installation-directory") auf dem Client nicht festgelegt ist.

Aktion:

Bearbeiten Sie "NX.env", fügen den Repository-Namen hinzu und vergewissern sich, dass der Namen richtig geschrieben ist, speichern die Datei und starten den Event Converter wieder.

Die Abhängigkeit existiert nicht oder wurde zur Löschung markiert.

Grund:

Diese Meldung tritt auf, wenn es bei dem Konverter eine Abhängigkeit (wahrscheinlich von MSSQL) gibt, die gelöscht werden muss.

Aktion:

Führen Sie "regedt32" aus und öffnen Sie die Baumstruktur "HKEY_LOCAL_MACHINE -> System -> Current Control Set -> Services -> AHD_Event_Converter". Löschen Sie die MSSQL-Abhängigkeit (oder, falls zutreffend, eine andere), und starten Sie Ihren Windows-Server neu.

Ziel unbekannt, Ereignisse in Warteschlange oder kein Topologie-Eintrag in der Datei "topology.cfg" für den Knoten, Ereignis in Warteschlange

Grund:

Diese Meldung zeigt an, dass die Datei "topology.cfg" auf dem CA SDM-Server korrigiert werden muss.

Aktion:

Korrigieren Sie die Datei topology.cfg nach Bedarf, und starten Sie dann CA SDM und den CA NSM-Konverter erneut. Es folgt ein Beispiel für die Datei "topology.cfg" für CA SDM auf einem Windows-Rechner mit dem Namen "AHD1" und auf einem CA NSM-Rechner mit dem Namen "TNG1":

TNG1:tngcnv	tngcnv	AHD1:tngfilter	tng
AHD1:tngfilter	filter_nxd	AHD1:tngwriter	-
AHD1:tngwriter	ehwriter	-	-

Überprüfen der Slump-Verbindung

Wenn der CA NSM-Konverter läuft und Sie feststellen, dass noch immer keine Ereignisse erstellt werden, müssen Sie die Slump-Verbindung zu CA SDM überprüfen.

Um die Verbindung zu überprüfen, führen Sie folgende Schritte aus:

1. Verwenden Sie den Befehl "s/stat" von der Befehlszeile auf dem CA SDM-Computer aus.

2. Suchen Sie eine Slump-Verbindung zu „tngcnv“.
Wenn Sie keine Verbindung finden, kommuniziert der Konverter nicht mit CA SDM.
3. Starten Sie den CA NSM-Konverter neu, und überprüfen Sie die Verbindung erneut.
4. Wenn die Verbindung noch immer nicht gefunden werden kann, überprüfen Sie die "tngcnv.n"-Dateien (im Verzeichnis "*installation-directory*\log") auf Fehler unter Bezug auf "tngcnv" und Slump-Anmeldung.

Einschalten der Protokollierung

Wenn Sie nach erfolgreicher Slump-Anmeldung noch keine neuen Ereignisse feststellen können, schalten Sie die Protokollierung ein und überprüfen die Dateien auf Hinweise darauf, dass ein Ereignis durch CA NSM durchgekommen ist. Sie können ein Ereignis erstellen, indem Sie in der 2D/3D-Zuordnung einfach den Status an einem verwalteten Objekt ändern.

Um die Protokollierung einzuschalten, ändern Sie die Datei "NX.env" Datei, die sich in "\$NX_ROOT" (UNIX) oder im Verzeichnis *installation-directory* (Windows) befindet, indem Sie die folgende Zeile in die Datei aufnehmen:

```
@NX_LOG_LEVEL_BSTRAP=VERBOSE.
```

Sie können dann die Dateien "tngcnv.n" (im Verzeichnis "*Installation-directory*\log") überprüfen, um zu bestimmen, ob Ereignisse bis zu CA SDM gelangen. Sie sollten etwa Folgendes vorfinden:

```
09/17 16:35:58:01 tngcnv 477 MILESTONE convrtr.c 399
Sending 1:::dogwood:::9994011e-2f7e-11d1-a435-00c04fd478c9:::17.09.97
:::16:35:41:::Object_Status_Updated minor:::BV:141.202.211.0:Segment.1
IP:141,202.211,14 MAC: CNT: LOC: DSC:::3:::tngcnv:1:::tng:::WindowsNT:
:::CNV:::CRT:::1:::
```

In diesem Beispiel weist die Meldung darauf hin, dass der Status an einem verwalteten Objekt in „Geringfügig“ aktualisiert worden ist.

Wenn Sie feststellen, dass Ereignisse bis zu CA SDM gelangen und im Protokoll erscheinen, überprüfen Sie zweimal, um sich zu vergewissern, dass Sie die Standard-Filter- und Standard-Erstellerregeln verwenden. Stellen Sie andernfalls den ursprünglichen Standardfilter und die Standard-Erstellerdateien wieder her, starten Sie den Server neu und erstellen Sie ein Ereignis.

Wenn Sie feststellen, dass Ereignisse nicht an CA SDM weitergegeben werden, vergewissern Sie sich, dass zwei CA NSM-Prozesse, die für die Weitergabe von Ereignissen verantwortlich sind ("canotify.exe" und "caoprdrmn.exe") ausgeführt werden. Wenn sie nicht ausgeführt werden, starten Sie sie anhand der Beschreibung in der CA NSM-Dokumentation. Wenn sie ausgeführt werden, nehmen Sie Kontakt mit dem Support von CA NSM auf.

Verwenden der CA NSM-Integration

Folgende Beispiele zeigen, wie Sie die Integration zwischen CA NSM und CA SDM verwenden:

1. [Erstellen Sie Meldungsdatensätze und Meldungsaktionen](#) (siehe Seite 222) mit begrenztem Inhalt.
2. [Erstellen oder Aktualisieren Sie eine Request mithilfe des cawto-Dienstprogramms](#) (siehe Seite 223).
3. [Verwenden Sie die Beispieldateien](#), (siehe Seite 224) um die vorherigen Aufgaben abzuschließen.

Hinweis: Die Beispiele stellen eine beispielhafte Vorgehensweise für die Konfiguration dieser Standardfunktionalität bereit, und diese Vorgehensweise ist nicht die einzige Möglichkeit, diese Aufgabe auszuführen.

Beispiel-Meldungsdatensätze/-aktionen mit begrenztem Inhalt

Zwei Nachrichtendatensätze, CFNEW und CFUPDATE, die jeweils mittels einer einzelnen Meldungsaktion geschrieben wurden, bilden die wesentlichen Elemente in dem Beispiel für die Integration von NSM in CA SDM (Beispieldateien sind ebenfalls enthalten). Um eine fehlerfreie, robuste und wartungsfreundliche Integration zu erreichen, können Sie die Möglichkeiten nutzen, die Ihnen die folgenden Elemente bieten:

- tngwriter_rule.dat
- Funktionen „CR_UPDATE“ und „CR_UPDATE_ONLY“
- Schlüsselwortliste „text_api“

Hinweis: In diesem Beispiel wird gezeigt, wie Sie Meldungsdatensätze und Meldungsaktionen mit wenig Inhalt erstellen. Der Inhalt wurde in die „cawto“-Befehle verlagert, die in den folgenden Beispielen dargestellt sind. Alternativ dazu können Sie die gewünschten Parameter und den Inhalt im „Text“-Feld der Meldungsaktion platzieren oder auch eine Kombination der beiden Ansätze verwenden.

Beispiel-Meldungsdatensatz für das Ereignis-Management

Wenn Sie diese Integration verwenden, können Sie die Detailseite des Meldungsdatensatzes nutzen, um einen Beispiel-Meldungsdatensatz für das Ereignis-Management anzuzeigen. Reagiert wird auf ein Ereignis mit "CFNEW" beim Start der Ereigniswarnung.

Beispiel-Meldungsaktionsliste

Wenn Sie diese Integration verwenden, können Sie die Meldungsaktionsliste nutzen, die dem Meldungsdatensatz "CFNEW*" zugeordnet ist. Wenn Sie auf dieses Element doppelklicken, können Sie die ausführlichen Informationen anzeigen, die als Teil der Meldungsaktion gespeichert sind. Wenn Sie mit der Integration fortfahren, wird eine detaillierte Ansicht angezeigt, in der das Feld "action" auf "EXTERNAL" festgelegt ist und das Feld "text" den Standard-Integrationstextwert von "AHD.dll AHD_Call" enthält.

Beispiel-Meldungsdatensatz (mit dem nach Ereignissen gesucht wird, die mit "CFUPDATE" beginnen)

Wenn Sie diese Integration verwenden, werden die Details angezeigt, die aus einem zweiten Meldungsdatensatz resultieren. Dieser ist für das Scannen nach Ereignissen konfiguriert, die mit "CFUPDATE" anfangen. Für diesen Meldungsdatensatz wird auch eine identische Meldungsaktion erstellt (wie anhand des vorhergehenden "CFNEW*" -Meldungsdatensatzes dargestellt).

Beispiele für "cawto"-Befehle zur Generierung/Aktualisierung von Anfragen

Um die zuvor erstellten Meldungsdatensätze zu verwenden, senden Sie mithilfe des CA NSM Event Management eine Meldung und nutzen dazu das Dienstprogramm/den Befehl "cawto" aus CA NSM. Mit Hilfe des Befehls "cawto" können Sie eine Anfrage erstellen oder aktualisieren, indem Sie den Befehl in den beiden nachfolgend dargestellten Formaten verwenden.

Hinweis: Mithilfe dieses Ansatzes können Sie alle Warnungen, die Sie benötigen und die zur Ereignis-Management-Konsole gelangen, erfassen und umformatieren (für die Übertragung in ein Format, das für die Einbeziehung in CA SDM geeignet ist).

Verwenden Sie den Befehl „opreload“ der NSM-Ereignisverwaltungskonsole, um die Datensätze der NSM-Ereignismeldungen und die Meldungsaktionen zu aktualisieren, die nach der Erstellung der NSM-Meldungs- und -Aktionsregeln im Arbeitsspeicher abgelegt werden.

Beispiel 1: "cawto"-Formate zum Generieren und Aktualisieren einer neuen Anfrage

Verwenden Sie das folgende "cawto"-Format zum Generieren einer neuen Anfrage:

```
CAWTO -n <NSM-server-name>  
CFNEW;%STRING1=KEYWORD1;%CUSTOMER=ServiceDesk;%SUMMARY=Photos  
required;%CATEGORY=Applications;%DESCRIPTION=Description: Photos required  
Justification: required by regulations for entry
```

Verwenden Sie das folgende "cawto"-Format zum Aktualisieren einer Anfrage:

```
CAWTO -n <NSM-server-name>  
CFUPDATE;%STRING1=KEYWORD1;%STATUS=Closed;%SUMMARY=Cancelled by ServiceDesk
```

Beispiel 2: Alternative "cawto"-Formate zum Generieren und Aktualisieren einer neuen Anfrage

Verwenden Sie das folgende alternative "cawto"-Format zum Generieren einer neuen Anfrage:

```
CAWTO -n <NSM-server-name> CFNEW2;%EVENT_TOKEN=KEYWORD2;%SUMMARY=Server  
Installation Approved;%STATUS=Work in  
Progress;%CATEGORY=Hardware;%DESCRIPTION=Install new server and level V drops to  
existing server location within the data center. Also, install wiring on patch  
panel in router cabinet
```

Verwenden Sie das folgende alternative "cawto"-Format zum Aktualisieren einer Anfrage:

```
CAWTO -n <NSM-server-name>  
CFUPDATE2;%EVENT_TOKEN=KEYWORD2;%STATUS=Closed;%SUMMARY=Closed by Server Team
```

Beispieldateien für die Verwendung bei der Integration

Folgende Beispieldateien sind für Sie verfügbar, wenn CA NSM und CA SDM integriert wird:

- [topology.cfg](#) (siehe Seite 224)
- [tngfilter_rule.dat](#) (siehe Seite 224)
- [tngwriter_rule.dat](#) (siehe Seite 225)

topology.cfg

```
# <remote_node>:uniconv uniconvert <IP_ADDR_tngfilter>:tngfilter uni  
<IP_ADDR_tngcnv>:tngcnv tngcnv <IP_ADDR_tngfilter>:tngfilter tng  
<IP_ADDR_tngfilter>:tngfilter filter_nxd <IP_ADDR_tngwriter>:tngwriter -  
<IP_ADDR_tngwriter>:tngwriter ehwriter - -
```

wobei:

<IP_ADDR_tngcnv>

die IP-Adresse des Servers ist, auf dem der CA NSM-Event Converter-Prozess läuft.

<IP_ADDR_tngfilter>

die IP-Adresse des Servers ist, auf dem CA SDM ausgeführt wird.

<IP_ADDR_tngwriter>

die IP-Adresse des Servers ist, auf dem CA SDM ausgeführt wird.

tngfilter_rule.dat

Verwenden Sie die Standardversion dieser Datei ohne Änderungen.

tngwriter_rule.dat

Die Datei tngwriter_rule.dat enthält Folgendes:

```
# evt
id:::dev:::user:::majorSrc:::minorSrc:::action:::template:::cmd:::log:::event_token:::user_parms
```

wobei:

event id

eine Zeichenfolge oder einen regulären Hexadezimalausdruck enthält.

device

eine Zeichenfolge, einen regulären Hexadezimalausdruck oder ein Sternchen (*) enthält oder leer ist.

Anwender

eine Zeichenfolge oder ein Sternchen (*) enthält oder leer ist.

majorSrc

die Zeichenfolgen „uni“ aus „uniconverter“ oder „tng“ aus „tngconverter“.

minorSrc

die Zeichenfolge oder ein Sternchen (*) enthält.

action

die Aktionsoptionen enthält. Folgende Optionen stehen zur Verfügung:

CR_CREATE

Schreiben eines neuen Request für jedes Event.

CR_UPDATE

Aktualisieren eines vorhandenen Request oder vorhandener Requests (falls vorhanden) oder Erstellen eines neuen Request, wenn keine Requests gefunden wurden. Standardmäßig werden Datensätze durch Vergleichen der Felder „log_agent“ und „affected_resource“ (Anlage) gesucht. Der Anwender kann die Standardwerte durch Angabe einer Liste von Aufruf-Request-Attributen überschreiben

CR_UPDATE_ONLY

Wie „CR_UPDATE“, mit der Ausnahme, dass kein neuer Request erstellt wird, wenn keine passenden Requests gefunden werden.

COMMAND

Führt das in dieser Tabelle beschriebene <cmd> aus.

template

Gibt den Namen einer Request-Vorlage an, die für die Erstellung eines Request zu verwenden ist. Dieser Parameter ist nicht erforderlich und wird ignoriert, wenn die Aktion nicht CR_CREATE ist.

Hinweis: Die Request-Vorlage muss erstellt werden, bevor diese Regel definiert wird.

cmd

Der Befehl wird an die Shell übergeben und bei allen Aktionen außer „COMMAND“ ignoriert.

Protokollierung

Die Optionen für die Protokollierung sind folgende:

KEINE

Keine Protokollierung außer der normalen Fehlerprotokollierung.

SYS

Protokolliert Incidents im UNIX-Systemprotokoll (Unicenter-Meldungskonsole)

PDM

Incidents in das Anwendungsprotokoll schreiben (\$NX_ROOT/log).

BOTH

Incidents in das Anwendungs- und das Systemprotokoll (syslog) schreiben

event_token

(Optional). Ein anwenderspezifischer Tag mit 30 Zeichen zur Kennzeichnung eines bestimmten Request, die einer „event_id“ (tng-Event-Meldung) oder allen Meldungen wie „event_id“ (z. B. einer „event_id“ mit Platzhaltern) zugeordnet ist.

„event_token“ ist ein Request-Attribut, das in allen Requests gespeichert wird, die durch die TNG-Schnittstelle generiert werden. Wenn kein „event_token“ in der Erstellerregel angegeben ist, wird die Zeichenfolge „tng_generated“ verwendet. Dadurch kann der Anwender alle Requests aktualisieren, die dem Attribut „event_token“ entsprechen. Zum Beispiel können jetzt zwei verschiedene Meldungen für dieselbe Anlage eindeutige Requests aktualisieren. Jede CR_UPDATE-Erstellerregel gibt die eindeutigen Meldungsteile und ein eindeutiges event_token an. Das event_token wird für die Suche und Aktualisierung des entsprechenden Request verwendet. Standardmäßig wird ein Aktivitätsprotokoll, das die Meldung enthält, zum entsprechenden Request hinzugefügt.

In einem weiteren Beispiel kann der Anwender in einem vorhandenen Request das Statusattribut aktualisieren (z. B. status=CL (geschlossen)), indem er dasselbe „event_token“ in der Erstellerregel „CR_UPDATE“ angibt, die verwendet wurde, als der Request mithilfe der Erstellerregel „CR_CREATE“ erstellt wurde.

user_parms

(Optional). Dieser Parameter enthält die folgenden drei Arten von Informationen:

- Request-Attributwerte
- Eine Liste der Request-Attribute, für die beim Aktualisieren vorhandener Request-Datensätze eine Übereinstimmung vorliegen muss
- Spezielle Parameternamen, die durch ihre entsprechenden Werte aus der Unicenter TNG-Event-Struktur ersetzt werden

Die Request-Werte und die Liste der Attribute werden mithilfe der folgenden Syntax angegeben: %<SCHLÜSSELWORT>=<Wert>. Wenn Sie mehrere Schlüsselwort/Wert-Paare verwenden, müssen Sie jedes Paar durch ein Semikolon („;“) trennen.

Request-Attributwerte werden mit Hilfe der Syntax "%<ATTRIBUT>=<Wert>" angegeben, wobei "ATTRIBUT" der in der Datei "text_api.cfg" (im Verzeichnis "\$NX_ROOT/site") aufgeführte Attributname ist, der die Zuordnung zu einem Majic-Request-Attribut der AHD-Funktion herstellt.

Die Syntax für die Liste der Attribute zur Überprüfung der Übereinstimmung wird wie folgt angegeben: %SEARCH=<Attribut1>[,<Attribut2>...], wobei „SEARCH“ ein feststehendes Schlüsselwort ist und „Attribut1“ usw. die in der Datei text_api.cfg angegebenen Attributnamen sind.

Sie können die folgenden speziellen Parameternamen an beliebiger Stelle in der Zeichenfolge „user_parms“ verwenden.

&Message

Der CA NSM-Meldung zugeordnete Meldungstext.

&Parm

Das Parameterfeld der Datei "AHD.DLL" im CA NSM-Meldungsaktionsdialogfeld

&Uuid

Eindeutiges Kennzeichen aus Unicenter TNG.

&Device

Das Gerät, z. B. Hostname, das die CA NSM-Meldung generiert hat.

&Majorsrc

Die wichtigste Quelle (Typ), die Events an den Event-Ersteller leitet. Bei Events aus CA NSM unter Windows lautet der Wert "tng". Bei Events aus CA NSM unter UNIX lautet der Wert "uni".

&Minorsrc

Die unbedeutendste Quelle (Typ), die Events an den Event-Ersteller leitet.

&Node

Das Gerät, z. B. Hostname, das die CA NSM-Meldung generiert hat.

&Addr

Die IP-Adresse des Hosts, der die CA NSM-Meldung generiert hat.

&Username

Der Anwendername auf dem Host, auf dem die CA NSM-Meldung generiert wurde.

&Date

Die Ganzzahl für die Zeit seit 1970, zu der die CA NSM-Meldung generiert wurde.

&Time

Datum und Uhrzeit der CA NSM-Meldung. Zum Beispiel Die, 4. Jul 10:23:37 2000.

&Severity

Der Schweregrad der CA NSM-Meldung.

&Tag

Der CA NSM-Meldung zugeordnete Tagdaten.

Beispielsweise sollten bei Verwendung der Angaben aus "Beispiel 2: Alternative "Cawto"-Formate für das Generieren und Aktualisieren eines neuen Request "die Standard-Event-Erstellungsregeln wie folgt geändert werden:

```
*:::.*:::.*:::uni:::.*:::CR_CREATE:::.....NONE
```

in:

```
CFNEW.*:::.*:::.*:::tnng:::.*:::CR_UPDATE:::.....NONE:::..&Parm;%SEARCH_EXPLICIT=STRING1
```

```
CFNEW2.*:::.*:::.*:::tnng:::.*:::CR_UPDATE:::.....NONE:::..&Parm;%SEARCH=Event_Token
```

```
CFUPDATE.*:::.*:::.*:::tnng:::.*:::CR_UPDATE_ONLY:::.....NONE:::..&Parm;%SEARCH_EXPLICIT=STRING1
```

```
CFUPDATE2.*:::.*:::.*:::tnng:::.*:::CR_UPDATE:::.....NONE:::..&Parm;%SEARCH=EVENT_TOKEN;%STATUS=CL
```

Hinweis: Der Parameter "%SEARCH_EXPLICIT" wird verwendet, um sicherzustellen, dass bei Durchführung einer Aktualisierung nach einem entsprechenden Request gesucht wird, indem die Inhalte des Feldes "STRING1" miteinander verglichen werden, bevor die Aktualisierung fortgesetzt wird. Weitere Informationen zu "text_api.cfg", und wie CA SDM die Text-API zum Erstellen von Requests aus CA NSM verwendet, finden Sie im *Administrationshandbuch*.

Weitere Informationen:

[Regeldefinitionen von Ereigniserstellern](#) (siehe Seite 201)

So installieren Sie CA EEM

Hinweis: Lesen Sie die Informationen zur Planung einer erfolgreichen Installation, bevor Sie diese Komponente installieren.

CA SDM r12.9 stellt CA EEM r12 CR2 auf dem Installationsmedium bereit. CA EEM authentifiziert und autorisiert Anwender von CA Technologies-Produkten wie CA Workflow und CA Service Management. Authentifizierung bedeutet, dass mit Hilfe einer Anwenderkennung und einem Kennwort bzw. durch andere Informationen überprüft wird, ob der Anwender ein zulässiger Produktanwender ist. Autorisierung bedeutet, dass der angemeldete Anwender auf bestimmte Funktionen des Produkts zugreifen kann.

Bei jedem Anmeldeversuch eines Anwenders muss CA EEM die zugehörigen Information authentifizieren. Danach wird der Zugriff entweder gewährt oder verwehrt. Zum Beispiel muss ein Anwender über einen CA EEM-Anwenderdatensatz verfügen, um auf die CA Workflow IDE- oder Worklisten-Anwendung zuzugreifen. Wenn Sie Ihre Geschäftsprozesse in CA SDM mit CA Workflow verwalten, müssen Sie zuerst die CA EEM-Installation auf einer unterstützten Betriebsumgebung starten und ausführen. Installieren Sie dann sofort CA Workflow.

Wichtig! Wenn Sie über eine vorhandene CA EEM-Installation verfügen, die Sie zur Authentifizierung von CA Technologies-Produkten verwenden können, dann installieren Sie CA EEM nicht erneut. Installieren Sie stattdessen CA Technologies-Produkte und verweisen Sie auf Ihre vorhandene CA EEM-Installation. Sie benötigen mindestens CA EEM r8.4 SP4 CR05, um eine Integration mit CA SDM r12.9 durchzuführen.

Weitere Informationen:

[Planen der Installation von CA EEM und CA Workflow](#) (siehe Seite 116)

[Installieren von CA EEM \(Windows\)](#) (siehe Seite 230)

[Installieren von CA EEM \(UNIX\)](#) (siehe Seite 232)

Installieren von CA EEM (Windows)

Die CA EEM-Installation können Sie in einer unterstützten Betriebssystemumgebung starten und ausführen.

Wichtig! Wenn Sie über eine vorhandene CA EEM-Installation verfügen, die Sie zur Authentifizierung von CA Technologies-Produkten verwenden können, dann installieren Sie CA EEM nicht erneut. Installieren Sie stattdessen CA Technologies-Produkte und verweisen Sie auf Ihre vorhandene CA EEM-Installation. Sie benötigen mindestens CA EEM r8.4 SP4 CR05, um eine Integration mit CA SDM r12.9 durchzuführen.

So installieren Sie CA EEM:

1. (Optional) Überprüfen Sie, dass Java Runtime Environment (JRE) 1.5 installiert und die JAVA_HOME-Variable gesetzt ist.

Hinweis: Sie können diesen Schritt in CA EEM 8.4 oder einer höheren Version überspringen. Doch dann wird eine Warnung angezeigt, die besagt, dass Sie CA SiteMinder und SAML nicht integrieren können.

2. Legen Sie den Installationsdatenträger in Ihr Laufwerk ein.

Wichtig! Wenn Ihr Computer nicht über ein geeignetes Laufwerk für den Installationsdatenträger verfügt, kopieren Sie die Inhalte des Datenträgers auf den Computer, auf dem Sie CA SDM installieren wollen. Starten Sie die Installation dann erneut. Für eine Remote-Installation über das Netzwerk können Sie ein Laufwerk oder einen Ordner auf dem Netzwerk freigeben und dann eine Verbindung über das Netzwerk herstellen, um die Installation zu starten.

3. Klicken Sie auf "Sprache auswählen".

Das Installationsmenü wird angezeigt.

Hinweis: Wenn das Installationsmenü nicht automatisch angezeigt wird, starten Sie die Installation durch einen Doppelklick auf die Datei "setup.exe", die sich im Stammverzeichnis des Installationsdatenträgers befindet.

4. Klicken Sie die Registerkarte "Produktinstallationen".
5. Klicken Sie auf "CA Embedded Entitlements Manager".
6. Folgen Sie weiterhin den Anweisungen auf dem Bildschirm, um die CA EEM-Installation fertig zu stellen.

CA EEM ist nun installiert und Sie können andere CA Technologies-Produkte installieren.

Hinweis: In CA SDM r12.9 sind Installationsprogramme sowohl für CA EEM 32-Bit als auch für 64-Bit enthalten. Auf einem 32-Bit-Windows-Computer wird CA EEM als 32-Bit-Anwendung ausgeführt, und auf einem 64-Bit-Rechner wird CA EEM als 64-Bit-Anwendung ausgeführt.

Wenn CA iTechnology iGateway jedoch als 32-Bit-Anwendung auf einem 64-Bit-Windows-Computer ausgeführt wird, dann wird CA EEM auch als 32-Bit-Anwendung ausgeführt.

Weitere Informationen:

[Planen der Installation von CA EEM und CA Workflow](#) (siehe Seite 116)

Konfigurieren des CA EEM-SDK im FIPS-Compliance-Modus

Wenn Sie den CA EEM-Server im "Federal Information Processing Standard (FIPS)"-Compliance-Modus konfigurieren, empfehlen wir Ihnen, auch das CA EEM-SDK im FIPS-Compliance-Modus zu konfigurieren.

Gehen Sie wie folgt vor:

1. Navigieren Sie zur Datei "NX_ROOT/pdmconf/eiam.config".
2. Ändern Sie die FIPS-Einstellung des CA EEM Java SDK auf "ON".
3. Speichern Sie die Datei "eiam.config".

Hinweis: Die FIPS-Einstellung von CA EEM C++ SDK ist standardmäßig auf "ON" festgelegt. Weitere Informationen über das Konfigurieren des CA EEM-SDK im FIPS-Compliance-Modus finden Sie in der CA EEM-Dokumentation.

Installieren von CA EEM (UNIX)

CA EEM für Linux und UNIX verwendet ein selbstextrahierendes Shellskript, das Sie durch den Installationsprozess führt. Während des Installationsprozesses zeigt das Skript die Lizenzinformationen an und fordert Sie auf, die Installationsparameter einzugeben. Nach der Eingabe der Installationsparameter beginnt die Installation.

Wichtig! Wenn Sie über eine vorhandene CA EEM-Installation verfügen, die Sie zur Authentifizierung von CA Technologies-Produkten verwenden können, dann installieren Sie CA EEM nicht erneut. Installieren Sie stattdessen CA Technologies-Produkte und verweisen Sie auf Ihre vorhandene CA EEM-Installation. Sie benötigen mindestens CA EEM r8.4 SP4 CR05, um eine Integration mit CA SDM r12.9 durchzuführen.

So installieren Sie CA EEM:

1. Führen Sie das entsprechende Installationsskript auf dem Zielcomputer aus:
 - (Linux) /lnxsrvr.cd1/ca_tps.lnx/EEM/EEMServer.bin -i console
 - (AIX) /aixsrvr.cd1/ca_tps.aix/EEM/EEMServer.bin -i console
 - (Oracle) /solsrvr.cd1/ca_tps.sol/EEM/EEMServer.bin -i console

Die Datei wird dekomprimiert und die Installation beginnt.

2. Geben Sie "Y" ein, um die Lizenzbedingungen anzunehmen (oder "N", um abzulehnen und die Installation abubrechen).

Die Skriptaufforderungen für die Installationsparameter.

3. Geben Sie den Installationspfad für CA EEM ein (oder übernehmen Sie den Standardwert).

Ein Bestätigungsbildschirm mit den Installationsparameterwerten, die Sie eingegeben haben, wird angezeigt.

4. Falls die Angaben im Bestätigungsfenster korrekt sind, geben Sie "Y" ein, um die Installation fortzusetzen. Falls Sie "N" eingeben, wird das Installationsprogramm abgebrochen.
5. Geben Sie das Kennwort für "EiamAdmin" ein.

Hinweis: Der Anwendername des Standard-Administrators lautet "EiamAdmin".

Der Installationsvorgang hängt von den Befehlszeilenparametern und dem Typ des installierten CA EEM-Pakets ab.

Das Skript des Installationsprogramms stellt die Installation von CA EEM auf Ihrem Computer fertig.

So installieren Sie CA Workflow

Hinweis: Lesen Sie die Informationen zur Planung einer erfolgreichen Installation, bevor Sie diese Komponente installieren.

Wichtig! CA Workflow wird nicht mit CA SDM-r12.9-Installationsdatenträgern gepackt. Wenn Sie CA Workflow verwenden wollen, laden Sie die CA SDM-r12.7-ISO von CA Support Online herunter, bevor Sie CA Workflow installieren.

Bei jedem Anmeldeversuch eines Anwenders bei CA Workflow authentifiziert CA EEM dessen Informationen. Danach wird der Zugriff entweder gewährt oder verwehrt. Ein Anwender muss einen CA EEM-Anwenderdatensatz haben, um auf die CA Workflow IDE oder Worklist zugreifen zu können.

Nachdem Sie CA EEM installiert haben, starten Sie die CA Workflow-Installation auf dem CA SDM-Server, um Ihre Geschäftsprozesse zu verwalten.

Wichtig! Wenn Sie CA Workflow installieren, und danach CA SDM deinstallieren, wird auch CA Workflow deinstalliert.

CA Workflow-Protokolle (*pdm_install_wf.log* und *pdm_tomcat_CAWF.log*) befinden sich unter `$NX_ROOT/log`. Nach erfolgreicher CA Workflow-Installation enthält `$NX_ROOT/site/Workflow/log` die Protokolle *wf_admin.log*, *wf_process.log*, *wf_security.log* und *wl_debug.log*.

Weitere Informationen:

[Planen der Installation von CA EEM und CA Workflow](#) (siehe Seite 116)

[Installieren von CA Workflow \(Windows\)](#) (siehe Seite 234)

[Starten und Anhalten von CA Workflow](#) (siehe Seite 284)

[Installieren von CA Workflow \(UNIX\)](#) (siehe Seite 234)

Installieren von CA Workflow (Windows)

Verwenden Sie CA Workflow, um Ihre Business-Prozesse in CA SDM zu verwalten.

Gehen Sie wie folgt vor:

1. Melden Sie sich abhängig von Ihrer CA SDM-Konfiguration bei folgendem CA SDM-Server an:
 - Konventionell: Primärserver oder Sekundärserver
 - Erweiterte Verfügbarkeit: Beliebiger Anwendungsserver.
2. Laden Sie die r12.7-ISO von CA Support Online herunter, und extrahieren Sie sie.
3. Wählen Sie die gewünschte Sprache aus der Liste aus, und klicken Sie auf "Sprache auswählen".

Das Installationsmenü wird angezeigt.

Hinweis: Wenn das Installationsmenü nicht automatisch angezeigt wird, starten Sie die Installation durch einen Doppelklick auf die Datei "setup.exe", die sich im Stammverzeichnis des Installationsdatenträgers befindet.

4. Klicken Sie auf die Registerkarte "Produkt-Installationen" und anschließend auf CA Workflow.
5. Folgen Sie weiterhin den Anweisungen auf dem Bildschirm, um die CA Workflow-Installation fertig zu stellen.

CA Workflow ist installiert, und Sie können die Komponente nun zur Verwendung mit CA SDM konfigurieren.

Weitere Informationen:

[Konfigurieren des Problem Management-Beispiel-Workflows](#) (siehe Seite 292)
[CA Workflow-Integration](#) (siehe Seite 631)

Installieren von CA Workflow (UNIX)

Verwenden Sie CA Workflow, um Ihre Business-Prozesse in CA SDM zu verwalten.

Gehen Sie wie folgt vor:

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

2. Laden Sie die r12.7-ISO von CA Support Online herunter, und extrahieren Sie sie.
3. Navigieren Sie zum Stammverzeichnis der extrahierten ISO, und starten Sie die Installation durch die Ausführung des folgenden Befehls:

```
sh ./setup.sh
```

4. Wählen Sie die gewünschte Sprache aus der Liste aus, und klicken Sie auf "Sprache auswählen".

Das Installationsmenü wird angezeigt.

5. Klicken Sie auf die Registerkarte "Produkt-Installationen" und anschließend auf CA Workflow.

6. Folgen Sie weiterhin den Anweisungen auf dem Bildschirm, um die CA Workflow-Installation fertig zu stellen.

CA Workflow ist installiert, und Sie können die Komponente nun zur Verwendung mit CA SDM konfigurieren.

Weitere Informationen:

[Konfigurieren des Problem Management-Beispiel-Workflows](#) (siehe Seite 292)

[CA Workflow-Integration](#) (siehe Seite 631)

Installieren des Standalone-Clients CA Workflow IDE

Den eigenständigen Client CA Workflow IDE können Sie von den CA SDM-Installationsdatenträgern unter Windows und Linux installieren. Bei UNIX-Installationen ermöglicht dieser Client die Verbindung mit dem UNIX CA Workflow-Server. Sie können unabhängig von der Betriebssystemumgebung auf eine beliebige CA Workflow-Serverinstallation verweisen, indem Sie die URL in der Benutzeroberfläche für die Anmeldung ändern.

<USDK> ist nicht erforderlich, um <WF>-IDE zu installieren. Das Verzeichnis des Installationsprotokolls unterscheidet sich je nachdem, ob auf dem System CA SDM vorhanden ist oder nicht.

- Wenn CA SDM unter Windows und Linux installiert ist, befindet sich das Protokoll im folgenden Verzeichnis:

```
$NX_ROOT/Logs
```

- Ist CA SDM nicht installiert, befindet sich das Protokoll in den nachfolgenden temporären Ordnern:

Windows

```
%temp%
```

Linux

```
/tmp
```

Gehen Sie wie folgt vor:

1. Öffnen Sie den CA SDM r12.7-Installationsdatenträger, und wählen Sie "CA Workflow IDE".
Der Installationsassistent für CA SDM-Komponenten wird angezeigt.
2. Geben Sie das Installationsverzeichnis des Workflow-Clients an, und klicken Sie auf Weiter.
Die Installation ist abgeschlossen.

Überprüfen Sie die CA Workflow IDE-Installation

Sie *müssen* sich vergewissern, dass die CA Workflow IDE-Installation erfolgreich abgeschlossen wurde.

So überprüfen Sie die CA Workflow IDE-Installation:

1. Navigieren Sie zu dem Verzeichnis, das im Feld "Installationsverzeichnis für den Workflow-Client" im Installationsassistenten für CA SDM-Komponenten angegeben ist.
2. Überprüfen Sie, dass das Verzeichnis Folgendes enthält:
 - die Ordner "Client" und "Deinstallation"
 - die Dateien *version.txt* und *wekinstall.log*

Hinweis: Wenn beim Installieren Fehler aufgetreten sind oder sich die Ordner und Dateien in falschen Verzeichnissen befinden, sehen Sie sich das Protokoll `pdm_install_wf_client.log` an.

Unter Windows starten Sie CA Workflow-IDE über das Startmenü, indem Sie "Programme" > "CA" > "Service Desk Manager" > "CA Workflow-IDE" wählen.

Deinstallieren des CA Workflow IDE-Clients (Windows und Linux)

Gehen Sie wie folgt vor:

1. Führen Sie folgenden Befehl aus:

```
<install_location>/jre/bin/java" -cp  
"<install_location>/uninstall/uninstall.jar" run -silent
```

install_location

Gibt das Stammverzeichnis an, in dem der CA Workflow IDE-Client installiert ist.

■ Beispiel für Windows

Wenn "c:\test" das Stammverzeichnis des installierten CA Workflow IDE-Clients ist:

```
"c:\test\jre\bin\java" -cp "c:\test\uninstall\uninstall.jar" run -silent
```

■ Beispiel für Linux

Wenn "/test" das Stammverzeichnis des installierten CA Workflow IDE-Clients ist:

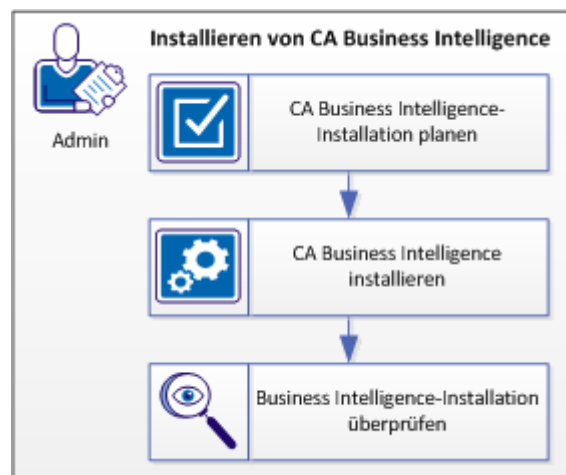
```
"/test/jre/bin/java" -cp "/test/uninstall/uninstall.jar" run -silent
```

2. Löschen Sie das Stammverzeichnis, in dem der CA Workflow IDE-Client installiert ist.
3. (Windows) Löschen Sie die zugehörige Verknüpfung im Startmenü.

So installieren Sie CA Business Intelligence für CA SDM

CA Business Intelligence CABI stellt eine konsistente Installation der SAP Business Objects Enterprise-Edition bereit. Mehrere CA-Produkte können eine CABI-Lizenz gemeinsam nutzen. Sie können CABI als Teil der CA SDM-Installation installieren.

Das folgende Diagramm veranschaulicht die Installation von CABI:



Gehen Sie wie folgt vor:

1. [Planen Sie die Installation für CA Business Intelligence.](#) (siehe Seite 238)
2. [Installieren Sie CA Business Intelligence.](#) (siehe Seite 239)
3. [Überprüfen Sie die Installation für CA Business Intelligence.](#) (siehe Seite 240)

Planen der CA Business Intelligence-Installation

Lesen Sie folgende Hinweise, bevor Sie die Implementierung von CABI für CA SDM planen:

- Verstehen Sie die Anforderungen und Installationshinweise für CABI. Weitere Informationen finden Sie in den *CA Business Intelligence-Versionshinweisen* und dem *CA Business Intelligence-Implementierungshandbuch*.
- Deaktivieren Sie vorübergehend jede Antivirussoftware auf dem Computer, auf dem Sie CABI installieren.
- Unterstützte Anwendungsserver: Die CA SDM-Integration mit CABI unterstützt nur Apache Tomcat als CABI-Anwendungsserver.
- Bestimmen Sie die Lokation der Komponenten, die Sie installieren möchten. Diese Komponenten umfassen das spezifische Subnetz, Computer, Datenbank, Sicherheit oder Cluster-Systeme, die erforderlich sind, um Ihr System auszuführen.
- Überprüfen Sie folgende Voraussetzungen für die Installation:
 - Die Datenbankserverdetails und die Authentifizierungsdetails sind verfügbar.
 - Sie haben die Berechtigung, eine neue SQL Anywhere-Datenbank zu installieren oder eine vorhandene SQL Anywhere-Datenbank zu verwenden.
 - Sie haben den Namen für "Server Intelligence Agent" (SIA).
 - Der Webanwendungsserver wurde installiert und konfiguriert.
 - Installations-Checkliste für das ausgewählte Betriebssystem

Hinweis: Die CABI-Installation ist auf Windows-Plattformen beschränkt. Sie können CABI jedoch auf allen unterstützten Betriebssystemen in CA SDM integrieren.

Installieren von CA Business Intelligence

Sie können die Version 3.3 von CA Business Intelligence auf einem eigenständigen Server installieren, indem Sie den Express-Modus oder den anwenderdefinierten Modus verwenden.

Hinweis: Für die Konfiguration für erweiterte Verfügbarkeit muss CA Business Intelligence auf einem separaten Server installiert sein.

Express-Installation

Verwenden Sie die Express-Installation, um CA Business Intelligence mit allen erforderlichen und optionalen Komponenten zu installieren.

Gehen Sie wie folgt vor:

1. Legen Sie den Installationsdatenträger "DVD 2" in Ihr Laufwerk ein.
Das Installationsmenü wird geöffnet.
2. Wählen Sie die gewünschte Sprache aus der Liste "Sprache auswählen" aus.
Das Installationsmenü wird geöffnet.
3. Klicken Sie auf die Registerkarte "Produktinstallationen".
4. Klicken Sie auf "CA Business Intelligence-Installation".
5. Folgen Sie den Anweisungen auf dem Bildschirm, um die CA Business Intelligence-Installation abzuschließen.

Hinweis: Weitere Informationen finden Sie im *CA Business Intelligence-Implementierungshandbuch*.

6. Starten Sie Ihren Computer neu, wenn Sie dazu aufgefordert werden.
7. CA Business Intelligence unterstützt den gesamten Bereich der Leistungsverwaltungs-, Berichterstellungs- sowie Abfrage- und Analyseanwendungen. Sie müssen das CA Business Intelligence R3.3 SP1-Patch installieren (CABI 3.3 SP1 ist eine Patchversion, die der SAP BOXI 3.1 SP6-Patchversion entspricht), um die CA Business Intelligence-Installation abzuschließen. Um den Patch herunterzuladen und zu installieren, öffnen Sie den folgenden Link:

ftp://ftp.ca.com/pub/CABI/CABI-3.x/boeXIR3_SP6/Windows/

Hinweis: Weitere Informationen zur Installation des Patches finden Sie in *CABI 3.3 SP1-Versionshinweise*.

8. Der CA Business Intelligence R3.3 SP1-Patch-Upgrade unterstützt JDK7. Weitere Informationen finden Sie im Dokument *Upgrading CABI 3.3 SP1 to 7.pdf* im Order "cabi-windows-boeXIR3_SP6\Docs".
9. Wenden Sie den cabi33sp1hotfix-Patch von der folgenden Site an:
ftp://ftp.ca.com/pub/CABI/CABI-3.x/boeXIR3_SP6/Windows/

Hinweis: Anweisungen zur Anwendung des Patches finden Sie in der Datei "readme.txt".

Sie haben CA Business Intelligence installiert.

Anwenderdefinierte Installation

Sie können die Option "Anwenderdefinierte Installation" verwenden, um die ausgewählten Komponenten von CA Business Intelligence zu installieren. Wir empfehlen diese Option nur dann, wenn Sie mit den angegebenen SAP BusinessObjects Enterprise-Komponenten und den Rollen vertraut sind. Die anwenderdefinierte Installation variiert mit der Auswahl des Betriebssystems und der Datenbanken. Weitere Informationen finden Sie im *CA Business Intelligence-Implementierungshandbuch*.

Überprüfen der CA Business Intelligence-Installation

Überprüfen Sie die CABI-Installation auf dem CABI-Server, um sicherzustellen, dass das Produkt ordnungsgemäß installiert wurde.

Gehen Sie wie folgt vor:

1. Wählen Sie "Start", "Programme", "BusinessObjects", "BusinessObjects Enterprise", "BusinessObjects Enterprise Java Infoview" aus.
2. Melden Sie sich beim Infoview an, indem Sie das Administratorkennwort angeben. Eine erfolgreiche Anmeldung weist auf die erfolgreiche Installation von CABI hin.

Überprüfen der Installation

Nachdem Sie CA SDM installiert haben, können Sie anhand der folgenden Informationen überprüfen, ob die Installation erfolgreich war.

1. Vergewissern Sie sich, dass eine Systemumgebungsvariable für den Pfad zum angegebenen Installationsverzeichnis für das Produkt gesetzt ist. Das standardmäßige Stammverzeichnis ist "C:\Programme\CA\Service Desk Manager".
2. Überprüfen Sie folgendes:
 - a. Überprüfen Sie in der Systemsteuerung ("Software" > "Programme hinzufügen oder entfernen"), ob das Produkt in der Liste der Anwendungen aufgeführt ist.
 - b. Stellen Sie im Startmenü sicher, dass folgende Optionen angezeigt werden:
 - Dokumentation anzeigen
 - Konfigurationsassistent starten
 - Web-Schnittstelle starten
 - Wenden Sie sich an den Technischen Support.
 - Starten Sie Web Screen Painter.
 - CA SDM deinstallieren
3. Überprüfen Sie, dass Sie die Web-Schnittstelle starten können.

Wichtig! Wenn Sie diese Information nicht überprüfen können, wurde das Produkt nicht richtig installiert. Starten Sie in diesem Fall die CA SDM-Installation erneut, um sie zu ändern.

Weitere Informationen:

[Starten der Web-Schnittstelle](#) (siehe Seite 252)

Das Installationsprotokoll

Wenn Sie CA SDM installieren, wird ein Installationsprotokoll erstellt, das die Aktionen, Events und Systemänderungen dokumentiert, die während der Installation aufgetreten sind. Wenn das Produkt nicht korrekt installiert wurde, können Sie als Unterstützung zur Fehlerbehebung die Fehler in der Protokolldatei anzeigen.

Die Datei *ServiceDesk_r12_7_Install.log* befindet sich im Ordner "\log" des Installationsverzeichnis. Beim Installieren von Remote-Komponenten befindet sich das Protokoll im Verzeichnis %TEMP%. Öffnen Sie die Datei mit einem Texteditor wie z. B. Editor oder vi.

Hinweis: Wenn Sie die Installation abbrechen, bevor sie abgeschlossen ist, wird das Installationsprotokoll auf Ihrem Desktop (Windows) oder im Stammverzeichnis erstellt (UNIX und Linux).

Kapitel 5: Konfigurieren

Dieses Kapitel enthält folgende Themen:

- [Produktkonfiguration](#) (siehe Seite 243)
- [Konfigurieren der CA SDM-Komponenten](#) (siehe Seite 244)
- [Konfigurieren der Webschnittstelle](#) (siehe Seite 248)
- [So implementieren Sie CA Business Intelligence für CA SDM](#) (siehe Seite 253)
- [So konfigurieren Sie integrierte Windows-Authentifizierung für CA SDM](#) (siehe Seite 274)
- [Ausführen der Automatisierungsrichtlinien](#) (siehe Seite 278)
- [Ausführen der Knowledge-Berichtskarte](#) (siehe Seite 279)
- [Knowledge Management-Beispieldatenimport](#) (siehe Seite 280)
- [Konfiguration der Such-Engine](#) (siehe Seite 281)
- [So konfigurieren Sie CA Workflow:](#) (siehe Seite 283)
- [Konfigurieren der Workflow-Integration in CA Process Automation](#) (siehe Seite 299)
- [Einrichten der automatischen Anmeldung \(CA MDB-Authentifizierung\)](#) (siehe Seite 307)
- [Konfigurieren des "Single Point of Entry"](#) (siehe Seite 308)
- [Implementieren der Mandantenfähigkeit](#) (siehe Seite 309)
- [So aktivieren Sie Auto-Failover](#) (siehe Seite 350)

Produktkonfiguration

Nachdem Sie CA SDM und zusätzlich ausgewählte Produkte installiert haben, müssen Sie bestimmte Schritte zur Konfiguration ausführen, so dass die Produkte zusammen richtig funktionieren. So konfigurieren Sie das Produkt:

- Konfigurieren Sie die CA SDM-Komponenten (Server, die Datenbank, die Web-Schnittstelle).
- Konfigurieren Sie die Web-Schnittstelle, wenn sich Webserver und Primärserver auf unterschiedlichen Computern befinden.
- Konfigurieren Sie Support-Automatisierung.
- Implementieren Sie Berichte zum Lebenszyklus von Knowledge-Dokumenten für Automatisierungsrichtlinien.
- Konfigurieren Sie CA Business Intelligence.
- Konfigurieren Sie CA Workflow.
- Implementieren Sie die Mandantenfähigkeit

Hinweis: Um Server für die erweiterte Verfügbarkeit zu konfigurieren, lesen Sie das Szenario "So konfigurieren Sie Server für erweiterte Verfügbarkeit".

Weitere Informationen:

[Konfigurieren des Problem Management-Beispiel-Workflows](#) (siehe Seite 292)

[Konfigurieren der CA SDM-Komponenten](#) (siehe Seite 244)

[Konfigurieren der Webschnittstelle](#) (siehe Seite 248)

[Ausführen der Automatisierungsrichtlinien](#) (siehe Seite 278)

[Implementieren der Mandantenfähigkeit](#) (siehe Seite 309)

Konfigurieren der CA SDM-Komponenten

Wenn Sie CA SDM nicht während der Installation oder nach der Installation manuell konfigurieren, können Sie mit Hilfe des Produkts den primären und sekundären Server, die Datenbank, die Web-Schnittstelle konfigurieren und zusätzliche Konfigurationsoptionen nutzen.

Um sicherzustellen, dass die Konfiguration von Produkt und Komponenten unter SQL Server erfolgreich ist, sollten Sie TCP/IP auf dem Computer aktivieren, auf dem Sie die Installation und Konfiguration durchführen wollen.

Wichtig! CA SDM r12.9 stellt "tools.jar" und "javac" *nicht* für AIX bereit. Sie *müssen* "tools.jar" unter AIX installieren, bevor Sie die Produktkonfiguration ausführen. Für die Konfiguration von REST-Webservices und Support-Automatisierung ist die Datei "tools.jar" erforderlich. Um die REST-Beispieldateien zu verwenden, müssen Sie "javac" unter AIX installieren. Sie können das Java-SDK für AIX von der IBM-Website im Abschnitt mit IBM Developer Kits für Linux herunterladen. Laden Sie die 32-Bit-Binärdateien von Java SE herunter, und installieren Sie JDK 1.6 SR10 an einem beliebigen Speicherort auf dem AIX-Computer. Kopieren Sie die Datei "tools.jar" aus dem JDK-Installationsverzeichnis in das Verzeichnis "<Shared Component>\JRE\1.6.0_10\lib" und die Datei "javac" in das Verzeichnis "\JRE\1.6.0_10\bin". Der JRE-Speicherort ist auch in Variablen "NX_JRE_INSTALL_DIR" angegeben.

Hinweis: Wenn Hosts mit Internet Protocol Version 4 (IPv4) und Internet Protocol Version 6 (IPv6) gleichzeitig im Netzwerk vorhanden sind, sollten Sie prüfen, ob die entsprechenden Übergangsstrategien, Tools und Mechanismen zur Unterstützung beider Technologien eingerichtet sind, bevor Sie mit der Konfiguration beginnen. Informationen zur Konfiguration von Servern finden Sie im *Administrationshandbuch*.

So konfigurieren Sie die Produktkomponenten:

1. Wählen Sie "Start" > "Programme" > "CA" > "Service Desk" > "Konfiguration".
Der Konfigurationsassistent wird angezeigt.
2. Geben Sie die entsprechenden Informationen ein, und wählen Sie die gewünschten Optionen, um das Produkt zu konfigurieren.
Hinweis: Weitere Informationen über die im Assistenten angezeigten Felder finden Sie in der *Online-Hilfe zur Serverkonfiguration*.
3. Folgen Sie den Anweisungen auf dem Bildschirm, um die Produktkonfiguration abzuschließen.

Wenn Sie das Konfigurationsprogramm zum ersten Mal ausführen, wird ein Standardwert angezeigt, der für die meisten Installationen als Nummer des TCP-Dienstes verwendet werden kann. Um die Nummer des TCP-Dienstes zu bestimmen, starten Sie auf Ihrer Windows-Arbeitsstation eine Telnet-Sitzung zum Server:

- Wenn in Ihrem Netzwerk NIS verwendet wird, geben Sie Folgendes ein:
`ypcat services | grep slump.`
Die Ausgabe umfasst eine Zeile ähnlich der folgenden:
`slump nnnn/tcp # Dies ist erforderlich, damit Slump funktioniert!`
- Wenn in Ihrem Netzwerk NIS nicht verwendet wird, geben Sie Folgendes ein:
`grep slump /etc/services.`
Die Ausgabe umfasst eine Zeile ähnlich der folgenden:
`#slump nnnn/tcp`
Geben Sie die Nummer *nnnn* in das Feld "TCP Service Number" ein.

Hinweis: Wenn die Konfiguration während der Validierung der Erweiterungstabellen fehlschlägt, können Probleme bei der Datenbankverbindung auftreten. Führen Sie die Konfiguration erneut aus, und überprüfen Sie, ob Sie die richtigen Datenbankkonnektivitätsdaten eingegeben haben. Um Server für die erweiterte Verfügbarkeit zu konfigurieren, lesen Sie das Szenario "So konfigurieren Sie Server für erweiterte Verfügbarkeit".

Einrichten des CA CMDB-Auditprotokolls

Die Objekt- und Auslöserdefinitionen, Attribute und HTML-Formulare, die von CA CMDB für das Auditprotokoll verwendet werden, wurden im Produkt geändert.

So richten Sie das CA CMDB-r12.9-Auditprotokoll ein

1. Entfernen Sie den Auslöser "*cmdb_write_audit_log_site*", wenn Sie "*site/mods/extension.mod*" erstellt haben ("*extension*" gibt den Erweiterungsnamen an).

In dieser Produktversion wird das Auditing automatisch erstellt und aktiviert.

2. 'Fügen Sie jedem Attribut, das protokolliert werden soll, 'UI_INFO("AUDIT_LOG")' hinzu.
3. Verwenden Sie die neuen, im Produkt bereitgestellten Vorlagen, um die vorhandenen HTML-Formulare zu migrieren.

Hinweis: Weitere Informationen zur Verwendung von Attributen und HTML-Formularen finden Sie im *Administrationshandbuch*.

Integrieren von CA Cohesion ACM in CA CMDB

Sie können CA Cohesion ACM mit Hilfe eines Patches in CA CMDB integrieren. Wenden Sie sich an die CA-Unterstützung, um den entsprechenden Patch für Ihre Version von CA CMDB und CA Cohesion ACM zu erhalten.

Konfigurieren von CA CMDB Visualizer unter AIX

Gültig für IBM AIX

CA SDM installiert CMDB Visualizer standardmäßig in allen Betriebsumgebungen. Bei Bedarf kann CA CMDB Visualizer konfiguriert werden. IBM AIX benötigt zusätzliche Sicherheitsrichtliniendateien.

So konfigurieren Sie CMDB Visualizer unter IBM AIX

1. Überprüfen Sie, ob CMDB Visualizer konfiguriert ist.
2. Importieren Sie uneingeschränkte Richtliniendateien (Version 1.4.2 oder höher) von der IBM-Website (Seite "Unrestricted JCE policy files").

Hinweis: Sie müssen sich auf der IBM-Website registrieren, um die Richtliniendateien herunterladen zu können.

3. Ersetzen Sie die Dateien "local_policy.jar" und "US_export_policy.jar" im JRE-Verzeichnis für gemeinsame Komponenten (Standardspeicherort: "/opt/CA/SC/JRE/1.6.0_10/lib/security") durch die von der IBM-Website heruntergeladenen Richtliniendateien.
4. Verwenden Sie die folgenden Befehle, um Visualizer anzuhalten und neu zu starten:

```
pdm_tomcat_nxd -c STOP -t VIZ  
pdm_tomcat_nxd -c START -t VIZ
```

CMDB Visualizer ist unter IBM AIX konfiguriert.

Modifizieren von Drittanbieter-Skripten für CA CMDB-Kompatibilität

Für Skripte in der aktuellen Produktversion wurde das Attribut "ext_asset" in "ID" umbenannt. Um die CA CMDB-Kompatibilität mit anderen CA Technologies-Produkten zu gewährleisten, die das "ID"-Attribut verwenden, können Sie die Skripte von Drittanbietern ändern, die CA SDM-Webservices verwenden, um die CA CMDB-Erweiterungstabellen zu aktualisieren.

So modifizieren Sie Drittanbieter-Skripte für CA CMDB

1. Öffnen Sie das Drittanbieter-Skript, das geändert werden soll.
2. Ersetzen Sie alle SQL-Verweise auf "ext_asset" durch "ID".

Das Skript ist mit der aktuellen Produktversion kompatibel.

Umschalten des Zielserver für CA CMDB-Berichte

In der Regel werden aus einem CA Cohesion ACM-System CI-Daten an einen einzigen CA CMDB-Server exportiert, um CA CMDB-Berichte zu erstellen. Sie können den CA CMDB-Zielserver für den Export von CI-Daten wie folgt wechseln:

1. Verwenden Sie einen CA CMDB-Server als Ziel für das Exportieren der CI-Daten, und führen Sie CA CMDB-Berichte aus.
2. Starten Sie den CA Cohesion ACM-Serverservice neu:
3. Wechseln Sie zu einem anderen CA CMDB-Zielserver für das Exportieren der CI-Daten, und führen Sie CA CMDB-Berichte aus.
4. (Optional) Wiederholen Sie die Schritte 2 und 3.

Konfigurieren der Webschnittstelle

Bei der Installation von CA SDM wird die *Web-Schnittstelle* (auch als *Browserschnittstelle* bezeichnet) automatisch installiert. Sie können die Web-Schnittstelle als Vorgang während der Installation konfigurieren.

Wählen Sie den Webserver abhängig von der CA SDM-Konfiguration aus. Denken Sie an die folgenden Verwendungsbeispiele:

- Konventionell: Es sind keine zusätzlichen Aktionen erforderlich, wenn der Webserver und der Primärserver auf dem gleichen Computer sind. Wenn Sie jedoch einen Webserver verwenden und der Primärserver auf einem anderen Computer installiert ist, müssen Sie sowohl den Primärserver als auch den Sekundärserver installieren und konfigurieren.
- Erweiterte Verfügbarkeit: Es sind keine zusätzlichen Aktionen erforderlich, wenn der Webserver und der Hintergrundserver auf dem gleichen Computer sind. Wenn Sie jedoch einen Webserver verwenden und der Hintergrundserver auf einem anderen Computer installiert ist, müssen Sie sowohl den Hintergrundserver als auch den Anwendungsserver installieren und konfigurieren. Die Web-Schnittstelle für Endanwender wird niemals über den Hintergrundserver gehostet. Die Web-Schnittstelle darf nur über die Anwendungsserver gehostet werden.

Wählen Sie den Computer aus, auf dem sich der Webserver befindet und auf dem Sie die Web-Schnittstelle von den folgenden CA SDM-Servern (abhängig von Ihrer CA SDM-Konfiguration) installieren und konfigurieren möchten:

- Konventionell: Sekundärserver. Installieren Sie diesen Server nach dem Primärserver.
- Erweiterte Verfügbarkeit: Anwendungsserver. Installieren Sie diesen Server nach dem Hintergrundserver.

Wichtig! Als Standardwebserver gilt immer Tomcat. Wenn Sie IIS als Webserver nutzen möchten, müssen Sie das Produkt manuell konfigurieren und IIS auswählen. Informationen finden Sie in der *Online-Hilfe zur Serverkonfiguration*.

So konfigurieren Sie die Web-Schnittstelle:

1. (Erforderlich) Aktivieren Sie die Web-Engine auf dem sekundären Server unter Windows oder UNIX.
2. (Erforderlich) [Konfigurieren Sie die Web-Schnittstelle](#) (siehe Seite 252).

Anschließend können Sie [start die Web-Schnittstelle starten](#) (siehe Seite 252).

Weitere Informationen:

[Starten der Web-Schnittstelle](#) (siehe Seite 252)

[Konfigurieren der Web-Schnittstelle](#) (siehe Seite 252)

Hinzufügen von Web-Engines oder Web-Directors

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

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

Gehen Sie wie folgt vor:

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

Die Seite Konfigurationsliste wird geöffnet.

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

Die Seite "Konfigurationsdetail" wird geöffnet.

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

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

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

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

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

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

5. Füllen Sie die folgenden Felder aus:

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

Hostname

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

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

Typ

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

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

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

Web Director

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

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

CGI Name

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

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

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

CGI-Portnummer

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

Standard: 8080

Protokoll

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

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

Datensatzstatus

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

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

Objektmanager

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

Standard

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

BELIEBIGE

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

Auswählen

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

6. Klicken Sie auf "Speichern".

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

Konfigurieren der Web-Schnittstelle

Wenn die während der CA SDM-Installation angegebene Standardkonfiguration für die Web-Schnittstelle Ihren Anforderungen nicht entspricht, ändern Sie die Datei *web.cfg* im Verzeichnis *installationsverzeichnis\bopcfg\www*. Bearbeiten Sie die Datei mit einem Texteditor wie z. B. Editor oder WordPad ohne Formatierung oder Steuerzeichen.

Jeder Eintrag in der Datei besteht aus einer einzelnen Zeile, die einen Eigenschaftsnamen enthält, dem optional ein Wert folgt. Zeilen, die mit einem Rautesymbol (#) beginnen, werden als Kommentare behandelt und daher ignoriert.

Hinweis: Informationen über Einträge in der Datei "web.cfg" finden Sie im *Administrationshandbuch*.

Starten der Web-Schnittstelle

Stellen Sie sicher, dass die Daemon-Serverdienste und der Datenbankserver gestartet sind, bevor Sie die Web-Schnittstelle aufrufen und CA SDM verwenden. Wenn Sie einen sekundären Server konfiguriert haben (wenn Sie z. B. die Web-Schnittstelle auf einem Webserver installiert haben, der sich nicht auf dem Computer mit dem Primärserver befindet), muss der Remote-Daemon-Proctor-Dienst ausgeführt werden, bevor Sie den Dienst für den primären Server starten.

- (Windows) Um die Dienste zu starten, wählen Sie "Systemsteuerung" > "Verwaltung" > "Services" aus. Klicken Sie mit der rechten Maustaste in CA SDM auf "Remote Daemon Proctor", und wählen Sie "Start".
- (Linux) Um die Dienste zu starten, öffnen Sie eine Eingabeaufforderung und führen den Befehl *pdm_client* aus.

Nachdem Sie die Dienste gestartet haben, können Sie die Web-Schnittstelle starten. Die Art und Weise, wie Sie die Web-Schnittstelle starten hängt davon ab, ob der Computer, von dem Sie die Web-Schnittstelle starten, ein primärer oder sekundärer Server ist, und ob Sie IIS verwenden. Sie können die Web-Schnittstelle auch von einer internen Website starten.

- Um die Web-Schnittstelle zu starten, wählen Sie "Start" > "Alle Programme" > "CA" > "Service Desk Manager" > "Webclient für Service Desk Manager".
- Um die Web-Schnittstelle von einem Computer zu starten, der nicht der Primärserver oder ein sekundärer Server ist, öffnen Sie einen Webbrowser und geben die folgende URL ein:

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

In dieser URL ist *servername* der Name des Computers, der den CA SDM-Webserver hostet.

- Um die Web-Schnittstelle von einem Computer zu starten, der weder Primärserver noch ein sekundärer Server ist, und wenn Sie IIS als Webserver nutzen, öffnen Sie einen Webbrowser und geben die folgende URL ein:

`http://servername/CAisd/pdmweb.exe`

- Um die Web-Schnittstelle von einer internen Website zu starten, fügen Sie der URL den Parameter `/pdmweb.exe` für Ihre Webseiten hinzu. Der folgende Beispiel-HTML-Code dient Ihnen als Anleitung:

A HREF=`http://<server-name>:<port-no>/CAisd/pdmweb.exe`

In dieser URL kennzeichnet *server-name* Ihren Computer und *port-no* ist der Empfangsport für den Webserver.

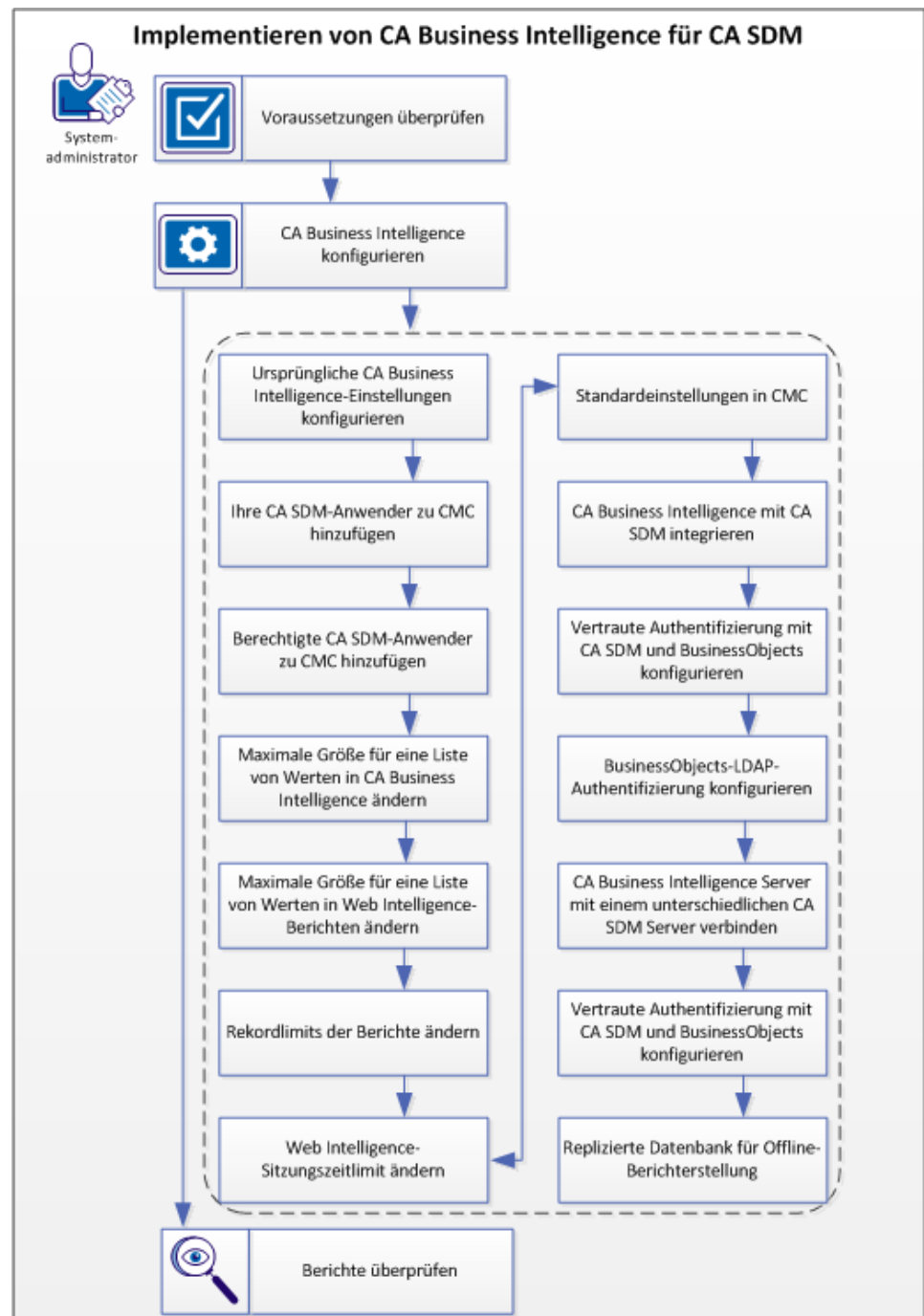
Hinweis: Wenn die Sicherheit Ihres Internet Explorer auf "Hoch" gesetzt ist, wird beim Starten der Web-Schnittstelle eine Warnmeldung über den Inhalt ausgegeben. Um diese Meldung zu vermeiden, fügen Sie diese Website Ihren vertrauenswürdigen Sites hinzu oder setzen Sie Ihre Sicherheitseinstellungen auf ein geringeres Niveau.

In der erweiterten Verfügbarkeit ist die standardmäßige Web-Schnittstelle bereits mit der standardmäßigen Installation und Konfiguration verfügbar.

So implementieren Sie CA Business Intelligence für CA SDM

CA Business Intelligence ist ein Berichts- und Analyse-Software-Set, das von CA SDM zur Präsentation von Informationen sowie zur Unterstützung von Geschäftsentscheidungen eingesetzt wird. CA SDM verwendet CA Business Intelligence, um Informationen zu integrieren und zu analysieren und sie anschließend über verschiedene Berichtsoptionen zu präsentieren. Um Berichte von CA SDM zu generieren, müssen Sie als Administrator CA Business Intelligence installieren, konfigurieren und mit CA SDM integrieren.

Folgendes Diagramm zeigt, wie Sie CA Business Intelligence für CA SDM implementieren können:



Gehen Sie wie folgt vor:

1. [Überprüfen Sie die Hinweise zu Berichten.](#) (siehe Seite 255)
2. [Konfigurieren Sie CA Business Intelligence.](#) (siehe Seite 255)
3. [Überprüfen Sie die Berichte.](#) (siehe Seite 273)

Überprüfen der Voraussetzungen

Lesen Sie folgende Hinweise, bevor Sie die Implementierung von CA Business Intelligence für CA SDM planen:

- CA SDM r12.9 verwendet CA Business Intelligence-Version 3.3.
- Für die Installation von CA Business Intelligence ist es erforderlich, dass Central Management Server (CMS) auf Port 6400 installiert ist.
- Die CA SDM-Anwender, die Zugriff auf Berichte benötigen, müssen zur CMS-Administratorliste hinzugefügt werden, bevor die Berichte verwendet werden.
- Wir empfehlen, dass SAP BusinessObjects-Anwender, die über eine vorhandene Installation von BusinessObjects verfügen, CA Business Intelligence installieren und konfigurieren.
- Wenn Sie Firefox verwenden, um die Berichte anzuzeigen, lesen Sie die *CA SDM-Versionshinweise*, um die empfohlene Version zu überprüfen.
- In den CA SDM-Versionshinweisen finden Sie die unterstützte JRE-Version.
- Crystal Reports Explorer und Desktop Intelligence werden nicht mit CA SDM unterstützt.
- Sie haben einen separaten Server, um CA Business Intelligence zu installieren, wenn Sie die Konfiguration für erweiterte Verfügbarkeit verwenden.

Konfigurieren von CA Business Intelligence

Sie können CA Business Intelligence nach einer erfolgreichen Installation konfigurieren. Sie führen obligatorische Einstellungen aus, um Berichte von CA SDM generieren zu können. Sie benötigen einige obligatorische Konfigurationen, wie z. B. das Hinzufügen von Anwendern und das Festlegen von Sicherheitsparametern, bevor Sie CA Business Intelligence mit CA SDM integrieren.

Gehen Sie wie folgt vor:

1. Konfigurieren Sie die Einstellungen von CA Business Intelligence.
2. Konfigurieren Sie die Datumsbereichswerte und Verknüpfungsparmeter.
3. Fügen Sie CA SDM-Anwender und Gruppen hinzu.
4. Fügen Sie das standardmäßige CA SDM-Konto für den berechtigten Anwender hinzu.
5. Ändern Sie die Standardsicherheits- und Web Intelligence-Einstellungen.
6. Integrieren Sie CA Business Intelligence mit CA SDM.
7. Konfigurieren Sie die vertrauenswürdige Authentifizierung für BusinessObjects und CA SDM.
8. (Optional) Konfigurieren Sie die BusinessObjects-LDAP-Authentifizierung.
9. (Nur für konventionelle Konfiguration anwendbar) Verbinden Sie den CA Business Intelligence-Server mit einem anderen CA SDM-Server
10. Ändern Sie die maximale Größe für eine Werteliste.
11. Ändern Sie das Zeitlimit der Web Intelligence-Sitzung.

Konfigurieren der Anfangseinstellungen von-CA Business Intelligence

In diesem Schritt werden CA SDM-Universe und Berichte geladen, Gruppen erstellt und optional ein Anwender für jede Gruppe erstellt sowie Gruppenberechtigungen festgelegt.

Gehen Sie wie folgt vor:

1. Fügen Sie den Installationsdatenträger DVD 2 in Ihr Laufwerk auf dem CA Business Intelligence-Server ein. Wenn das Installationsmenü nicht automatisch angezeigt wird, starten Sie die Installation durch einen Doppelklick auf die Datei "setup.exe", die sich im Stammverzeichnis des Installationsdatenträgers befindet.

Hinweis: Falls Ihr Computer nicht über ein für den Installationsdatenträger geeignetes Laufwerk verfügt, können Sie den Medieninhalt auf den Computer kopieren, auf dem Sie CA Business Intelligence installieren möchten. Starten Sie dann die Konfiguration. Bei einer Remote-Konfiguration über das Netzwerk können Sie ein Laufwerk bzw. einen Netzwerkordner freigeben und dann zum Starten der Konfiguration die Verbindung herstellen.

2. Wählen Sie die gewünschte Sprache aus der Liste aus, und klicken Sie auf "Sprache auswählen".

Das Installationsmenü wird angezeigt.

3. Klicken auf Sie die Registerkarte "Produktinstallationen".

4. Klicken Sie auf "CA Business Intelligence-Konfiguration".
5. Füllen Sie auf der Seite CA Business Intelligence-Konfiguration die folgenden Felder aus:

BI-Administratoranwendername

Gibt den Namen eines CA Business Intelligence-Anwenders an, der der Administratorgruppe angehört. Bei einer Neuinstallation von CA Business Intelligence lautet der Anwendername "Administrator".

BI-Administratorkennwort

Gibt das Kennwort für den CA Business Intelligence-Administrator an.

Service Desk-Administratoranwendername

Gibt den Anwendernamen für den CA SDM-Administrator an.

Service Desk - Administratorkennwort

Gibt das Kennwort für den berechtigten CA SDM-Anwender an.

Standardanwender erstellen

Erstellt Standardgruppen und entsprechende Anwender in CA Business Intelligence.

Wenn Sie CA Business Intelligence auf einem anderen Rechner als CA SDM installiert haben, werden in der CA Business Intelligence-Konfiguration die folgenden Felder angezeigt:

Primär-Host von Service Desk

Geben Sie abhängig von Ihrer Konfiguration den Hostnamen des CA SDM-Servers an:

- Konventionell: Primärserver.
- Erweiterte Verfügbarkeit: Anwendungsserver.

ODBC-Port

Gibt die Portnummer des CA SDM-ODBC-Treibers an.

Empfohlen: 19987.

ODBC-Installationsverzeichnis

Gibt den anwenderdefinierten Speicherort für die ODBC-Installation an, wenn sich der Speicherort vom Standardspeicherort unterscheidet.

6. Überprüfen Sie die CA Business Intelligence-Konfiguration.

Konfigurieren der Failover-Einstellungen

Dieser Prozess ist nur für die Konfiguration für erweiterte Verfügbarkeit anwendbar. Sie können Failover-Einstellungen konfigurieren, wenn mehrere Anwendungsserver konfiguriert sind. Sie konfigurieren Failover, um aktive Anwendersitzungen an den anderen Anwendungsserver umzuleiten. Sie können den Lastenausgleich auch zwischen mehreren Anwendungsservern konfigurieren.

Gehen Sie wie folgt vor:

1. Rufen Sie die Eingabeaufforderung als Administrator auf.
2. Führen Sie "odbcad32.exe" vom Speicherort "C:\Windows\SysWOW64" auf dem CA Business Intelligence-Server aus.

Das Dialogfeld "DataDirect OpenAccess SDK ODBC Driver Setup" wird angezeigt.

Hinweis: Der angegebene Pfad ist für eine Windows-64-Bit-Installation gültig.

3. Geben Sie die Anwendungsserverdetails in die Registerkarte "Allgemein" ein.
4. Geben Sie die alternativen Anwendungsserverdetails auf der Registerkarte "Failover" mit folgender Syntax ein:

(Host=AppServer1:Port=19987,Host=AppServer2:Port=19987,...)

5. Wählen Sie Lastenausgleich aus, um die Last auf die Server zu verteilen. Die Last wird zwischen den Servern verteilt, deren Details auf der Registerkarte "Allgemein" angegeben sind, und den Servern, deren Details auf der Registerkarte "Failover" angegeben sind. Die Server werden nach dem Zufallsprinzip ausgewählt.

Hinweis: Wählen Sie das Erzwingen von "SQL_DRIVER_NOPROMPT" für Failover oder die Konfiguration für den Lastenausgleich aus.

6. Klicken Sie auf "Übernehmen" und anschließend auf "OK".

Sie haben die Post-Konfigurationseinstellungen für die erweiterte Verfügbarkeit konfiguriert.

Konfigurieren der Werte für den Datumsbereich und die Join-Parameter

Führen Sie nach der Installation von CA Business Intelligence folgende Schritte aus:

- Konfigurieren Sie die Datumsbereichswerte, damit die Datumsbereichsfilter in CA Business Intelligence richtig funktionieren.
- Konfigurieren Sie die Verknüpfungparameter so, dass Universums-Inklusionsverknüpfungen unterstützt werden.

Gehen Sie wie folgt vor:

1. Navigieren Sie auf dem Computer, auf dem CA Business Intelligence installiert wurde, zum folgenden Speicherort:

```
C:\Programme\CA\SC\CommonReporting3\BusinessObjects-Unternehmen  
12,0\win32_x86\dataAccess\connectionServer\odbc\
```

2. Öffnen Sie die Datei "odbc.prm" in einem Texteditor, navigieren Sie zum Abschnitt <Configuration>, und suchen Sie die folgende Zeile, um die Werte des Datumsbereichs zu konfigurieren:

```
<Parameter Name="USER_INPUT_DATE_FORMAT">{\d 'yyyy-mm-dd'}</Parameter>
```

3. Fügen Sie der Zeile wie im folgenden Beispiel dargestellt "hh:mm:ss am/pm" hinzu:

```
<Parameter Name="USER_INPUT_DATE_FORMAT">{\d 'yyyy-mm-dd HH:mm:ss  
am/pm'}</Parameter>
```

4. Suchen Sie die folgende Zeile, um die Join-Parameter zu konfigurieren:

```
<Parameter Name="EXT_JOIN">NO</Parameter>
```

5. Ändern Sie die Zeile, um NO durch YES zu ersetzen, wie im Folgenden dargestellt:

```
<Parameter Name="EXT_JOIN">YES</Parameter>
```

6. Suchen Sie die folgende Zeile:

```
<Parameter Name="OUTERJOINS_GENERATION">NO</Parameter>
```

7. Ändern Sie die Zeile, um NEIN durch FULL_ODBC zu ersetzen, wie im Folgenden dargestellt:

```
<Parameter Name="OUTERJOINS_GENERATION">FULL_ODBC</Parameter>
```

8. Fügen Sie die folgenden drei Zeilen nach dem Parameter "OUTERJOINS_GENERATION" hinzu:

```
<Parameter Name="LEFT_OUTER"></Parameter> <Parameter  
Name="RIGHT_OUTER"></Parameter> <Parameter  
Name="OUTERJOINS_COMPLEX">Y</Parameter>
```

9. Speichern Sie die Datei "odbc.prm".

10. Starten Sie die Business Objects Enterprise-Dienste neu.

Die Datumsbereichswerte und Verknüpfungparameter sind jetzt richtig konfiguriert. Datumsbereichsfilter funktionieren zusammen mit CA Business Intelligence, und Universums-Inklusionsverknüpfungen werden unterstützt.

Hinzufügen Ihrer CA SDM-Anwender zu CMC

CMC ist ein Verwaltungsdienstprogramm, mit dem Sie den Anwenderzugriff auf InfoView und andere BusinessObjects-Anwendungen steuern können. Mit CMC können Sie Ordern und Dokumenten Sicherheits- und Anwenderzugriffsrechte zuweisen.

Hinweis: Während der Konfigurationsphase können Sie über optionales Kontrollkästchen auswählen, ob der CMC Musteranwender hinzugefügt werden. Wenn Sie dieses Kontrollkästchen aktivieren, enthält Ihre CMC mehrere Beispielanwender. Sie können diese Muster als Modelle bei der Definition von Anwenderberechtigungen und Authentifizierungsoptionen für Ihre Berichterstellungsumgebung verwenden. Weitere Informationen über Beispielanwender finden Sie im *Administrationshandbuch*.

Gehen Sie wie folgt vor:

1. Wählen Sie auf dem CA Business Intelligence-Server vom Startmenü die Option "BusinessObjects XI Release 3.1", "BusinessObjects Enterprise", "BusinessObjects Enterprise Central Management Console" aus.
Die Seite "CMC-Management-Konsole" wird geöffnet.
2. Geben Sie Anwendernamen und Kennwort des privilegierten Anwenders ein.
3. Wählen Sie in der Liste "Authentifizierungstyp" "Enterprise" aus.
4. Klicken Sie auf "Anmelden".
Die Startseite von CMC wird geöffnet.
5. Klicken Sie auf der CMC-Startseite im Abschnitt "Organize" (Organisieren) auf "Users and Groups" (Anwender und Gruppen).
6. Klicken Sie auf "Manage" (Verwalten) > "New" (Neu) > "New User" (Neuer Anwender).
Das Dialogfeld "New User" (Neuer Anwender) wird geöffnet.
7. Wählen Sie "Enterprise" (Unternehmen) in der Liste "Authentication Type" (Authentifizierungstyp) aus.
8. Geben Sie unter "Account Name" (Kontonamen) die CA SDM Anwenderkennung an.
9. Geben Sie auf der Registerkarte "Properties" (Eigenschaften) Ihre Kennwortdaten und -einstellungen folgendermaßen an:

Kennwort

Geben Sie das Kennwort ein, und bestätigen Sie es. Dieses Kennwort muss mit dem Kennwort des CA SDM-Anwenders übereinstimmen. Die maximale Kennwortlänge beträgt 64 Zeichen.

Dieses Kennwort muss Groß- und Kleinbuchstaben enthalten, mindestens sechs Zeichen lang sein und darf das Wort "Administrator" in keiner Form enthalten. Es sollte auch mindestens zwei der folgenden Zeichentypen enthalten:

- Uppercase
- Lowercase
- Numerisch
- Zeichensetzung

Kennwort läuft nie ab

Aktivieren Sie das Kontrollkästchen.

Der Anwender muss das Kennwort bei der nächsten Anmeldung ändern

Dieses Kontrollkästchen ist standardmäßig aktiviert. Wenn Sie Anwender nicht zwingen wollen, das Kennwort bei der ersten Anmeldung zu ändern, deaktivieren Sie das Kontrollkästchen.

10. Um den Datenzugriff für Berichte mit Datenpartitions- und Mandantenfähigkeitsbeschränkungen einzuschränken, aktivieren Sie das Kontrollkästchen "Enable Data Source Credentials for Business Objects Universes" (Datenquelle-Anmeldeinformationen für Business Objects Universes). Geben Sie in den angezeigten Feldern den Kontonamen und das Kennwort des CA SDM-Anwenders ein, und bestätigen Sie dann das Kennwort.
11. Klicken Sie auf die "Actions, Members Of" (Aktionen und die Mitglieder), um die Anwender den Gruppen zuzuordnen.
12. Klicken Sie auf "Join Group" (Zur Gruppe hinzufügen), um die verfügbaren Gruppen anzuzeigen. Standardmäßig gehört der Anwender der Gruppe "Alle" an.
13. Wählen Sie im "Available groups" (Verfügbare Gruppen) eine oder mehrere zusätzliche Gruppen aus.
14. Klicken Sie auf den Pfeil ">", um die Gruppe(n) hinzuzufügen.
15. Klicken Sie auf "OK".

Das Dialogfeld "Members Of" (Mitglieder von) wird angezeigt und listet die Gruppen auf, bei denen der Anwender Mitglied ist.

Hinweis: Weitere Informationen über das Hinzufügen von Anwendern und Gruppen sowie über das Konfigurieren von Datenpartitionen finden Sie im *Administrationshandbuch*.

Hinzufügen des privilegierten CA SDM-Anwenders zu CMC

Die Verbindung für CA SDM-Universum ist standardmäßig so konfiguriert, dass beim Zugriff auf Daten der Benutzernamen und das Kennwort von CA SDM verwendet wird. Dieses Anwenderkonto wird in CMC als neuer CA Business Intelligence-Anwender hinzugefügt. Sie benötigen diesen Anwender, wenn Sie für die Berichtserstellung Datenpartitionssicherheit einrichten und Berichte über die Registerkarte "Berichte" testen wollen. Für die Registerkarte "Berichte" muss der Anwender sowohl in CA SDM als auch in CA Business Intelligence definiert sein.

Gehen Sie wie folgt vor:

1. Klicken Sie auf den Bereich zur Verwaltung von Anwendern und Gruppen in der CMC.
2. Wählen Sie unter "Account Name" (Kontoname) das Konto des berechtigten CA SDM-Anwenders aus.
3. Geben Sie auf der Registerkarte "Properties" (Eigenschaften) Ihre Kennwortinformationen an.
4. Aktivieren Sie das Kontrollkästchen "Enable Data Source Credentials for Business Objects Universes" (Datenquelle-Anmeldeinformationen für BusinessObjects-Universen aktivieren). Geben Sie in den angezeigten Feldern den Kontonamen und das Kennwort des privilegierten Anwenders ein, und bestätigen Sie das Kennwort.
5. Klicken Sie auf die Registerkarte "Members Of" (Mitglieder von), um die Gruppe der berechtigten Anwender anzugeben.
6. Klicken Sie auf "Join Group" (Zur Gruppe hinzufügen), um die verfügbaren Gruppen anzuzeigen.
7. Wählen Sie im Bereich der verfügbaren Gruppen die Gruppen "Administrators" (Administratoren) und "CA Universe Developer" (CA-Universum-Entwickler) aus.
8. Klicken Sie auf den >-Pfeil, um diese Gruppen hinzuzufügen.
9. Klicken Sie auf "OK".

Die Registerkarte "Member Of" (Mitglied von) wird angezeigt und führt die Gruppen auf, bei der Anwender Mitglied ist.

Ändern der maximalen Größe für eine Werteliste in CA Business Intelligence

Wenn Sie CA Business Intelligence installieren, wird die maximale Anzahl der Werte, die in einem Batch für eine Werteliste in Crystal Reports zurückgegeben werden, automatisch auf 5.000 Datensätze von der Datenbank gesetzt. Um bessere Leistungen zu erzielen, können Sie die Größe ändern, so dass Wertelisten dieser Größe oder kleinere Wertelisten in mehreren Batches an den Anwender zurückgegeben werden.

Hinweis: Informationen zur Leistungsoptimierung des Web Intelligence Report Server finden Sie in der Dokumentation zu BusinessObjects.

Gehen Sie wie folgt vor:

1. Erstellen Sie folgenden Registrierungsschlüssel:

HKEY_CURRENT_USER\SOFTWARE\Business Objects\Suite
12.0\CrystalReports\DatabaseOptions\LOV

Hinweis: Der erstellte Registrierungsschlüssel überschreibt die Einstellungen des Registrierungsschlüssels "HKEY_LOCAL_MACHINE\SOFTWARE\Business Objects\Suite 12.0\CrystalReports\DatabaseOptions\LOV".

2. Fügen Sie einen Zeichenfolgenwert als "MaxRowsetRecords" hinzu.
3. Legen Sie den Wert von "MaxRowsetRecords" auf die maximale Anzahl der Werte fest, die Sie für den Bericht haben möchten. Zum Beispiel gibt der Wert "2000" bis zu 2000 Werte in der niedrigsten Ebene eines Überlappungsparameters an.

Hinweis: Der Wert null (Unbegrenzt) funktioniert nicht mit BusinessObjects Enterprise oder Crystal Reports Server. Immer wenn auf Crystal Reports von InfoView zugegriffen wird, dauert es bei Auswahl von null länger, die Liste zu füllen, da die maximale Anzahl an Listenwerten abgerufen wird.

4. Starten Sie den betroffenen Service oder die betroffene Anwendung gegebenenfalls neu.

Hinweis: Diese Registrierungsschlüssel wirken sich nicht auf die Werteliste aus, die zurückgegeben wird, wenn ein Bericht auf einem Universe basiert.

Ändern der maximalen Größe für eine Werteliste in Web Intelligence-Berichten

Wenn Sie CA Business Intelligence installieren, wird die maximale Anzahl der Werte, die in einem Batch für eine Werteliste in Web Intelligence-Berichten zurückgegeben werden, automatisch auf 5.000 Datensätze von der Datenbank gesetzt. Um bessere Leistungen zu erzielen, können Sie die Größe ändern, so dass Wertelisten dieser Größe oder kleinere Wertelisten in mehreren Batches an den Anwender zurückgegeben werden.

Hinweis: Informationen zur Leistungsoptimierung des Web Intelligence Report Server finden Sie in der Dokumentation zu BusinessObjects.

Gehen Sie wie folgt vor:

1. Melden Sie sich in der "Central Management Console" an.
2. Klicken Sie auf "Servers".
3. Klicken Sie mit der rechten Maustaste auf "Web Intelligence Processing Server", und klicken Sie auf "Properties".

4. Erhöhen Sie den Wert von "Maximum List Of Values Size (entries)".
5. Speichern und starten Sie "Web Intelligence Processing Server" neu.

Hinweis: Wenn Sie eine große Anzahl von "Maximum List Of Values Size (entries)" festlegen, kann dies Auswirkungen auf die Leistung von Web Intelligence haben. Es wird empfohlen, die angemessene Anzahl entsprechend der Systemleistung festzulegen.

Ändern der Berichtsdatensatzgrenzen

Wenn Sie CA Business Intelligence installieren, wird die Anzahl der Datensätze, die der Server von der Datenbank abrufen, wenn ein Anwender eine Abfrage oder einen Bericht in Crystal Reports ausführt, automatisch auf 20.000 Datensätze gesetzt. Diese Einstellung können Sie so ändern, dass Anwender beim Ausführen von Berichten die erwartete Anzahl an Datensätzen erhalten.

Hinweis: Vollständige Informationen über Verwaltungsaufgaben für den Crystal Reports Page Server finden Sie in Ihrer BusinessObjects-Dokumentation.

Gehen Sie wie folgt vor:

1. Melden Sie sich über BusinessObjects Enterprise bei der Central Management Console an.
2. Navigieren Sie zu der Seite, auf der die Server angezeigt werden.
3. Klicken Sie auf "Crystal Reports Page Server".
4. Ändern Sie auf der Registerkarte "Eigenschaften" die Einstellungen für das Feld "Database Records To Read When Previewing or Refreshing a Report" auf unbegrenzte Datensätze, oder legen Sie eine konkrete Datensatzgrenze fest.
5. Klicken Sie auf "Anwenden".
6. Starten Sie den Crystal Report Page Server neu.

Der Grenzwert für die Berichtsdatensätze wird geändert und bei der Ausführung der Berichte angewendet.

Ändern des Web Intelligence-Sitzungs-Zeitlimits

Anwender verfügen standardmäßig über einen vollständigen Steuerungszugriff auf die Anwendung Web Intelligence.

Die Anwendung "Web Intelligence" verfügt standardmäßig über ein Sitzungs-Zeitlimit von 20 Minuten. Ungespeicherte Berichte gehen verloren, wenn das Sitzungs-Zeitlimit überschritten wird, und der Anwender muss sich wieder anmelden, um die Anwendung nutzen zu können.

Administratoren können den Sitzungszeitlimitwert über die zentrale Verwaltungskonsole (CMC) ändern.

Gehen Sie wie folgt vor:

1. Wählen Sie auf der CMC-Startseite "Server" aus.
Das Fenster "Server" wird geöffnet.
2. Wählen Sie in der Spalte "Servername" "Web_IntelligenceReportServer".
3. Geben Sie den geeigneten Zeitlimitwert (in Minuten) im Feld "Zeitlimit für Verbindung" ein.
4. Klicken Sie auf "Anwenden".
Ihre Änderungen treten in Kraft, nachdem der Server neu gestartet wurde.
5. Klicken Sie auf "OK".
Der Sitzungszeitlimitwert wird festgelegt.

Standardeinstellungen in CMC

Berichte werden während der CA Business Intelligence-Installation größtenteils unbemerkt konfiguriert. Die Berichterstellungskonfiguration enthält folgende Aktionen:

- Einrichten der Sicherheit
- Bereitstellen von Berichten
- Bereitstellen von Universes
- Bereitstellen von Programmobjekten
- Konfigurieren der Web Intelligence-Einstellungen

Der Administrator kann sich bei der BusinessObjects-CMC anmelden und die Standardeinstellungen jederzeit ändern. Die Zugriffsrechte der Anwender entsprechen der CA SDM-Gruppe, der sie angehören.

Hinweis: Weitere Informationen über BusinessObjects CMC, finden Sie im *Implementierungshandbuch zu CA Business Intelligence*.

Integrieren von CA Business Intelligence mit CA SDM

Nachdem Sie CA Business Intelligence installiert haben, aktualisieren Sie die Webberichtsoptionen, damit CA SDM korrekt in CA Business Intelligence integriert wird.

Gehen Sie wie folgt vor:

1. Wählen Sie auf der Registerkarte "Administration" die Option "Optionsmanager" > "Webbericht" aus.
Die Optionsliste wird angezeigt.

2. Legen Sie die Werte für die folgenden Web-Berichtsoptionen fest:

bo_server_auth

Gibt an, welcher Authentifizierungstyp für die Berichterstellung verwendet werden soll. Die folgenden Authentifizierungstypen sind möglich:

- **secEnterprise:** (Standard) Legen Sie die Unternehmens-Authentifizierung fest, wenn Sie unterschiedliche Konten und Gruppen in BusinessObjects für CA Business Intelligence erstellen möchten oder wenn noch keine Anwenderhierarchie in einer Windows NT-Anwenderdatenbank, auf einem LDAP-Server oder einem Windows-AD-Server eingerichtet wurde.

Hinweis: Wenn Sie die Option "secEnterprise" wählen, müssen Sie Ihre [CA SDM-Berichtsanwender](#) (siehe Seite 260) der BusinessObjects Central Management Console (CMC) hinzufügen. In der CMC müssen Sie dieselben Anmeldenamen und Kennwörter eingeben, die in CA SDM konfiguriert sind.

- **secLDAP:** Legen Sie die LDAP-Authentifizierung als Ihren Authentifizierungstyp fest, wenn Sie bereits einen LDAP-Verzeichnisserver eingerichtet haben und nun Ihre LDAP-Anwenderkonten und -gruppen in BusinessObjects für CA Business Intelligence verwenden möchten.

Wenn Sie LDAP-Konten BusinessObjects zuordnen, können die Anwender mit ihrem LDAP-Anmeldernamen und -Kennwort auf CA Business Intelligence zugreifen. Dadurch müssen Sie nicht mehr einzelne Anwender neu erstellen und die Konten in BusinessObjects gruppieren.

- **secWinAD:** Legen Sie die Windows-AD-Authentifizierung fest, wenn Sie in einer Arbeitsumgebung mit Windows 2000 arbeiten und nun Ihre vorhandenen Active Directory-Anwenderkonten und -Gruppen in BusinessObjects für CA Business Intelligence verwenden möchten.
- **secExternal:** Legen Sie die externe Authentifizierung fest, wenn Sie die BusinessObjects-Authentifizierungslösung in eine Authentifizierungslösung eines Drittanbieters integrieren möchten (z. B. JCIFS in Tomcat). Dieser Authentifizierungstyp erfordert die Einrichtung der vertrauenswürdigen Authentifizierung in BusinessObjects, damit die Anwender sich ohne ihr Kennwort anmelden können.

Hinweis: Weitere Informationen zu alternativen Sicherheitsoptionen finden Sie im *CA Business Intelligence-Implementierungshandbuch*.

bo_server_cms

Geben Sie den Namen des CMS (Central Management Server) an, auf dem eine Datenbank mit Informationen zu den BusinessObjects gepflegt wird, die Sie in CA Business Intelligence verwenden.

Geben Sie unter bo_hostname den Hostnamen des Computers an, auf dem CA Business Intelligence installiert ist. Der Standardwert für "bo_cms_port" lautet 6400.

Hinweis: Weitere Informationen zu erweiterten Optionen für die Serverkonfiguration finden Sie im *Installationshandbuch für CA Business Intelligence*.

bo_server_location

Gibt den Hostnamen des Computers an, auf dem CA Business Intelligence installiert ist. Geben Sie "bo_hostname" an. CA SDM verwendet diese URL für Berichts-URLs, um die Berichte vom BusinessObjects-Server anzufordern. Der CMS-Speicherort wird durch den Hostnamen und den Port bestimmt.

Hinweis: Ausführliche Informationen zu jeder Option finden Sie im *Implementierungshandbuch zu CA Business Intelligence*.

3. Klicken Sie auf "Speichern" und dann auf "Aktualisieren".

Die Seite "Optionen – Detail" wird gemäß Ihrer Auswahl aktualisiert.

4. Klicken Sie auf "Fenster schließen".
5. Beenden Sie den Dienst mit der Bezeichnung "CA SDM-Server", und starten Sie diesen Dienst neu.

Die Web Reporting-Einstellungen sind nun für die Zusammenarbeit mit CA SDM konfiguriert. Sie können jetzt die webbasierten Berichte einrichten.

Hinweis: Informationen zum Einrichten von webbasierten Berichten finden Sie im *Administrationshandbuch*.

Konfigurieren der vertrauenswürdigen Authentifizierung für CA SDM und BusinessObjects

Die vertrauenswürdige Authentifizierung bietet eine einfache Art der Anmeldung (Single Sign On) bei der Integration von CA SDM und CA Business Intelligence. Mit "Single Sign On" können sich Anwender beim System anmelden, wobei sie ihr Kennwort nur einmal eingeben müssen.

Gehen Sie wie folgt vor:

1. Installieren und konfigurieren Sie CA SDM.
2. Installieren und konfigurieren Sie CA Business Intelligence.

3. Melden Sie sich bei CMC als Administrator an.
4. Greifen Sie auf die Central Management Console (CMC) zu, um die vertrauenswürdige Authentifizierung einzurichten.
5. Erstellen Sie CA SDM-Kontakte und BusinessObject-Anwender.
6. Installieren Sie die CA SDM-Webberichtsoptionen, und legen Sie die Option `bo_server_auth` auf "Unternehmen" fest.

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

7. Starten Sie den BusinessObjects-Apache Tomcat.
8. Anschließend starten Sie den CA SDM-Server in den Windows-Diensten erneut.

Konfigurieren der vertrauenswürdigen Authentifizierung in CA Business Intelligence

Konfigurieren Sie vertrauenswürdige Authentifizierung für CA Business Intelligence, indem Sie zunächst die Datei "`web.xml`" bearbeiten.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei CMC als Administrator an, und gehen Sie in den Bereich "Authentication management" (Authentifizierungsverwaltung).
Die Seite "Enterprise" (Unternehmen) wird angezeigt.
2. Wählen Sie unten auf der Seite die Option "Trusted Authentication is enabled" (Vertrauenswürdige Authentifizierung ist aktiviert) aus, und geben Sie in das Feld "Shared secret" (Gemeinsamer geheimer Schlüssel) eine Textzeichenfolge ein.

Hinweis: Der gemeinsame geheime Schlüssel wird verwendet, um ein vertrauenswürdiges Authentifizierungskennwort zu erstellen.

3. Geben Sie einen Zeitlimitwert für Ihre Anforderungen an die vertrauenswürdige Authentifizierung ein.

Hinweis: Der Zeitlimitwert bestimmt, wie lange der CMS auf den Aufruf "`EnterpriseSession.logon()`" von der Client-Anwendung wartet.

4. Klicken Sie auf "Update" (Aktualisieren).
Trusted Authentication wird konfiguriert.

Konfigurieren der vertrauenswürdigen Authentifizierung in CA SDM

Für das Konfigurieren der vertrauenswürdigen Authentifizierung in CA SDM ist die Bearbeitung der Datei "TrustedPrincipal.conf" erforderlich.

Gehen Sie wie folgt vor:

1. Öffnen Sie die Datei "TrustedPrincipal.conf" in dem folgenden Verzeichnis:
NX_ROOT\bopcfg\www\CATALINA_BASE\webapps\CAisd
2. Bearbeiten Sie die Zeile
SharedSecret=<Gemeinsamer geheimer Schlüssel wie in CMC eingegeben>
wie folgt:
SharedSecret=xxxx
(wobei xxxx der gemeinsame geheime Schlüssel ist, der in Schritt 3 in CMC eingegeben wurde)
3. Klicken Sie auf "Speichern".
4. Wiederholen Sie die Schritte 1 bis 3 für alle konfigurierten Anwendungsserver.
5. Starten Sie den CA Business Intelligence-Tomcat-Server neu.
Die vertrauenswürdige Authentifizierung in CA SDM wird konfiguriert.

Hinweis: Sie müssen die vertrauenswürdige Authentifizierung im CA SDM-Hintergrundserver konfigurieren, um Berichte über die URL des Hintergrundservers zu starten.

Konfigurieren der BusinessObjects-LDAP-Authentifizierung

Beim Konfigurieren der LDAP-Authentifizierung muss der Wert "cn" der LDAP-Server-Anmeldeinformationen des Administrators einem vollqualifizierten Namen (Vorname, Nachname) entsprechen. Die Konfiguration der LDAP-Authentifizierung ermöglicht es Ihnen, die LDAP-Attribute für die Verwendung des Anmeldenamen des Endanwenders zuzuordnen.

Wichtig! Der Name des Anwenderkontos für BusinessObjects muss mit der Anwender-ID des CA SDM-Kontakts übereinstimmen, wenn LDAP-Authentifizierung konfiguriert wird.

Gehen Sie wie folgt vor:

1. Greifen Sie in der zentralen Verwaltungskonsole (CMC) auf den Bereich "Authentifizierungsverwaltung" zu.
2. Doppelklicken Sie auf "LDAP".

3. Geben Sie in das Feld "Add LDAP host" (LDAP-Host hinzufügen) den Namen und die Portnummer Ihrer LDAP-Hosts ein (Hostname:Port). Beispiel: "myserver:123".
4. Klicken Sie auf "Add" (Hinzufügen) und dann auf "OK".
5. Wählen Sie in der Liste "LDAP Server Type" (LDAP-Servertyp) den Servertyp "Custom" (Anwenderspezifisch) aus.
6. Befolgen Sie die Eingabeaufforderungen im CMS-Konfigurations-Assistenten, und stellen Sie die Konfiguration fertig.

BusinessObjects-LDAP-Authentifizierung wird konfiguriert.

Hinweis: Weitere Informationen zum Konfigurieren von LDAP-Authentifizierung finden Sie in der *CMS-Online-Hilfe* und dem *Administratorhandbuch für BusinessObjects Enterprise*.

Verbinden des CA Business Intelligence-Servers mit einem anderen CA SDM-Server

Dies ist erforderlich, um Berichte von einer weiteren CA SDM-Instanz zu generieren, die auf einem anderen Server installiert ist.

Gehen Sie wie folgt vor:

1. [Erstellen Sie einen ODBC-DSN für den CA SDM-Server](#) (siehe Seite 270).
2. [Verbinden Sie das CA SDM-Universum mit diesem CA SDM-Server](#) (siehe Seite 271).

Erstellen einer ODBC-DSN für den CA SDM-Server

Mit dem ODBC-Datenquellenadministrator können Sie einen ODBC DSN erstellen.

Gehen Sie wie folgt vor:

1. Starten Sie den Windows ODBC-Datenquellenadministrator (Datenquellen (ODBC)).
2. Wählen Sie im Formular "ODBC DataSource Administrator" die Registerkarte "System-DSN" aus, und wählen Sie "Hinzufügen".
3. Wählen Sie im Formular "Neue Datenquelle erstellen" den DataDirect OpenAccess-Treiber, und wählen Sie "Fertig stellen".
4. Weisen Sie im Formular "DataDirect OpenAccess ODBC 32 Setup" einen ODBC-Namen zu, und wählen Sie "Erweitert".

Die zu verwendende Benennungskonvention lautet "casd_hostname". Wenn der Hostname des CA SDM-Servers zum Beispiel "MyServer" lautet, würden Sie "casd_MyServer" verwenden.

5. Wählen Sie im Formular "OpenAccess Database Configuration" "Hinzufügen" aus.
6. Geben Sie im Formular "OpenAccess Database Setup" die folgenden Informationen ein:
 - Name: Geben Sie "casd_hostname" ein.
 - IP-Adresse: Geben Sie die IP-Adresse des CA SDM-Servers ein.
 - Port: Geben Sie 19987 an.
 - Typ: Wählen Sie "SQL" aus.
7. Klicken Sie auf "OK".
8. Wählen Sie im Formular "OpenAccess Database Configuration" "OK" aus.
9. Wählen Sie im Formular "DataDirect OpenAccess ODBC 32 Setup" aus dem Dropdown-Menü "Datenbank" die Option "casd_hostname" und anschließend "OK" aus.

Die ODBC-DSN ist nun erstellt.

Verbinden des CA SDM-Universes mit dem Server

Die Verbindung können Sie mit dem Designer in BusinessObjects Enterprise aufbauen.

Gehen Sie wie folgt vor:

1. Wählen Sie im Startmenü "BusinessObjects XI Release 3.1" > "BusinessObjects Enterprise" > "Designer" aus.
2. Melden Sie sich beim Designer mit den folgenden Anmeldeinformationen an.
 - System: Gibt den Hostnamen des Servers an, auf dem CA Business Intelligence installiert ist.
 - Anwendername: Gibt den Namen des Administrators für CA Business Intelligence an (i. d. R. Administrator).
 - Kennwort: Gibt das Kennwort des Administrators für CA Business Intelligence an.
 - Authentifizierung: Wählen Sie "Unternehmen".

Das Fenster "Designer" wird angezeigt.

3. Klicken Sie auf "Datei" > "Importieren".

Das Dialogfeld "Universe importieren" wird angezeigt.
4. Wählen Sie den Ordner "CA-Universes" aus der Dropdown-Liste aus, wählen Sie dann das CA SDM-Universum, und klicken Sie auf "OK".

Hinweis: Wenn dies das erste Mal ist, dass Sie Designer verwenden, kann es sein, dass Sie zunächst "Durchsuchen" auswählen müssen, um den Ordner "CA Universes" auszuwählen.

5. Klicken Sie im Meldungsfenster "Universum wurde erfolgreich importiert" auf "OK".
Das Universe-Fenster wird angezeigt.
6. Wählen Sie "Datei" > "Parameter" aus.
Das Dialogfeld "Universe-Parameter" wird angezeigt.
7. Klicken Sie auf der Registerkarte "Definition" auf "Bearbeiten".
Das Dialogfeld "Anmeldeparameter" wird angezeigt.
8. Wählen Sie "Bearbeiten".
9. Wählen Sie den zuvor erstellten ODBC DSN (casd_hostname) aus der Dropdown-Liste mit den Datenquellen aus, und geben Sie den Anwendernamen und das Kennwort des berechtigten CA SDM-Anwenders ein.
10. Klicken Sie auf "Weiter" > "Verbindungstest", und gehen Sie durch die angezeigten Dialogfelder "Universe-Verbindung".
11. Klicken Sie auf "OK", um den Vorgang zu beenden.
12. Wählen Sie "Datei" > "Exportieren" aus.
Das Dialogfeld "Universe exportieren" wird angezeigt.
13. Wählen Sie in der Dropdown-Liste "Domäne" den Eintrag "CA Universes" aus.
14. Wählen Sie in der Liste der Gruppen die Option "Jeder".
15. Klicken Sie auf "OK".
Das Universum wird exportiert und die Verbindung mit dem Server ist hergestellt.

Replizierte Datenbank für Offline-Berichterstellung

Um potenziellen Leistungsproblemen vorzubeugen, die sich auf die mit CA SDM installierten Berichtskomponenten auswirken könnten, können Sie eine replizierte Datenbank für Offline-Berichterstellungszwecke erstellen.

Hinweis: Weitere Informationen zum Erstellen einer replizierten Datenbank für Offline-Berichterstellung finden Sie in der Beispieldokumentation und den Skripts im Verzeichnis "NX_ROOT\samples\reporting".

Überprüfen der Berichte

Um sicherzustellen, dass die Berichte problemlos generiert wurden, überprüfen Sie die CA Business Intelligence-Konfiguration.

Gehen Sie wie folgt vor:

1. Klicken Sie auf die Registerkarte "Berichte".
Die Seite "Webbericht" wird geöffnet.
2. Klicken Sie auf "InfoView".
Das Fenster "Business Objects InfoView" wird geöffnet.
3. Klicken Sie auf die Verknüpfung "Liste der Dokumente".
4. Blenden Sie "Public Folders", "CA Reports", "CA Service Desk" ein.
5. Wählen Sie den Ordner "Asset" im linken Bereich aus.
6. Doppelklicken Sie auf den Bericht "Asset-Liste".

Der Bericht zeigt null oder mehrere gefundene Ergebnisse an. CA Business Intelligence ist jetzt für CA SDM konfiguriert.

So konfigurieren Sie integrierte Windows-Authentifizierung für CA SDM

Als Systemadministrator können Sie die CA SDM-Anwender über eine vorhandene externe Authentifizierungsmethode authentifizieren. Dieses Szenario beschreibt den Prozess zur Verwendung der integrierten Windows-Authentifizierung (IWA), um CA SDM-Anwender über Microsoft Active Directory (AD) zu authentifizieren. Wenn Sie CA SDM-Zugriffstypen, wie z. B. Administratoren, für die Verwendung von IWA konfigurieren, werden die Anwender der ausgewählten Zugriffstypen direkt über AD authentifiziert.

Folgendes Diagramm zeigt, wie Sie IWA für CA SDM konfigurieren können:



Um IWA für CA SDM zu konfigurieren, gehen Sie folgendermaßen vor:

1. [Überprüfen der Voraussetzungen](#) (siehe Seite 275)
2. [Konfigurieren von Internet Information Services \(IIS\) für IWA](#). (siehe Seite 276)
3. [Konfigurieren von CA SDM für IWA](#). (siehe Seite 277)

4. [Testen von IWA](#) (siehe Seite 277)

Überprüfen der Voraussetzungen

Überprüfen Sie folgende Anforderungen, bevor Sie die externe Authentifizierung für CA SDM konfigurieren:

- Sie haben Server für CA SDM konfiguriert.
- Sie haben abhängig von Ihrer Konfiguration IIS 7.0 auf folgendem Server installiert:
 - Konventionelle Konfiguration: Primärserver.
 - Erweiterte Verfügbarkeit: Anwendungsserver.
- Sie haben CA SDM für die Verwendung von IIS 7.0 konfiguriert.
- Sie haben die Liste der Zugriffstypen, für die die externe Authentifizierung erforderlich ist. Zum Beispiel: "CMDB-Administrator", "Mitarbeiter" und "CMDB-Anwender".

Konfigurieren von IIS für IWA

Sie konfigurieren den IIS-Server, um IWA zu aktivieren. Die Konfiguration ändert den Authentifizierungsmodus von IIS von "Anonym" in "Windows-Authentifizierung". Nach der Konfiguration leitet der Server Authentifizierungs-Requests zur externen Quelle um.

Gehen Sie wie folgt vor:

1. Melden Sie sich abhängig von Ihrer Konfiguration bei folgendem Server als Administrator an:
 - Konventionell: Primärserver oder Sekundärserver.
 - Erweiterte Verfügbarkeit: Hintergrundserver.
2. Öffnen Sie in der Verwaltung den Internetinformationsdienste-Manager.
3. Blenden Sie den Knoten "Servername" ein, wobei "Servername" der Name des CA SDM-Servers ist.
4. Blenden Sie die Knoten "Standorte", "Standardwebsite", "CAisd" ein.
Die Startseite von CAisd wird geöffnet.
5. Doppelklicken Sie auf das Symbol "Authentifizierung".
Die Seite "Authentifizierungseinstellungen" wird geöffnet.
6. Deaktivieren Sie die anonyme Authentifizierung, indem Sie auf den vorhandenen Statuswert klicken.
7. Aktivieren Sie die Windows-Authentifizierung, indem Sie auf den vorhandenen Statuswert klicken.
8. Starten Sie IIS neu, um die Änderungen anzuwenden.

Sie haben IIS für IWA konfiguriert.

Konfigurieren von CA SDM für IWA

Sie konfigurieren die IWA für alle ausgewählten Zugriffstypen. Nachdem ein Zugriffstyp für die externe Authentifizierung konfiguriert wurde, werden die Kontakte dieses Zugriffstyps von CA SDM extern authentifiziert.

Gehen Sie folgendermaßen vor:

1. Melden Sie sich bei CA SDM als Systemadministrator an.
2. Wählen Sie auf der Registerkarte "Administration" die Option "Sicherheits- und Rollenmanagement", "Zugriffstypen" aus.
Die Seite "Zugriffstypen - Liste" wird geöffnet.
3. Klicken Sie auf den Zugriffstyp, für den die externe Authentifizierung erforderlich ist.
Das Formular "Zugriffstyp aktualisieren" wird geöffnet.
4. Aktivieren Sie auf der Registerkarte "Webauthentifizierung" das Kontrollkästchen "Externe Authentifizierung zulassen".
5. Wählen Sie einen entsprechenden Wert aus der Dropdown-Liste "Validierungstyp" aus. Für folgende Werte ist eine Beschreibung erforderlich:

Kein Zugriff

Gibt an, dass auf den ausgewählten Zugriffstyp nicht zugegriffen werden darf.

Öffnen

Gibt an, dass der Zugriff für alle offen ist.

OS

Gibt an, dass die Anmeldeinformationen für das Betriebssystem des CA SDM-Servers erforderlich sind, um auf CA SDM zuzugreifen. Wenn Sie EEM konfiguriert haben, wird der Anmelde-Request an den EEM-Server umgeleitet.

PIN

Gibt an, dass der Wert des ausgewählten Felds für den CA SDM-Kontaktdatensatz für die Authentifizierung erforderlich ist. Wenn Sie zum Beispiel "PIN" als Validierungstyp auswählen und "Contact_Number" in der Dropdown-Liste "PIN-Feld" ausgewählt wird, dann wird die Kontaktnummer des Anwenders für die Authentifizierung erforderlich sein.

Hinweis: Der Validierungstyp wird nicht für die IWA-Validierung verwendet, aber der Validierungstyp wird verwendet, wenn sich der Anwender über das CA SDM-Anmeldeformular anmeldet. Die CA SDM-Anmeldungsseite wird nur dann angezeigt, wenn der Anwender auf die Verknüpfung zum Abmelden klickt oder wenn die Anmeldeinformationen nicht mit den IIS-Anmeldeinformationen übereinstimmen.

6. Klicken Sie auf "Speichern".

Um die externe Authentifizierung für andere Zugriffstypen zu konfigurieren, wiederholen Sie die Schritte 1 bis 6.

Testen von IWA

Sie testen die IWA mit einer Anwender-ID, die den entsprechenden Kontaktdatensatz in CA SDM hat. Eine erfolgreiche Anmeldung zeigt an, dass Sie die IWA erfolgreich konfiguriert haben.

Gehen Sie wie folgt vor:

1. Melden Sie sich abhängig von Ihrer Konfiguration bei folgendem Server an. Verwenden Sie dazu eine Anwender-ID, die den entsprechenden Kontaktdatensatz in CA SDM hat:

- Konventionell: Primärserver oder Sekundärserver.
- Erweiterte Verfügbarkeit: Anwendungsserver.

Hinweis: Wenn die LDAP-Optionen im Optionsmanager installiert wurden, können Sie auch neue Kontakte in CA SDM von einem beliebigen Active Directory-Kontakt erstellen.

2. Starten Sie den Browser, und geben Sie die CA SDM-URL ein.
Die Service Desk-Startseite wird geöffnet.

Sie haben die IWA erfolgreich konfiguriert.

Ausführen der Automatisierungsrichtlinien

Die Funktion "Automatisierungsrichtlinien" in Knowledge Management stellt automatisierte Richtlinien bereit, mit denen Sie Knowledge für Ihre Organisation effizienter und effektiver verwalten können. 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.

Die Seite "Automatisierungsrichtlinien - Liste" enthält Details zu den Automatisierungsrichtlinien, die Sie verwalten können. Diese Seite zeigen Sie an, indem Sie auf der Registerkarte "Administration" die Option "Knowledge" > "Automatisierungsrichtlinien" auswählen.

Jede Richtlinie enthält eine gespeicherte Abfrage, die dann ausgeführt wird, wenn während der Verarbeitung übereinstimmende Dokumente gefunden werden. Nach der Verarbeitung wird auf dem CA SDM-Scoreboard ein Bericht zur Lebenszyklusrichtlinie angezeigt. Um einen Bericht anzuzeigen, wählen Sie "Knowledge-Dokumente" > "Automatisierungsrichtlinien". Auf dem Scoreboard können Analysten eigene Dokumente und der Administrator kann alle Dokumente für jede Rolle verwalten.

Um die Berichte zu implementieren, müssen Sie mit dem Automatisierungsrichtlinien-Scheduler einen Batch-Vorgang ausführen. Der Scheduler wird abhängig von der Konfiguration auf folgendem CA SDM-Server ausgeführt, und es werden die Daten angezeigt, die erforderlich sind, um die Berichte anzuzeigen.

- Konventionell: Primärserver oder Sekundärserver
- Erweiterte Verfügbarkeit: Hintergrundserver

Anschließend führen Sie die [Knowledge-Berichtskarte](#) (siehe Seite 279) aus.

So führen Sie den Automatisierungsrichtlinien-Scheduler aus

1. Wählen Sie auf der Registerkarte "Administration" die Option "Knowledge" > "Automatisierungsrichtlinien" > "Ablaufplanung" aus.

Die Seite "Automatisierungsrichtlinien-Scheduler" wird angezeigt.

2. Füllen Sie die folgenden Felder aus:
 - **Letzte Aktualisierung:** Aktivieren Sie das Kontrollkästchen "Berechnung ausführen".
 - **Ablaufplan:** Geben Sie Datum und Uhrzeit für die Berechnung an, zu dem CA SDM die Richtlinie ausführt.
3. Klicken Sie auf "Speichern".

Ausführen der Knowledge-Berichtskarte

Die Knowledge-Berichtskarte zeigt Informationen über den Wissensbeitrag jedes Endanwenders an und gibt an, welche der Knowledge-Dokumente am nützlichsten sind. Sie können diese Informationen verwenden, um die Prozesse für das Erstellen von Knowledge-Dokumenten zu optimieren und um Endanwendern in Ihrer Umgebung den bestmöglichen Support anzubieten.

So führen Sie die Knowledge-Berichtskarte aus:

1. Klicken Sie auf die Registerkarte "Administration".
2. Navigieren Sie zu "Knowledge" > "Knowledge-Berichtskarte".
Die Knowledge-Berichtskarte wird angezeigt.
3. Füllen Sie die folgenden Felder aus, und klicken Sie dann auf "Speichern".
 - **Letzte Aktualisierung:** Aktivieren Sie das Kontrollkästchen "Berechnung ausführen".
 - **Ablaufplan:** Geben Sie Datum und Uhrzeit für die Berechnung an, zu dem CA SDM die Berichtskarte ausführt.

Hinweis: Informationen über die Verwendung von Automatisierungsrichtlinien und die Knowledge-Berichtskarte finden Sie im *Administrationshandbuch*.

Knowledge Management-Beispieldatenimport

Es stehen Ihnen Beispiel-Knowledge-Daten aus Knowledge Broker und Knowledge Accelerators zur Verfügung. Wenn Sie die Beispiel-Knowledge-Daten verwenden möchten, müssen Sie die Daten in die Knowledge Management-Datenbank importieren.

Hinweis: Die Beispieldateien sind nicht lokalisiert. Beim Importieren funktionieren Beispieldaten nicht auf lokalisierten Umgebungen.

Führen Sie für die erweiterte Verfügbarkeit "ImportSampleData.bat" oder "ImportSampleData.sh" vom Hintergrundserver aus.

Installation unter Windows

1. Wechseln Sie in das Verzeichnis "\$NX_ROOT\samples\data" und entpacken die Datei "SampleData.zip" in dasselbe Verzeichnis.
2. Gehen Sie vom Befehlsfenster zu "\$NX_ROOT/bin" und führen Sie "ImportSampleData.bat" aus.

Installation unter UNIX

1. Führen Sie den Befehl "tar -xvf SampleData.tar" im Verzeichnis "\$NX_ROOT/samples/data" aus.
2. Gehen Sie vom Befehlsfenster zu "\$NX_ROOT/bin" und führen Sie "ImportSampleData.sh" aus.

Konfiguration der Such-Engine

Die EBR-Such-Engine wird standardmäßig mit CA SDM installiert.

Hinweis: Weitere Informationen über die Optionen der Such-Engine finden Sie in der *Online-Hilfe*.

"pdm_k_reindex" — Dienstprogramm zur Knowledge-Neuindizierung

Das Hilfsprogramm zur Neuindizierung von Knowledge, "pdm_k_reindex.exe", befindet sich im Installationsverzeichnis von Knowledge Management.

Hinweis: Die Neuindizierung der Dokumente in der Knowledge Base kann in Abhängigkeit von der Größe Ihrer Datenbank ein zeitaufwändiger Vorgang sein. Wir empfehlen, dass Sie das Programm zur Neuindizierung der Knowledge Base ausführen, nachdem alle Änderungen hinzugefügt worden sind. Für die Konfiguration für erweiterte Verfügbarkeit können Sie während des Failovers das Hilfsprogramm zur Neuindizierung der Knowledge nicht ausführen.

Wichtig! Unter UNIX muss "LIBPATH" festgelegt sein, bevor mehrere CA SDM-Hilfsprogramme ausgeführt werden. Verwenden Sie "pdm_task", um "LIBPATH" festzulegen, bevor Sie ein Hilfsprogramm ausführen. Geben Sie zum Beispiel "pdm_task pdm_clean_attachments ..." ein.

Gehen Sie wie folgt vor:

1. Öffnen Sie die Eingabeaufforderung.
2. Geben Sie folgenden Befehl in der Eingabeaufforderung ein, um die Neuindizierung der Knowledge auszuführen:

Beispiel:

```
pdm_k_reindex
```

Folgende Optionen sind mit diesem Befehl verfügbar.

-D

Definiert den Debug-Modus, zum Beispiel Drucken in das Befehlsfenster.

-v

Definiert den Modus "Verbose" (Ausführlich), zum Beispiel Drucken in die Datei "stdlog".

-i

Erstellt keine Tabellenindizes in der Neuindizierungstabelle, nachdem die Neuindizierung durchgeführt wurde.

Hinweis: Parameter mit einem Bindestrich als Präfix, z. B. "-D", müssen anderen Parametern, die dieses Präfix nicht haben, vorausgehen.

Die andere Option ist:

Datei:reindex.txt

Dokumente werden zur angegebenen Datei neu indiziert.

+i

Erstellt nur die Indizes der neu indizierten Tabelle (entspricht der Suchtabelle nach der Neuindizierung). Die alten Indizes werden vor der Neuindizierung entfernt.

+t

Tauscht nur die Namen der Tabellen "search" und "reindex" aus.

Hinweis: Das Präfix "+" kennzeichnet nur diesen Parameter.

sdtout

Definiert, wie häufig die Statistik im Befehlsfenster erscheint. Standardmäßig zeigt das Dienstprogramm zur Knowledge-Neuindizierung jeweils nach 1.000 verarbeiteten Dokumenten Statistiken im Befehlsfenster an. Es kann jedoch vorkommen, dass Statistiken häufiger erforderlich sind. Verwenden Sie den folgenden Parameter:

```
pdm_k_reindex -i sdtout:10
```

In diesem Fall wird im Befehlsfenster die Statistik für alle 10 Dokumente angezeigt.

Die Dokumente werden in der Knowledge Base neu indiziert.

Neue Tags für die Konfiguration eines Domservers für die Crawler-Oberfläche

Wenn CA SDM eine große Datenmenge zu indizieren hat, müssen Sie abhängig von Ihrer CA SDM-Konfiguration einen dedizierten Server für die Crawler-Oberfläche haben, um die Beeinträchtigung der gesamten CA SDM-Umgebung zu minimieren.

- Konventionell: Primärserver oder Sekundärserver
- Erweiterte Verfügbarkeit: Anwendungsserver

Weitere Informationen zur Konfiguration des CA SDM-Servers finden Sie in der *Online-Hilfe der Server-Konfiguration*

Die folgenden zwei neuen Tags wurden in der Datei "crawler_surface_config.xml" eingeführt und betreffen das Indexieren:

- Ein neuer Tag wurde in der Datei "crawler_surface_config.xml" (root\general_configuration\sdm_domsrvr_name) eingeführt, damit der Kunde den Namen einer dedizierten Domserver-Instanz für die Crawler-Oberfläche angeben kann.

Standard: domsrvr

Dieser Wert ist ein standardmäßiger Instanzname eines Domservers (Objektmanager).

- Ein weiterer neuer Tag wurde in der Datei "crawler_surface_config.xml" *sharepoint_properties_file* bei *root\general_configuration* eingeführt, damit der Kunde den Wert editieren und löschen kann, wenn die Crawler-Oberfläche keine CA SDM-Daten für SharePoint indizieren soll.

Standard: sharepoint

Dieser Wert ist der Name der standardmäßig unter NX_ROOT\CATALINA_BASE_FS\lib verfügbaren *sharepoint.properties-Datei*.

So konfigurieren Sie CA Workflow:

Um CA Workflow für die Verwendung mit CA SDM zu konfigurieren, führen Sie die Schritte in diesem Abschnitt aus.

Weitere Informationen:

[Starten und Anhalten von CA Workflow](#) (siehe Seite 284)

[Einrichten der automatischen Anmeldung \(Externe Authentifizierung\)](#) (siehe Seite 288)

[Konfigurieren der Worklist und des Workflow-Managers für die automatische Anmeldung](#) (siehe Seite 289)

[Konfigurieren der Workflow-Entwicklungsumgebung für die automatische Anmeldung](#) (siehe Seite 290)

[CA Workflow-Optionen](#) (siehe Seite 291)

[Konfigurieren des Problem Management-Beispiel-Workflows](#) (siehe Seite 292)

[Konfigurieren des Beispiel-Workflows "PC-Auftrag"](#) (siehe Seite 294)

[Beispiel einer Change-Management-Prozessdefinition](#) (siehe Seite 295)

Starten und Anhalten von CA Workflow

Vor der Installation von CA Workflow müssen Sie zuerst CA SDM-Server installieren und konfigurieren. Der standardmäßige CA SDM-Tomcat wird automatisch durch den CA SDM-Daemon-Manager konfiguriert, gestartet und angehalten. Auch das Befehlszeilendienstprogramm `pdm_tomcat_nxd` kann zum Starten und Anhalten der Tomcat-Instanz verwendet werden.

Gehen Sie wie folgt vor:

1. (Anwendbar nur für die konventionelle Konfiguration) Bestimmte auf dem Sekundärserver zu startende Prozesse konfigurieren.

- a. Führen Sie `pdm_edit` aus (auf dem Primärserver).
- b. Starten Sie den CA SDM-Dienst erneut.

Dadurch werden spezifische Umgebungsvariablen für die Versionskontrolle, die für die Installation und Ausführung von CA Workflow erforderlich sind, auf einen Sekundärserver geleitet.

2. Installieren und konfigurieren Sie abhängig von Ihrer CA SDM-Konfiguration CA Workflow auf dem folgenden Server:
 - Konventionell: Primärserver oder Sekundärserver
 - Erweiterte Verfügbarkeit: Beliebiger Anwendungsserver.
3. Führen Sie `pdm_tomcat_nxd -d start -t CAWF` aus.
CA Workflow wird manuell gestartet.
Hinweis: Führen Sie `pdm_tomcat_nxd -d start -t CAWF` aus, um CA Workflow anzuhalten.
4. Installieren Sie abhängig von Ihrer CA SDM-Konfiguration CAWF-Optionen auf dem folgenden Server:
 - Konventionell: Primärserver
 - Erweiterte Verfügbarkeit: HintergrundserverDadurch wird CA Workflow automatisch gestartet und angehalten und die Kommunikation zwischen CA SDM und CA Workflow ermöglicht.

Weitere Informationen:

[pdm_tomcat_nxd: Starten und Anhalten einer Tomcat-Instanz](#) (siehe Seite 285)

pdm_tomcat_nxd: Starten und Anhalten einer Tomcat-Instanz

Das `pdm_tomcat_nxd`-Dienstprogramm wird als Daemon-Vorgang und als Befehlszeilendienstprogramm ausgeführt. Das Dienstprogramm bietet folgende Möglichkeiten:

- Bearbeitet Anforderungen vom Befehlszeilendienstprogramm, um eine bestimmte Tomcat-Instanz zu starten (START) und anzuhalten (STOP).
- Gibt den Tomcat-STATUS zurück.
- Beendet den Daemon und stoppt die Tomcat-Instanz (EXIT).

Der Daemon bearbeitet auch Anforderungen eines Tomcat "Listener"-Servlets zur Aktualisierung des STATUS der Tomcat-Instanz, wenn diese angehalten oder gestartet wird.

Das Befehlszeilendienstprogramm "pdm_tomcat_nxd" leitet START-, STOP-, STATUS- und EXIT-Anforderungen an einen Tomcat-Daemon weiter, kann aber auch eine bestimmte Tomcat-Instanz direkt, d. h. ohne Tomcat-Daemon, starten und anhalten.

Pdm_tomcat_nxd bietet mehrfache Daemons auf einem CA SDM-Server, wobei jeder Daemon eine bestimmte Tomcat-Instanz verwaltet. Jeder Daemon wird mit einem bestimmten Tomcat- und Servernamen initialisiert, der für die Slump-Adressen von Daemon und "Listener" sowie für das Catalina-Hauptverzeichnis verwendet wird, in dem die Tomcat-Instanz definiert ist. Diese Änderung wird durch einen neuen Parameter für Tomcat-Namen unterstützt.

Mit dem folgenden Befehl starten Sie einen pdm_tomcat_nxd-Daemon. Beim Start des Daemons startet dieser automatisch eine Tomcat-Instanz mit dem angegebenen Tomcat-Namen.

Hinweis: In den folgenden Beispielen ist der standardmäßige Tomcat-Name leer (das bedeutet "ServiceDesk").

```
pdm_tomcat_nxd -s [ -t tomcat ]
```

Beispiel: Eine Anforderung an einen bestimmten Tomcat-Daemon auf einen bestimmten Server senden

Falls es sich um eine STATUS-Anforderung handelt, wird zunächst eine Meldung an den Tomcat-"Listener" gesendet. Erfolgt keine Antwort, wird die Anforderung an den Tomcat-Daemon gesendet. Der Standardservername lautet NX_LOCAL_HOST. Der Tomcat-Standardname ist leer (das bedeutet "ServiceDesk").

```
pdm_tomcat_nxd -c <request> [ -t <tomcat_name> ] [-S <server_name> ]
```

Anforderung

STOP | SHUTDOWN | START | STATUS | EXIT

Beispiel: Einen bestimmten Tomcat auf diesem Server (ohne Tomcat-Daemon) starten oder anhalten

```
pdm_tomcat_nxd -d <request> [ -t <tomcat_name> ]
```

Anforderung

STOP | START

Beispiel: Tomcat-Befehl zum Starten und Anhalten einer Tomcat-Instanz anzeigen

```
pdm_tomcat_nxd -T [ -t <tomcat_name> ]
```

Zu Beginn meldet sich der Daemon beim Slump-Server an und verwendet dabei einen Prozessnamen, der sich aus server_name und Tomcat-Name (falls er nicht leer ist) zusammensetzt. Das Befehlszeilen-Hilfsprogramm verwendet diese Adresse, um dem Deamon Meldungen zu senden. Um STATUS-Anforderungen an den Tomcat-"Listener" zu senden, verwendet das Befehlszeilendienstprogramm den Namen des "Listener"-Vorgangs, der sich ebenfalls aus server_name und tomcat_name (falls es nicht leer ist) zusammensetzt. Der Daemon öffnet auch eine Protokolldatei für die Tomcat-Instanz mit Hilfe eines Dateinamens, in dem der Tomcat-Name (falls er nicht leer ist) enthalten ist. Im folgenden Beispiel werden daemon_name, listener_name und Variablen des Protokolldateinamens angezeigt:

```
daemon_name

    "pdm_tomcat -" +
    server_name
    [+ "-" + tomcat_name] falls tomcat_name nicht leer ist

listener_name = server_name + "-" +
    "container-pdmContextListener"
    [+ "-" + tomcat_name] falls tomcat_name nicht leer ist

tomcat_log = pdm_tomcat +
    "-" + tomcat_name +] falls tomcat_name nicht leer ist
    ".log"
```

Wenn das Befehlszeilen-Hilfsprogramm oder der Daemon-Prozess eine Tomcat-Instanz nicht startet oder anhält, wird unter Verwendung verschiedener NX-Umgebungsvariablen ein Befehl (catalina_cmd) generiert. Alle folgenden Umgebungsvariablen sind erforderlich (mit Ausnahme von NX_JAVA_OPTIONS und NX_TOMCAT_HOTSPOT, die nur auf einem HP-System verwendet werden).

In den Namen der Umgebungsvariablen (für die standardmäßige ServiceDesk-Tomcat-Instanz) ist kein Tomcat-Name enthalten. Dagegen können die Namen von Umgebungsvariablen für alle anderen Tomcat-Instanzen optional auch Tomcat-Namen umfassen. Eine Ausnahme bildet die Variable NX_XXX_CATALINA_BASE, denn hier muss der Tomcat-Name (XXX) angegeben werden. Ist keine Tomcat-spezifische Umgebungsvariable vorhanden, muss der Standardumgebungsvariablenname verwendet werden.

```
CATALINA_BASE | NX_XXX_CATALINA_BASE
NX_TOMCAT_INSTALL_DIR + [ _XXX ]
NX_TOMCAT_INSTALL_DIR + [ _XXX ]
NX_JRE_INSTALL_DIR + [ _XXX ]
NX_JDBC_DRIVER + [ _XXX ]
NX_JAVA_OPTIONS + [ _XXX ]
NX_JDBC_DRIVER_CLASSPATH + [ _XXX ]
NX_TOMCAT_HOTSPOT + [ _XXX ]
```

Einrichten der automatischen Anmeldung (Externe Authentifizierung)

Um den Anmeldeprozess für <WF>-Worklist-Aufgaben beim Arbeiten mit Changes, Requests, Incidents, Problemen und Issues zu automatisieren, können Sie eine automatische Anmeldung einrichten. Bei der automatischen Anmeldung müssen Sie keine Anwenderkennung und kein Kennwort eingeben, wenn Sie auf eine Worklist-Verknüpfung klicken. Die automatische Anmeldung verwendet zum Anmelden bei einer Worklist die Anmeldeinformationen Ihrer Windows-Domäne.

Hinweis: Damit die automatische Anmeldung korrekt funktioniert, muss der Anwender in CA EEM *nicht* den Gruppen Workflow-Administratoren, Initiatoren für Workflow-Prozesse oder Workflow-SuperUser angehören. Für diese Gruppen werden andere Zugriffsebenen für Anwender bereitgestellt, die in der Workflow-Entwicklungsumgebung angemeldet sind.

So richten Sie die automatische Anmeldung für Worklist-Aufgaben ein (nur Windows):

1. Installieren und konfigurieren Sie CA Workflow.
2. [Konfigurieren Sie Worklist und Workflow Manager für die automatische Anmeldung](#) (siehe Seite 289).
3. Konfigurieren Sie CA EEM so, dass es auf ein externes Verzeichnis verweist (z. B. Microsoft Active Directory), um Anwender zu authentifizieren. Weitere Informationen finden Sie in der Dokumentation zu CA EEM.

Hinweis: Ein Anwender muss über einen CA EEM-Anwenderdatensatz und einen entsprechenden gültigen CA SDM-Kontaktdatensatz für das gleiche Anwenderkonto verfügen, um auf die Worklist zugreifen und sich automatisch anmelden zu können. Damit ein Element in der Worklist aufgeführt wird und Sie sich die Gruppen "Workflow-Administrator", "Workflow-Prozessinitiator" und "Workflow-SuperUser" in CA EEM zunutze machen können, ist ein gültiger CA EEM-Anwenderdatensatz erforderlich.

4. Melden Sie sich bei CA SDM an.
5. Klicken Sie auf die Registerkarte "Administration".
6. Klicken Sie in der Baumstruktur auf der linken Seite auf "Optionsmanager" und CA Workflow.

Das Fenster "Optionen - Liste" wird angezeigt.

7. Vergewissern Sie sich, dass der Anwendername in `cawf_username` und das Kennwort in `cawf_password` ein gültiger Anwender in der in CA EEM eingerichteten Domäne ist. Ist dies nicht der Fall, fügen Sie den Anwender mit CA EEM der Domäne hinzu.

Wichtig! Im Optionsmanager werden die Werte in `cawf_username` und `cawf_password` gesetzt. Sie basieren auf den Werten, die für den Namen und das Kennwort des berechtigten Anwenders beim Konfigurieren von CA SDM nach der Installation angegeben wurden. Wenn der privilegierte Anwender, der während der CA SDM-Konfiguration angegeben wurde, bei der Konfiguration von CA EEM für die Referenz auf das externe Verzeichnis nicht verfügbar ist, funktioniert die automatische Anmeldung *nicht*. In diesem Fall verwenden Sie CA EEM, um den Anwender der Domäne hinzuzufügen. Sie können auch die Informationen in `cawf_username` und `cawf_password` so ändern, dass ein gültiger Domänenanwender in CA EEM eingerichtet ist.

8. Melden Sie sich bei CA SDM an, und erstellen Sie einen neuen Change, Request, Incident, ein neues Problem oder einen neuen Issue mit der geeigneten Kategorie.

Hinweis: Stellen Sie sicher, dass die Kategorie zur Verwendung von CA Workflow konfiguriert und ihr eine CA Workflow-Definition angehängt ist, bevor Sie einen Change, einen Request, einen Incident, ein Problem oder einen Issue erstellen.

Nun können Sie auf eine Verknüpfung in der Worklist klicken und sich anmelden, ohne Ihre Anwenderkennung und Ihr Kennwort einzugeben.

Weitere Informationen:

[Konfigurieren der Workflow-Entwicklungsumgebung für die automatische Anmeldung](#)
(siehe Seite 290)

Konfigurieren der Worklist und des Workflow-Managers für die automatische Anmeldung

Sie können die automatische Anmeldung für Worklist und Workflow Manager aktivieren, indem Sie den Wert der Variablen `automaticLoginEnabled` in den `web.xml`-Dateien für Worklist und Workflow Manager (`wl.xml` und `pm.xml`) auf "wahr" setzen. Die Einträge sind in beiden `web.xml`-Dateien identisch.

```
<env-entry>
  <env-entry-name>automaticLoginEnabled</env-entry-name>
  <env-entry-value>true</env-entry-value>
  <env-entry-type>java.lang.Boolean</env-entry-type>
</env-entry>
```

Der Anfangswert für Worklist und Workflow Manager wird während der Installation basierend auf der Einstellung in der Antwortdatei definiert.

Automatische Anmeldung aktivieren oder deaktivieren (auch bekannt als Single Sign On oder SSO)

-P serverAction.automaticLoginEnabled="true"

So konfigurieren Sie Worklist und Workflow Manager für die automatische Anmeldung:

1. Navigieren Sie zu den Dateien pm.xml und wl.xml im folgenden Verzeichnis:
`$NX_ROOT\bopcfg\www\CATALINA_BASE_WF\conf\Catalina\localhost`
2. Bearbeiten Sie pm.xml und wl.xml und ändern Sie den Wert in der folgenden Zeile:
 - (Vor dem Bearbeiten) `<Environment name="automaticLoginEnabled" override="true" type="java.lang.Boolean" value="false"/>`
 - (Nach dem Bearbeiten) `<Environment name="automaticLoginEnabled" override="true" type="java.lang.Boolean" value="true"/>`
3. Halten Sie den Tomcat-Server mit folgendem Befehl an:
`pdm_tomcat_nxd -d STOP -t CAWF`
4. Starten Sie den Tomcat-Server erneut mit folgendem Befehl, um diese beiden Ordner neu zu erstellen:
`pdm_tomcat_nxd -d START -t CAWF`
5. Öffnen Sie ein Ticket mit einer Workflow-Aufgabe, und wählen Sie eine Aufgabe aus.
6. Die Worklist wird nach der erfolgreichen automatischen Anmeldung angezeigt.

Hinweis: Wenn Sie CA Workflow neu konfigurieren und auf einen anderen CA EEM-Server verweisen, müssen Sie CAWF-Tomcat herunterfahren, die beiden Ordner *pm* und *wl* im Verzeichnis `$NX_ROOT\bopcfg\www\CATALINA_BASE_WF\webapps` löschen und dann CAWF-Tomcat erneut starten, damit diese Ordner mit den neuen CA EEM-Serverinformationen neu erstellt werden.

Konfigurieren der Workflow-Entwicklungsumgebung für die automatische Anmeldung

Die automatische Anmeldung für die Workflow-Entwicklungsumgebung wird durch den Befehlszeilenparameter *-auto* aktiviert.

CA Workflow-Optionen

Die nachstehenden Optionen steuern die CA Workflow-Funktionen:

Wichtig! Nach dem Installieren von CA Workflow und CA EEM müssen Sie einige Optionen manuell im Optionsmanager festlegen, z. B. die Portnummer. So wird beispielsweise eine separate Tomcat-Webanwendung für CA Workflow verwendet, damit der Standardport 8080 nicht mehr genutzt werden kann. Um Port-Konflikte zu vermeiden, wird der Standardwert 8090 verwendet. Weitere Informationen finden Sie im *Implementierungshandbuch*.

cawf_hostname

Gibt den Hostnamen des Servers an, auf dem CA Workflow installiert ist. Legen Sie diese Variable nur fest, wenn CA Workflow von den CA SDM-Medien installiert wurde. Installieren Sie diese Option sonst nicht.

cawf_password

Gibt das Kennwort für den CA Workflow-IDE-Anwender an. Während der CA Workflow-Installation verwendet der CA SDM-Installationsassistent für Komponenten den Workflow-Anwendernamen, um das "cawf_password" zu setzen.

cawf_pm_location

Gibt den Speicherort der Anwendung CA Workflow-Prozess-Manager ein. Die URL muss das folgende Format aufweisen:

`http://<wf_hostname>:8090/pm`

cawf_pm_url

Gibt die URL für den CA Workflow-Prozess-Manager-Webservice an. Die URL muss das folgende Format aufweisen:

`http://<wf_hostname>:8090/pm/services/pmService2`

cawf_username

Gibt den CA Workflow-Anwendernamen für den CA Workflow-IDE-Anwender an. Während der CA Workflow-Installation verwendet der CA SDM-Installationsassistent für Komponenten den Workflow-Anwendernamen, um den "cawf_username" zu setzen.

cawf_wl_location

Gibt den Speicherort der Anwendung CA Workflow-Worklist-Manager an. Die URL muss das folgende Format aufweisen:

`http://<wf_hostname>:8090/wl`

cawf_wl_url

Gibt die URL für den CA Workflow-Worklist-Webservice an. Die URL muss das folgende Format aufweisen:

`http://<wf_hostname>:8090/wl/services/wlService`

Wichtig! Wenn eine Option installiert oder deinstalliert wird, ist es erforderlich, dass Sie die CA SDM-Server neu starten. Bei der Konfiguration für erweiterte Verfügbarkeit ist es nicht für alle Optionen erforderlich, dass Sie alle Server neu starten. Stellen Sie sicher, dass Sie die Liste des Server-Neustarts lesen, bevor Sie einen Server neu starten.

Konfigurieren des Problem Management-Beispiel-Workflows

Der Problem Management-Beispiel-Workflow lenkt den Entscheidungsprozess, ob für ein bestimmtes Problem-Ticket ein Change erstellt werden soll. Nachdem ein Zuständiger das Problem untersucht hat, führt er eine Umfrage durch und erstellt eine Empfehlung. Die Umfrage gibt der genehmigenden Person eine Vorstellung von der Auswirkung des Problems und zeigt auf, ob eine Lösung über das Change Management erforderlich ist. Das diesem Workflow (Problemstellung/Wertanalyse) zugrunde liegende Konzept ist von ITIL v3 abgeleitet.

Hinweis: Ausführliche Informationen über die Durchführung von CA SDM-Aufgaben im folgenden Prozess finden Sie in der *Online-Hilfe*.

So konfigurieren Sie den Problem Management-Beispiel-Workflow:

1. Erstellen Sie einen CA SDM-Kontakt für einen Analysten (z. B. Jane Analyst) mit den folgenden Werten:

Kontakttyp

Wählen Sie "Analyst".

Datenaufteilung

Wählen Sie "Service Desk-Analyst".

Zugriffstyp

Wählen Sie "Service Desk-Mitarbeiter".

E-Mail-Adresse

Geben Sie eine E-Mail-Adresse ein.

Hinweis: Zu Testzwecken können Sie Ihre eigene E-Mail-Adresse eingeben.

Benachrichtigungsmethode

Wählen Sie E-Mails für eilige Benachrichtigungen sowie für niedrige, normale und hohe Wichtigkeit aus.

2. Erstellen Sie einen CA SDM-Kontakt für einen Supervisor (z. B. Joe Supervisor) mit den folgenden Werten:

Kontakttyp

Wählen Sie Manager.

Datenaufteilung

Wählen Sie "Service Desk-Administrator".

Zugriffstyp

Wählen Sie "Service Desk-Management".

E-Mail-Adresse

Geben Sie eine E-Mail-Adresse ein.

Hinweis: Zu Testzwecken können Sie Ihre eigene E-Mail-Adresse eingeben.

Benachrichtigungsmethode

Wählen Sie Benachrichtigungen für niedrige, normale und hohe Priorität oder eilige Benachrichtigungen aus.

3. Erstellen Sie einen zugeordneten EEM-Benutzerdatensatz für die CA SDM-Kontakte Jane Analyst und Joe Supervisor.

Hinweis: Die Benutzer-IDs der EEM-Datensätze müssen mit denen der Kontaktdatensätze übereinstimmen. Informationen über das Erstellen von EEM-Benutzerdatensätzen finden Sie in der *EEM Online-Hilfe*.

4. Weisen Sie Joe Supervisor als Supervisor dem Kontaktdatensatz von Jane Analyst zu.
5. Erstellen Sie ein CI (z. B. Exchange Server).
6. Erstellen Sie einen Ursachen-Code (z. B. RAM Upgrade erforderlich).
7. Erstellen Sie einen Problembereich (z. B. ProblemMgmt.SampleWF).
8. Verknüpfen Sie den Problembereich ProblemMgmt.SampleWF mit dem Problem Management-Beispiel-Workflow.
9. Erstellen Sie ein Problem-Ticket mit den folgenden Attributen:

Problembereich

Wählen Sie "ProblemMgmt SampleWF" aus.

Konfigurationselement

Wählen Sie Exchange Server aus.

Zuständiger

Wählen Sie Analyst, Jane.

10. Melden Sie sich als Jane Analyst bei CA SDM an, und testen Sie die Workflow-Konfiguration.

Hinweis: Sie müssen die Problemforschung abschließen, bevor Sie das erste Formular im Workflow ausfüllen. Informationen über die Durchführung von Workflow-Aufgaben finden Sie in der *CA Workflow-Online-Hilfe*.

Weitere Informationen:

[Einrichten der automatischen Anmeldung \(CA MDB-Authentifizierung\)](#) (siehe Seite 307)

[Einrichten der automatischen Anmeldung \(Externe Authentifizierung\)](#) (siehe Seite 288)

[Starten und Anhalten von CA Workflow](#) (siehe Seite 284)

Konfigurieren des Beispiel-Workflows "PC-Auftrag"

Der Beispiel-Workflow "PC-Auftrag" führt Sie durch den Change Management-Prozess bei Bestellung eines neuen PC.

Hinweis: Ausführliche Informationen darüber, wie Sie jede der CA SDM-Aufgaben im folgenden Prozess ausführen, finden Sie in der *Online-Hilfe*.

So richten Sie den Beispiel-Workflow "PC-Auftrag" ein und testen ihn:

1. Erstellen Sie einen CA SDM-Kontakt für einen Mitarbeiter (z. B. William Mitarbeiter) mit den folgenden Werten:

Kontakttyp

Wählen Sie "Mitarbeiter" aus.

Datenaufteilung

Wählen Sie "Mitarbeiter" aus.

Zugriffstyp

Wählen Sie "Mitarbeiter" aus.

E-Mail-Adresse

Geben Sie eine E-Mail-Adresse ein.

Hinweis: Zu Testzwecken können Sie Ihre eigene E-Mail-Adresse eingeben.

Benachrichtigungsmethode

Wählen Sie E-Mails für eilige Benachrichtigungen sowie für niedrige, normale und hohe Wichtigkeit aus.

2. Erstellen Sie einen CA SDM-Kontakt für einen Analysten (z. B. Jane Analyst) mit den folgenden Werten:

Kontakttyp

Wählen Sie "Analyst".

Datenaufteilung

Wählen Sie "Service Desk-Analyst".

Zugriffstyp

Wählen Sie "Service Desk-Mitarbeiter".

E-Mail-Adresse

Geben Sie eine E-Mail-Adresse ein.

Hinweis: Zu Testzwecken können Sie Ihre eigene E-Mail-Adresse eingeben.

Benachrichtigungsmethode

Wählen Sie E-Mails für eilige Benachrichtigungen sowie für niedrige, normale und hohe Wichtigkeit aus.

3. Erstellen Sie einen zugeordneten EEM-Benutzerdatensatz für die CA SDM-Kontakte "William Mitarbeiter" und "Jane Analyst".

Hinweis: Die Benutzer-IDs der EEM-Datensätze müssen mit denen der Kontaktdatensätze übereinstimmen. Informationen über das Erstellen von EEM-Benutzerdatensätzen finden Sie in der *EEM Online-Hilfe*.

4. Erstellen Sie eine Change-Kategorie (zum Beispiel PC.Order).
5. Weisen Sie Anna Analyst als Zuständige der Change-Kategorie zu.
6. Erstellen Sie ein Change-Ticket mit den folgenden Attributen:

Änderungskategorie

Wählen Sie "PC Auftrag" aus.

Zuständiger

Wählen Sie "Analyst, Jane".

7. Melden Sie sich als Jane Analyst bei CA SDM an, und testen Sie die Workflow-Konfiguration.

Hinweis: Informationen über das Durchführen von Workflow-Aufgaben finden Sie in der *CA Workflow-Online-Hilfe*.

Beispiel einer Change-Management-Prozessdefinition

Dieses Beispiel zeigt, wie die Change-Management-Prozessdefinition unter Verwendung der folgenden ITIL-v3-Richtlinien Changes handhabt:

- Risikobewertung
- Konflikt- und Auswirkungsanalyse

- Genehmigungen sowohl durch den Change Manager als auch durch den CAB
- Implementierungsbewertung und -prüfung

Hinweis: In diesem Beispiel wird angenommen, dass CA SDM CA Workflow verwendet und die Change-Management-Prozessdefinition eingerichtet ist. Informationen zur Einrichtung der Change-Management-Prozessdefinition finden Sie im *Administrationshandbuch*.

Beispiel für das Vorbereiten eines Change für die Genehmigung

Dieses Beispiel konfiguriert eine Change-Kategorie und bereitet einen Change für die Genehmigung vor. Als Administrator konfigurieren Sie die Change-Kategorie, um die Change-Management-Prozessdefinition zu verwenden und Gruppen und Kontakte einzurichten. Als Anforderer füllen Sie eine Risikobewertungsumfrage aus, führen eine Konflikt- und Auswirkungsanalyse und eine Änderungsanalyse durch.

Hinweis: Information zur Konfiguration der Change-Kategorie und zum Arbeiten mit der Change-Management-Prozessdefinition finden Sie in der *Online-Hilfe* und im *Administrationshandbuch*.

Um einen Change für die Genehmigung vorzubereiten, tun Sie Folgendes:

1. Melden Sie sich als Administrator an und erstellen oder bearbeiten Sie eine Change-Kategorie mit folgenden Optionen. Klicken Sie dann auf "CA Workflow verwenden":
 - **CAB** - Wählen Sie die CAB-Gruppe aus.
 - **Gruppe** - Geben Sie die Implementierungsgruppe an.
 - **Risikoumfrage** - Wählen Sie "Allgemein" aus.
 - **CA Workflow - Definitionsname** - Wählen Sie "Change Mgmt - Service Desk r12.1 (auf der Registerkarte "Workflow")".
2. Erstellen Sie die folgenden CA SDM-Anwender-IDs und -Kontakte und weisen Sie sie den entsprechenden Gruppen in CA SDM und CA EEM zu:
 - **Peter Anforderer** - Kontakt, der den Change erstellt
 - **Johann Genehmiger** - Manager der Implementierungsgruppe, der als Change Manager zur Genehmigung eines Change fungiert. Ein Manager der CAB-Gruppe, die als CAB-Genehmiger fungiert.
 - **Susanne Implementierer** - Mitglied der Implementierungsgruppe, das auch die Arbeitselemente des Change abschließt.
3. Melden Sie sich als Peter Anforderer an und erstellen Sie einen Change mit folgenden Werten:
 - **Angefordert von** - Geben Sie Peter Anforderer an.
 - **Kategorie** - Geben Sie die Change-Kategorie mit der Change-Management-Prozessdefinition an.

- **Typ** - Wählen Sie "Normal".
- **Zusammenfassung des Change/Change-Beschreibung** - Geben Sie den Grund für den Change an.
- **Startdatum des Ablaufplans** - Geben Sie ein Startdatum an.
- **Dauer des Ablaufplans** - Geben Sie die Dauer an.
- **CI**s - Geben Sie die betroffenen CI's auf der Registerkarte "Config. Items") an.

Peter Anforderer erhält eine E-Mail-Benachrichtigung zum Abschluss der Risikobewertungsumfrage. Die Change-Detailseite zeigt "Status - RFC" an.

4. Klicken Sie auf die Risikoumfrage und beantworten Sie die Fragen der Risikobewertungsumfrage, so dass der Change ein hohes Risiko besitzt. Klicken Sie "Absenden" und "Bestätigen".

Das System erzeugt einen Risikowert für den Change, und der Anforderer erhält eine E-Mail-Benachrichtigung, um die Konflikt- und Auswirkungsanalyse zu starten.

Hinweis: Sie können nur zur nächsten Aufgabe gehen, nachdem Sie auf der Seite zum Ausführen der Aufgabe auf "Bestätigen" geklickt haben.

5. Folgen Sie auf der Registerkarte "Workflow-Aufgaben" den Verknüpfungen, um zur Registerkarte "Konflikte" des Change zu gelangen.
6. Klicken Sie auf "Konfliktanalyse", um alle Planungskonflikte für CI's zu überprüfen und zu lösen.
7. Klicken Sie auf der Registerkarte "Configuration Items" auf Auswirkungsanalyse, um Informationen zu jedem CI zu überprüfen.
8. Klicken Sie auf der Registerkarte "Configuration Items" auf Auswirkungs-Explorer und navigieren Sie zur Registerkarte "CMDB-Beziehungen", um die Auswirkung des Change auf entsprechende CI's abzuschätzen.
9. Navigieren Sie zur Seite zum Durchführen der Aufgabe und klicken Sie auf "Bestätigen".

Peter Anforderer erhält eine E-Mail-Benachrichtigung, um die Change-Analyse aufzuführen.

10. Folgen Sie auf der Registerkarte "Workflow-Aufgaben" den Verknüpfungen, um zur Registerkarte für die Change-Analyse des Change zu gelangen. Beantworten Sie die Fragen, um den Change zu bestätigen, und klicken Sie auf "Absenden".

Johann Genehmiger erhält eine E-Mail-Benachrichtigung, um den Change zu genehmigen. Die Seite "Change - Detail" zeigt Folgendes an: "Status - Genehmigung in Bearbeitung".

- CAB-Genehmigung: Ja

Beispiel für das Genehmigen und Implementieren eines Change

Dieses Beispiel zeigt den Genehmiger und die Implementierungsaufgaben, die durchgeführt werden müssen, wobei die Change-Management-Prozessdefinition verwendet wird, um Changes zu verarbeiten. Als genehmigende Person überprüfen Sie die Informationen aus der Change-Analyse und genehmigen den Change. Als Mitglied der Implementierungsgruppe schließen Sie die zugewiesene Arbeit am Change ab und senden eine Implementierungsprüfung, welche das Ergebnis des Change beschreibt.

Hinweis: Informationen zur Handhabung der Change-Management-Prozessdefinition finden Sie im *Administrationshandbuch*.

Um den Change zu genehmigen und zu implementieren, tun Sie Folgendes:

1. Melden Sie sich als Johann Genehmiger an und öffnen Sie den Change.
2. Folgen Sie auf der Registerkarte "Workflow-Aufgaben" den Verknüpfungen, um zur Registerkarte für die Genehmigung durch den Change Manager zu gelangen, und klicken Sie auf "Genehmigen".

Da der Change als hochriskant eingestuft ist, lautet der Status "Genehmigung in Bearbeitung". Da dieses Beispiel Johann Genehmiger auch als Mitglied des CAB-Ausschusses verwendet, erhält Johann Genehmiger eine E-Mail-Benachrichtigung, um den Change als CAB-Mitglied zu überprüfen.

3. Klicken Sie auf der Registerkarte zur CAB-Genehmigung auf "Genehmigen".

Die Change-Detailseite zeigt den Status "Genehmigt". Susanne Implementierer erhält eine E-Mail-Benachrichtigung.

4. Melden Sie sich als Susanne Implementierer an und öffnen Sie den Change.
5. Navigieren Sie auf der Registerkarte "Workflow-Aufgaben" zur Seite zum Durchführen von Aufgaben und klicken Sie auf "Bestätigen".

Die Seite "Changes – Detail" zeigt den Status "Implementierung in Bearbeitung" an.

6. Folgen Sie auf der Registerkarte "Workflow-Aufgaben" den Verknüpfungen, um zur Registerkarte zur abgeschlossenen Implementierung zu gelangen.
7. Beantworten Sie die Fragen, um zu beschreiben, wie der Change fortgeschritten ist, und klicken Sie auf "Abschließen".

Der Change wird nun geschlossen. Die Change-Detailseite zeigt "Status - Implementiert" und "Schließungscode - Erfolgreich". Susanne Implementierer erhält eine E-Mail-Benachrichtigung, um das PIR auszuführen.

8. Folgen Sie auf der Registerkarte "Workflow-Aufgaben" den Verknüpfungen, um zur PIR-Registerkarte zu gelangen.
9. Beantworten Sie auf der Registerkarte "PIR" die Fragen, um die Behebung zu beschreiben, und klicken Sie auf "Absenden".

Der Change wird nun geschlossen. Die Change-Detailseite zeigt "Status - Geschlossen" an. Die Registerkarte "Workflow-Aufgaben" zeigt die Verknüpfung zum Schließen des Change mit zusätzlichen Informationen an. Die Registerkarte "Change-Aktivitäten" zeigt den endgültigen Status der Change-Management-Prozessdefinition an.

Konfigurieren der Workflow-Integration in CA Process Automation

Um die Workflow-Integration in CA Process Automation zu konfigurieren, führen Sie die folgenden Schritte aus:

1. Überprüfen Sie, dass CA Process Automation und CA SDM als eigenständige Einheiten funktionieren.

Wichtig! Wenn CA Process Automation im FIPS-Modus konfiguriert wird, müssen Sie auch EEM-Server und EEM-SDK im FIPS-Modus konfigurieren. Weitere Informationen über die Konfiguration von EEM-SDK im FIPS-Modus finden Sie in der EEM-Dokumentation.

2. Konfigurieren Sie die CA Process Automation Workflow-Optionen.
3. Erstellen Sie die notwendigen Gruppen und Anwender-IDs, um CA SDM-Anwendern den entsprechenden Zugriff auf CA Process Automation zu gewähren.

Weitere Informationen:

[Überprüfen der Installationen von CA Process Automation und CA SDM](#) (siehe Seite 300)
[Konfigurieren von CA Process Automation Workflow-Optionen](#) (siehe Seite 300)
[CA Process Automation-Anwenderverwaltung](#) (siehe Seite 304)
[Unterstützen von Single Sign-On von CA SDM bei CA Process Automation mithilfe CA EEM](#) (siehe Seite 305)

Überprüfen der Installationen von CA Process Automation und CA SDM

Sie können CA Process Automation und CA SDM integrieren, damit sie auf einem Server gemeinsam ausgeführt werden, wenn die Serverarchitektur beide Produkte unterstützt. Wenn CA Process Automation- oder CA SDM-Komponenten nicht auf dem gleichen Server integriert werden können, sollten Sie die Produkte auf getrennten Servern installieren.

Bevor Sie CA Process Automation und CA SDM konfigurieren, können Sie bestätigen, dass beide Produkte installiert sind und unabhängig voneinander funktionieren.

Hinweis: Informationen über Produktvoraussetzungen für CA SDM und CA Process Automation finden Sie in den *CA SDM Versionshinweisen*.

So überprüfen Sie die Installationen von CA Process Automation und CA SDM

1. Öffnen Sie einen Browser auf dem Server, der CA SDM hostet, und überprüfen Sie, dass CA Process Automation-Benutzer sich bei CA Process Automation anmelden können. Ändern Sie die Platzhalter so, dass sie mit der Zielinstallation von CA Process Automation übereinstimmen.

`http(s)://<server>:CA Portal/itpam`

2. Geben Sie die folgende URL ein. Ändern Sie die Platzhalter so, dass sie mit der Zielinstallation von CA Process Automation übereinstimmen.

`http(s)://<server>:CA Portal/itpam/JNLRequestProcessor?processType=startUI`

Auf das CA Process Automation-Produkt kann vom CA SDM-Host aus zugegriffen werden.

Konfigurieren von CA Process Automation Workflow-Optionen

Wenn Sie CA Process Automation-Workflow-Optionen konfigurieren, geben Sie die Konnektivität zwischen CA SDM und CA Process Automation an. Wenn Sie CA EEM für die Authentifizierung verwenden, geben Sie auch den CA EEM-Hostnamen an.

So konfigurieren Sie CA Process Automation Workflow-Optionen

1. Wählen Sie auf der Registerkarte "Administration" die Optionen "Optionsmanager", "CA IT PAM-Workflow" aus.

Die Optionsliste wird angezeigt.

2. Klicken Sie mit der rechten Maustaste auf die einzelnen Optionen, und wählen Sie im Kontextmenü die Option "Bearbeiten". Konfigurieren Sie die folgenden Optionen:

caextwf_eem_hostname

Gibt den Namen des CA EEM-Servers an. Beispiel: *pam.host.com* identifiziert den Authentifizierungshost. Sie installieren "caextwf_eem_hostname" nur, wenn Sie CA Process Automation für die Verwendung von CA EEM als Authentifizierungsserver konfiguriert haben. CA SDM verwendet diesen Wert, um einen Anwendernamen und ein Kennwort in ein CA EEM-Token zu transformieren. So werden der Anwendername und das Kennwort nicht als reiner Text über HTTP übermittelt.

Hinweis: Wenn die CA Process Automation-Installation nicht CA EEM verwendet, platzieren Sie keinen Wert in der Option "caextwf_eem_hostname" und installieren "caextwf_eem_hostname" nicht. Bei Platzierung eines falschen Werts oder unnötiger Installation von "caextwf_eem_hostname" schlägt die Integration fehl.

caextwf_endpoint

Gibt die URL an, die auf die CA Process Automation-Webservices verweist. Sie umfasst den CA Process Automation-Hostnamen, den Port und den obligatorischen Pfad "/itpam/soap". Beispiel:

"http://pam.host.com:pam-Tomcat-port/itpam/soap" identifiziert den Endpunkt. Wenn Ihre Implementierung CA EEM verwendet, dann ist die Installation der Option "caextwf_eem_hostname" erforderlich, damit die Integration zwischen CA Process Automation und CA SDM ordnungsgemäß funktioniert.

caextwf_log_categories

Gibt eine kommagetrennte Liste der Namen von CA Process Automation-Prozessinstanzprotokoll-Kategorien an, die auf den Registerkarten für CA SDM-Request-, Change- und Issue-Workflow-Aufgaben angezeigt werden sollen. Beispiel: *Operator,Response,MyOwnCategory* stellt drei Protokollkategorien bereit.

Sie installieren "caextwf_log_categories" aufgrund von Geschäftsentscheidungen des CA SDM- und CA Process Automation-Prozessdesignpersonals. Diese Option passt die Standarddaten an, die auf der Registerkarte "Workflow-Aufgaben" für Requests, Changes und Issues angezeigt werden.

Wenn Sie die Option "caextwf_log_categories" installieren, werden alle CA Process Automation-Prozessinstanzprotokoll-Meldungen der Prozesskategorie und der von Ihnen angegebenen Kategorien auf der Registerkarte "Workflow-Aufgaben" angezeigt. Installieren Sie "caextwf_log_categories" nicht, werden nur die CA Process Automation-Prozessinstanzprotokoll-Meldungen der Prozesskategorie auf der Registerkarte "Workflow-Aufgaben" angezeigt.

Hinweis: Informationen zu den von CA Process Automation vordefinierten Protokollmeldungskategorien und der Definition von anwenderspezifischen Meldungskategorien finden Sie in der CA Process Automation-Referenzdokumentation.

caextwf_processdisplay_url

Gibt an, wie ein grafischer Snapshot einer CA Process Automation-Prozessinstanz durch Angabe des Hostnamens und des obligatorischen Pfads "/itpam/JNLRequestProcessor?processType=startUI&roid" gestartet wird.

Beispiel:

"http://pam.host.com:pam-Tomcat-port//itpam/JNLRequestProcessor?processType=startUI&roid=" startet einen Snapshot einer Prozessinstanz. Der Anwender wählt auf der Registerkarte "Workflow-Aufgaben" für einen Request, einen Change oder einen Issue die Option "Prozess anzeigen", um den Snapshot anzuzeigen.

Sie müssen die Option "caextwf_processdisplay_url" installieren, damit die Integration zwischen CA Process Automation und CA SDM entsprechend funktioniert.

caextwf_worklist_url

Gibt den Pfad der Prozessinstanz an, der den Hostnamen und den obligatorischen Pfad "/itpam?webPage=mytaskfilter&view=tasklist" umfasst.

Beispiel:

"http://pam.host.com:pam-Tomcat-port/itpam?webPage=mytaskfilter&view=tasklist" ermöglicht es den CA SDM-Anwendern, eine Liste von CA Process Automation-Prozessinstanzen anzuzeigen, die einen Anwendereingriff erfordern. Die Liste wird in CA Process Automation angezeigt, wenn der CA SDM-Anwender einen Link auswählt, der mit einer der aufgelisteten Aufgaben auf der Registerkarte "Workflow-Aufgaben" für die Requests, den Change oder den Issue verknüpft ist.

Sie müssen die Option "caextwf_worklist_url" installieren, damit die Integration zwischen CA Process Automation und CA SDM ordnungsgemäß funktioniert.

caextwf_ws_password

Gibt das Administratorkennwort an, das mit dem CA Process Automation-Anwendernamen der Option "caextwf_ws_user" verknüpft ist. CA SDM greift mithilfe des Anwendernamens und des Kennworts auf die Webservice-Funktionen von CA Process Automation zu, um Integrationsaktivitäten auszuführen, wie die Auswahl von Startauftragsformularen, Prozessdefinitionsinformationen und Prozessinstanzinformationen.

Die Installation der Option "caextwf_ws_password" ist für die Integration zwischen CA Process Automation und CA SDM erforderlich. Die Angabe von Kennwort und Anwendername setzt entsprechenden Zugriff auf CA Process Automation voraus. Anwendername und Kennwort für CA Process Automation müssen jedoch nicht in den Kontaktdatensätzen von CA SDM enthalten sein.

caextwf_ws_user

Gibt den CA Process Automation-Administratornamen an, der mit dem CA Process Automation-Anwendernamen der Option "caextwf_ws_password" verknüpft ist. CA SDM verwendet den Anwendernamen und das Kennwort für den Zugriff auf die CA Process Automation-Webservicesfunktionen. Diese Services führen Integrationsaktivitäten aus, wie z. B. das Auswählen von Startauftragsformularen, das Auswählen von Informationen zur Prozessdefinition, das Auswählen von Prozessinstanz-Informationen oder das Starten von Prozessinstanzen.

Sie müssen die Option "caextwf_ws_user" installieren, damit die Integration zwischen CA Process Automation und CA SDM ordnungsgemäß funktioniert. Die Angabe von Anwendername und Kennwort setzt entsprechenden Zugriff auf CA Process Automation voraus. Anwendername und Kennwort für CA Process Automation müssen jedoch nicht in den Kontaktdatensätzen von CA SDM enthalten sein.

3. Klicken Sie auf "Installieren".
4. Starten Sie den CA SDM-Service neu.

CA SDM und CA Process Automation können kommunizieren, auch wenn keine Prozessinstanzdaten vorhanden sind. CA SDM und CA Process Automation sind jetzt entsprechend vorbereitet, damit Sie CA Process Automation-Prozessdefinitionen und CA Process Automation-Startauftragsformulare erstellen können.

Hinweis: Weitere Informationen zum Erstellen von CA Process Automation-Prozessdefinitionen und CA Process Automation-Startauftragsformularen finden Sie im *Administrationshandbuch* und in der CA Process Automation-Anwenderdokumentation.

CA Process Automation-Anwenderverwaltung

Sowohl CA Process Automation als auch CA SDM haben als eigenständige Produkte individuelle Anforderungen an Authentifizierung und Autorisierung. Um eine einheitliche serviceorientierte Architektur zu unterstützen, können Sie beide Produkte für die Verwendung von CA EEM zur Authentifizierung konfigurieren.

Wenn Sie CA Process Automation mit CA EEM als Authentifizierungsserver installieren, werden vom Installationsprogramm standardmäßig mehrere Richtlinien und vier grundlegende Einheiten erstellt:

- Zwei Anwendungsbenutzer: "itpamadmin", "itpamuser". Für CA Process Automation 3.1 SP1, "pamadmin" und "pamuser".
- Zwei Anwendungsgruppen: "ITPAMAdmins", "ITPAMUsers". Für CA Process Automation 3.1 SP1, "PAMAdmins" und "PAMUsers".

CA SDM-Anwender, die auch CA Process Automation verwenden, können zwischen "ITPAMAdmins" ("PAMAdmins" für CA Process Automation 3.1 SP1) und "ITPAMUsers" folgendermaßen aufgeteilt werden:

- CA SDM-Analysten müssen ITPAMUsers-Mitglieder sein ("PAMUsers" für CA Process Automation 3.1 SP1), wenn sie folgende Aufgaben haben:
 - CA Process Automation Interaktionsauftragsformulare genehmigen, ablehnen oder auf andere Weise beantworten.
 - CA Process Automation-Prozessinstanzen auflisten, die dem Anwender zugewiesen sind.
 - Die graphische Anzeige durch Anklicken der Schaltfläche "Vorgang anzeigen" auf dem Prozessstatusbildschirm in CA Process Automation anzeigen. Für die CA Process Automation-"ITPAMUsers"-Gruppe ("PAMUsers" für 3.1 SP1) ist eine zusätzliche CA Process Automation-Richtlinie erforderlich, um den Zugriff auf die Grafik zu gewähren.
- CA SDM-Analysten sind ITPAMAdmins-Mitglieder ("PAMAdmins" für 3.1 SP1), wenn sie folgende Aufgaben haben:
 - CA Process Automation-Prozessdefinitionen und/oder Startauftragsformulare erstellen und einchecken.
 - Prozessinstanzen direkt innerhalb von CA Process Automation beenden. Das Beenden von Prozessinstanzen ist eine administrative Ausnahme von erwarteten Integrationsverfahren.
 - CA Process Automation-Prozessinstanzaufgaben delegieren.
 - Wenn der Anwender der in CA SDM-Optionsmanager definierte Anwendername ist.

- CA SDM-Anwender benötigen keinen Zugriff auf CA Process Automation, wenn sie folgende Aufgaben haben:
 - Requests, Changes und Issues erstellen, mit denen CA Process Automation-Instanzen gestartet werden.
 - Die Registerkarte "Workflow" überprüfen, die CA Process Automation-Prozessinstanzstatus und Aufgabeninformationen anzeigt.
 - Wenn der Status eines Request, Change oder Issue geändert wird, führt dies zur Beendigung eines CA Process Automation-Prozesses (z. B. das Abbrechen eines Change).
 - Eine CA Process Automation-Prozessdefinition in einem CA SDM-Request-Bereich, einer Change-Kategorie oder einer Issue-Kategorie auswählen.

Hinweis: Informationen zur CA EEM-Konfiguration finden Sie in der CA Process Automation-Dokumentation.

Unterstützen von Single Sign-On von CA SDM bei CA Process Automation mithilfe CA EEM

Wenn Sie CA SDM und CA Process Automation integriert haben, können Sie Single Sign-On einrichten, um von CA SDM zu CA Process Automation zu gehen. Führen Sie die folgenden Schritte aus:

1. Vergewissern Sie sich, dass die folgenden Anforderungen erfüllt sind:
 - CA SDM und CA Process Automation sind für die Verwendung der gleichen CA EEM-Installation konfiguriert.
 - Der Benutzer, der sich bei CA SDM anmeldet, ist auch ein Benutzer in CA Process Automation.
 - Wenn CA EEM die interne Datenbank als Benutzerspeicher verwendet, müssen die Benutzer entweder globale Berechtigungen haben oder zum gleichen Ordner gehören. Andernfalls müssen die Benutzer, wenn CA EEM auf einen externen Benutzerspeicher wie ein externes Verzeichnis oder CA SiteMinder verweist, zum gleichen Speicher gehören, um auf Single Sign-On zuzugreifen.
2. Installieren Sie CA EEM von der CA SDM-Installations-DVD oder verwenden Sie ein anderes vorhandenes Installationsprogramm für CA EEM (z. B. CA EEM für CA Process Automation).

3. Gehen Sie auf der Registerkarte "Administration" in CA SDM zu "Optionsmanager" > "Sicherheit", und installieren Sie die folgenden Optionen:

- eiam_hostname
- use_eiam_authentication

Hinweis: Es ist nicht erforderlich, unter "Optionsmanager" > "CA Process Automation" die Option "caextwf_eem_hostname" zu installieren. Wenn Sie sie jedoch installieren, muss der Wert der gleiche wie für die Option "eiam_hostname" sein.

4. Starten Sie CA SDM neu.
5. Gehen Sie wie folgt vor, um einen Benutzer in CA Process Automation zu erstellen:
 - a. Melden Sie sich im CA Process Automation-Anwendungskontext bei CA EEM an. Verwenden Sie die Benutzer-ID "EiamAdmin" oder eine sonstige Administrator-ID.
 - b. Klicken Sie auf die Registerkarte "Identitäten verwalten", und klicken Sie auf das Symbol neben dem Benutzerordner.
 - c. Auf der Seite "Neuer Benutzer" enthält das Namensfeld oben die Benutzer-ID, die der Benutzer-ID in der CA SDM-Kontakttable entsprechen muss.
 - d. Klicken Sie auf die Schaltfläche "Anwendungsbenutzerdetails hinzufügen", und gehen Sie wie folgt vor:
 - Fügen Sie eine der beiden aufgeführten Gruppen bzw. beide Gruppen hinzu. Fügen Sie mindestens eine dieser zwei Gruppen hinzu, um sich bei CA Process Automation anmelden zu können.
 - Füllen Sie die Felder für "Neuer Benutzer" aus ("Vorname", "Nachname", "Anzeige" und "Kennwort").
6. Erstellen Sie in der CA SDM-Kontakttable einen Benutzer mit der gleichen Benutzer-ID. Überprüfen Sie, dass das Feld für den Zugriffstyp-Validierungstyp auf CA EEM gesetzt ist.

Sie können sich bei CA EEM und CA SDM mit diesem Benutzer und dem in CA EEM angegebenen Kennwort anmelden.

Einrichten der automatischen Anmeldung (CA MDB-Authentifizierung)

Um den Anmeldeprozess für <WF>-Worklist-Aufgaben beim Arbeiten mit Changes, Anfragen, Incidents, Problemen und Issues zu automatisieren, können Sie eine automatische Anmeldung einrichten. Bei der automatischen Anmeldung müssen Sie keine Benutzerkennung und kein Kennwort eingeben, wenn Sie auf eine Worklist-Verknüpfung klicken. Die automatische Anmeldung verwendet zum Anmelden bei einer Worklist die Anmeldeinformationen Ihrer Windows-Domäne.

Hinweis: Damit die automatische Anmeldung korrekt funktioniert, muss der Benutzer in CA EEM *nicht* den Gruppen Workflow-Administratoren, Initiatoren für Workflow-Prozesse oder Workflow-SuperUser angehören. Für diese Gruppen werden andere Zugriffsebenen für Benutzer bereitgestellt, die in der Workflow-Entwicklungsumgebung angemeldet sind.

So richten Sie die automatische Anmeldung für Worklist-Aufgaben ein (nur Windows):

1. [Installieren und konfigurieren Sie CA Workflow](#) (siehe Seite 233).
2. [Konfigurieren Sie Worklist und Workflow Manager für die automatische Anmeldung](#) (siehe Seite 289).
3. Konfigurieren Sie CA EEM so, dass Benutzer mit CA MDB authentifiziert werden. Beim Installieren und Konfigurieren von CA Workflow wird Ihr *Workflow-Benutzername* und *Workflow-Kennwort* automatisch zu CA EEM hinzugefügt. Weitere Informationen finden Sie in der Dokumentation zu CA EEM.
Hinweis: Ein Benutzer muss einen CA EEM-Benutzerdatensatz haben, um auf die Worklist zuzugreifen.
4. Melden Sie sich bei CA SDM an, und erstellen Sie einen neuen Change, eine neue Anfrage, einen neuen Incident, ein neues Problem oder einen neuen Issue mit der geeigneten Kategorie.

Hinweis: Stellen Sie sicher, dass die Kategorie zur Verwendung von CA Workflow konfiguriert und ihr eine CA Workflow-Definition angehängt ist, bevor Sie einen Change, eine Anfrage, einen Incident, ein Problem oder einen Issue erstellen.

Nun können Sie auf eine Verknüpfung in der Worklist klicken und sich anmelden, ohne Ihre Benutzerkennung und Ihr Kennwort einzugeben.

Weitere Informationen:

[Konfigurieren der Workflow-Entwicklungsumgebung für die automatische Anmeldung](#)
(siehe Seite 290)

Konfigurieren des "Single Point of Entry"

Wenn CA SDM und CA Service Management integriert sind, ermöglicht ein "Single Point of Entry" Single Sign-Ons beim CA Service Catalog.

So konfigurieren Sie den "Single Point of Entry"

1. Installieren Sie die Option "General" (Allgemein) von "catalog_server".
Hinweis: Weitere Informationen hierzu finden Sie in der Online-Hilfe des Optionsmanagers.
2. Starten Sie CA SDM neu.
3. Navigieren Sie zur Mitarbeiter-Self-Service-Seite von CA SDM.
4. Klicken Sie auf "Katalogdienste durchsuchen".
Die Anmeldeseite von CA Service Management wird angezeigt.

Wenn CA EEM sowohl für CA SDM als auch für CA Service Management konfiguriert ist, ermöglicht ein "Single Point of Entry" ein Single Sign-On beim CA Service Catalog. Wenn Single Sign-On konfiguriert ist, wird die CA Service Management-Anmeldeseite nicht angezeigt.

Hinweis: Single Sign-On ist nicht verfügbar, wenn Sie als Gast auf den Mitarbeiter-Self-Service in CA SDM zugreifen.

So konfigurieren Sie Single Sign-On bei CA Service Management

1. Überprüfen Sie, dass die CA EEM-Sicherheitsoptionen "eiam_hostname" und "use_eiam_authentication" installiert sind.
2. Richten Sie Ihre Benutzer in CA EEM ein und überprüfen Sie, dass diese Benutzer auch CA Service Management-Benutzer sind.
3. Klicken Sie auf die Registerkarte "Verwaltung".
4. Öffnen Sie den Ordner "Sicherheits- und Rollenmanagement".
5. Klicken Sie auf "Zugriffstypen".
6. Wählen Sie die Mitarbeiterrolle aus.
7. Überprüfen Sie, dass der Validierungstyp auf der Registerkarte "Webauthentifizierung" auf "CA EEM CA Embedded Entitlements Manager verwenden" festgelegt ist.
8. Melden Sie sich als der definierte CA EEM-Benutzer an und navigieren Sie zur Mitarbeiter-Self-Service-Seite
9. Klicken Sie auf "Katalogdienste durchsuchen".
Die Hauptseite von CA Service Management wird angezeigt.

Implementieren der Mandantenfähigkeit

Der *Service Provider* ist der primäre Mandant einer mandantenfähigen CA SDM-Installation.

Hinweis: Weitere Informationen über Service Provider und Mandantenfähigkeit finden Sie im *Administrationshandbuch*.

Definieren Sie zunächst alle benötigten Mandanten, indem Sie das Attribut "Mandant" mit allen erforderlichen und optionalen Mandantenobjekten füllen. Anschließend können Sie die Mandantenfähigkeit in einem anderen als dem Setupmodus aktivieren. Die Option "Erzwingen mehrerer Mandanten" können Sie jedoch bereits auswählen, bevor allen Objekten die erforderlichen Mandanten zugewiesen sind. Objekte mit null Mandanten in einer mandantenabhängigen Tabelle werden wie öffentliche Objekte behandelt, die für alle Anwender sichtbar sind, und die Benutzeroberfläche erkennt und unterstützt Aktualisierungen dieser Objekte. Je nach Umfang der erzwungenen Mandantenfähigkeit erfordert CA SDM möglicherweise einen Anwender, damit ein mandantenabhängiges Objekt aktualisiert und ein Mandant bereitgestellt wird.

Hinweis: Sie müssen einen Mandanten erstellen, bevor eine Instanz eines mandantenabhängigen Objekts aktualisiert werden kann. Außerdem können die Hilfsprogramme "pdm_settenant" und "pdm_buildtenant" nach der Aktivierung der Mandantenfähigkeit verwendet werden, um die Einstellung des Attributs abzuschließen. Wenn Tabellen, die Mandanten erfordern, inkorrektweise Daten ohne Mandanten in einem mandantenfähigen System enthalten, wird in Tabellen, die Mandanten erfordern, eine Dropdown-Liste für öffentliche Daten angezeigt.

Wichtig! Bevor Sie "pdm_buildtenant" ausführen, *müssen* Sie den Service Provider konfigurieren.

So implementieren Sie die Mandantenfähigkeit:

1. [Legen Sie für die Mandantenfähigkeiten-Option die Einstellung "Setup." fest](#) (siehe Seite 329), und führen Sie CA SDM zurück. Bei jeder Änderung des Mandantenstatus ("setup", "on", "on(allow)") ist eine Zurückführung der Services erforderlich.

Wichtig! Wenn sich die Mandantenfähigkeit im Setup-Modus befindet, sind Web-Schnittstellenänderungen für Service Provider-Administratoren aktiv. Dies bedeutet, dass auf Mandanten bezogene Objekte und Daten angezeigt und in der Web-Schnittstelle bearbeitet werden können. Einschränkungen der Mandantenfähigkeit werden jedoch nicht durchgesetzt, und andere Anwender (außer Service Provider-Administratoren) können Änderungen der Produktschnittstelle nicht sehen. Daher können Sie das Produkt weiterhin im Modus ohne Mandanten verwenden und sich auf die Mandantenfähigkeit vorbereiten.

2. [Ordnen Sie dem Mandantenobjekt alle vorhandenen Mandantenimplementierungen zu.](#) (siehe Seite 331)

3. [Füllen Sie die Mandantenspalten](#) (siehe Seite 332).

Hinweis: Es empfiehlt sich, zuerst die Mandantenspalte in den Kontakten zu füllen und dann die Kontakte mit Mandanten zum Füllen der Mandantenspalte in den anderen Objekten zu verwenden.

4. Überprüfen Sie, ob der Mandant in allen mandantenabhängigen Tabellen festgelegt ist.
5. [Erstellen Sie Mandanten](#). (siehe Seite 333)

Wichtig! Als erster Mandant muss der Service Provider-Mandant erstellt werden. Nachdem Sie den Service Provider-Mandanten erstellt haben, melden Sie sich bei CA Service Desk ab und dann als Mitglied des Service Provider wieder an. Eine einfache Möglichkeit für diese Anmeldung besteht darin, sich als der berechnete Anwender anzumelden (z. B. ServiceDesk), weil dieser Anwender automatisch zum Service Provider-Mandanten gehört. Wenn Sie sich als ein anderer Kontakt anmelden möchten, weisen Sie den Kontakt dem Service Provider zunächst mit "pdm_settenant" zu.

6. [Erstellen von Mandantengruppen](#). (siehe Seite 335)
7. [Legen Sie für die Mandantenfähigkeits-Option die Einstellung "on" fest](#). (siehe Seite 329)

Starten Sie nach Auswahl dieser Option die Services neu, und führen Sie die folgenden Schritte aus:

- a. Melden Sie sich mit dem Anmeldenamen des Anwenders mit Administratorrechten an (in der Regel *ServiceDesk*).
- b. Überprüfen Sie, ob der berechnete Anwender dem Service Provider-Mandanten zugewiesen ist.
- c. Überprüfen Sie, ob Ihre Mandantenfähigkeits-Einschränkungen durchgesetzt wurden.

Wichtig! Wenn Daten ohne Mandanten in der Datenbank bleiben, können Sie das Erzwingen mehrerer Mandanten auf *Warnen* oder *Zulassen* setzen. Dadurch werden Aktualisierungen von mandantenabhängigen Tabellen mit null Mandanten ermöglicht. Dies verhindert den Verlust von Daten, falls ein Service Level Agreement (SLA) oder ein angehängtes Ereignis für ein Ticket ausgeführt wird, das noch nicht dahingehend aktualisiert wurde, dass es einen Mandanten enthält.

Hinweis: Sie können "pdm_settenant" selbst nach Aktivierung der Mandantenfähigkeit ausführen, einmal um die Vollständigkeit der Implementierung zu überwachen (mit der Option "-r"), und ggf. zur Massenaktualisierung des Mandanten.

8. Erstellen Sie eine Sicherungskopie von Datenaufteilungsbedingungen und Rollen.

Durch Mandantenfähigkeit wird sowohl die Zahl als auch die Komplexität der erforderlichen Datenaufteilungsbedingungen verringert, die daher vereinfacht werden können. Fertigen Sie vor dem Durchführen von Änderungen eine Sicherungskopie der Tabellen "Domain_Constraint" und "usp_role" an.

9. Entfernen Sie nicht benötigte Datenaufteilungsbedingungen.

Viele Domänenbedingungen, die für einzelne Mandanten definiert wurden, sind nach der Aktivierung der Mandantenfähigkeit nicht länger erforderlich und können entfernt werden. Durch Entfernung dieser zusätzlichen Bedingungen wird die Abfrageleistung verbessert.

10. Führen Sie eine Überprüfung und ein Audit aus.

Führen Sie `pdm_settenant -r` aus, um zu überprüfen, ob Bedarf an zusätzlicher Mandantenbefüllung in mandantenabhängigen Tabellen besteht. Überprüfen Sie, ob Tabellen, in denen Mandanten optional sind, Mandanten hinzugefügt werden müssen (z. B. "Kategorie" und "Aktivitätsbenachrichtigung").

11. (Optional) Deaktivieren Sie die Mandantenfähigkeit, wenn Probleme auftreten. Wenn nach der Implementierung Probleme auftreten, können Sie die folgenden Schritte ausführen:

- a. Stellen Sie die Tabellen "Domain_Constraint" und "usp_role" wieder her.
- b. Legen Sie für die Mandantenfähigkeits-Option wieder die Option "Setup" fest.
- c. Führen Sie eine Zurückführung des Systems durch.

Am Standort können die vorherigen Vorgänge wieder aufgenommen werden, während Sie mit dem Füllen der Mandantenspalten fortfahren und ggf. Probleme korrigieren.

Hinweis: Wenn mandantenabhängige Tabellen in einem mandantenfähigen System fälschlicherweise Daten ohne Mandanten enthalten, wird eine Dropdownliste mit öffentlichen Daten eingeblendet und folgende Meldung angezeigt: "AHD05358 *nn* aktive xxx-Objekte ohne Mandant waren beim Start von Service Desk vorhanden."

Mehrere Mandanten

Mehrere Mandanten ermöglichen es, dass mehrere unabhängige Clients (*Mandanten*) und ihre Anwender eine einzelne Implementierung des Produkts gemeinsam nutzen. Mandanten nutzen Hardware- und Anwendungsressourcen gemeinsam, wodurch die Kosten für beide reduziert werden.

Mandantenanwender interagieren nur auf definierte Art und Weise miteinander, wie durch ihre *Rollen* und *Mandantenhierarchien* angegeben.

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

- **Mandantenhierarchie:** 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.

Normalerweise zeigt jeder Mandant die Implementierung ausschließlich für die eigene Verwendung an. Jeder Mandant kann die Daten eines anderen Mandanten nicht aktualisieren oder anzeigen.

Der Service Provider-Mandant

Ein *Service Provider* stellt Services für andere Entitäten bereit. In einer Implementierung für mehrere Mandanten ist der Service Provider der primäre Mandant (Eigentümer) und verwaltet andere Mandanten.

Der Mandant "Service Provider" kann eine der folgenden Aufgaben ausführen:

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

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 höheren Mandanten (falls vorhanden) innerhalb dieser Hierarchie. Ein *übergeordneter Mandant* ist ein Mandant, der über einem anderen Mandanten (der zugehörige *untergeordnete Mandant*) in der gleichen Mandantenhierarchie liegt. 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.

Das Produkt 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. Der Service Provider kann optional den Mandantenhierarchien angehören. Der Service Provider kann keinen übergeordneten Mandanten haben.

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

Mandantenattribute und Objekte

Wenn Sie die Option "Mehrere Mandanten" aktivieren, können Sie jedem Kontakt (Anwender) Zugriff auf alle Mandanten (öffentlich), einen einzelnen Mandanten oder eine Gruppe von Mandanten (anwenderspezifisch oder systemverwaltet) gewähren. Die Rolle für einen Kontakt steuert den Zugriff, der Lese- und Schreibzugriff unabhängig angibt. Da der Mandantenzugriff rollenabhängig ist und ein Kontakt während einer Sitzung verschiedene Rollen einnehmen kann, kann sich der Kontaktmandantenzugriff auch ändern.

Wenn die Implementierung für mehrere Mandanten installiert wird, schließen die meisten Datenobjekte 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. Das Produkt setzt diese Beschränkung durch, nicht das Datenbank-Management-System. Alle Daten in diesen Objekten sind mit individuellen Mandanten verbunden. Es gibt keine öffentlichen Daten.

Beispiele: Tickettabellen (Request, Issue und Change)

Mandant optional

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

Beispiele: Kategorie und Lokation

Multi-Tenancy Access

Wenn ein Anwender die Datenbank abfragt, beschränkt das Produkt die Ergebnisse auf Datenobjekte, auf die der Anwender zugreifen darf. Diese Beschränkung gilt zusätzlich zu den geltenden Beschränkungen in Bezug Datenpartitionen. Den Anwendern werden nur Daten in mandantenabhängigen und mandantenoptionalen Tabellen angezeigt, und es werden nur Daten angezeigt, die den Mandanten gehören, auf die sie zugreifen dürfen.

Wenn ein Mandantenanwender ein Datenbankobjekt erstellen oder aktualisieren möchte, überprüft das Produkt Folgendes:

- Es wird überprüft, ob das Objekt einem Mandanten gehört, der die aktuelle Rolle für den Anwender aktualisieren darf.
- Es wird überprüft, ob alle Fremdschlüssel-Referenzen (SREL) vom Objekt zu anderen Objekten folgende sind:
 - Öffentliche Objekte (ohne Mandant)
 - Objekte vom gleichen Mandanten
 - Objekte von Mandanten in der Mandantenhierarchie über dem Objekt des Mandanten. Das heißt, Ein Mandantenobjekt darf sich auf solche Objekte beziehen, die sich auf seinen übergeordneten Mandanten beziehen, auf dessen übergeordneten Mandanten usw.

Hinweis: Es ist eine Ausnahme zur Einschränkung der SREL-Referenzen vorhanden. Manche SREL-Referenzen (wie z. B. der Zuständige eines Incidents) können auf Objekte verweisen, die zu Mandanten in der Mandantenhierarchie ihres Objekts gehören. Solche Referenzen werden im Objektschema des Produkts 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 Objekt des Mandanten befindet. Wenn sich der Service Provider-Mandant in der Hierarchie befindet, erlauben die Mandantenvalidierungsregeln das Erstellen von Service Provider-Referenzen.

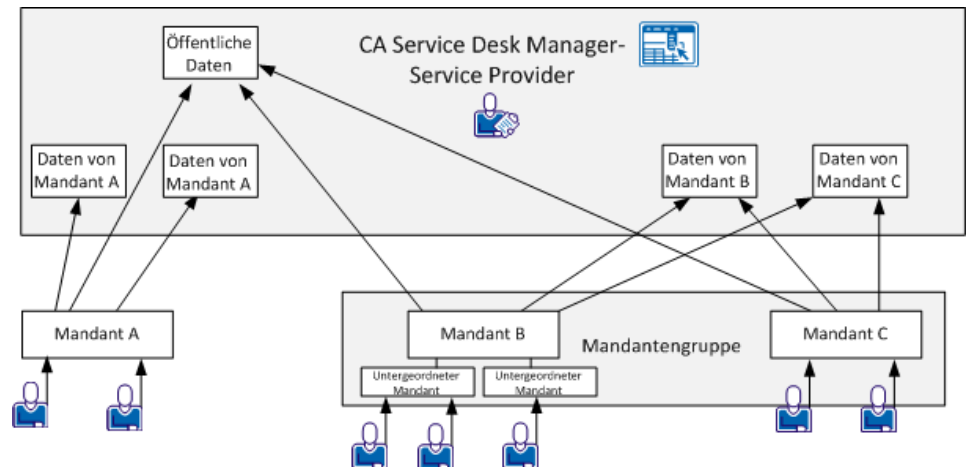
Wenn ein Anwender, der ein Objekt erstellt, Aktualisierungszugriff auf mehrfache Mandanten hat, muss der Anwender den Mandanten explizit angeben, entweder direkt oder indirekt.

Ein Service Provider-Anwender, der darum bittet, ein Objekt zu erstellen oder zu aktualisieren, unterliegt den gleichen Beschränkungen wie Mandantenanwender. Eine Ausnahme ist, dass es Service Provider-Anwendern genehmigt werden kann, öffentliche Objekte zu erstellen oder zu aktualisieren. Die aktive Rolle des Service Provider-Anwender steuert diese Autorisierung.

Hinweis: Wenn das Produkt einen Anwender 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.

Beispiel: Mandantenzugriff auf CA SDM-Daten

Dieses Beispiel zeigt, wie Mandant A, Mandant B und Mandant C auf ihre eigenen und öffentlichen Daten in CA SDM zugreifen.



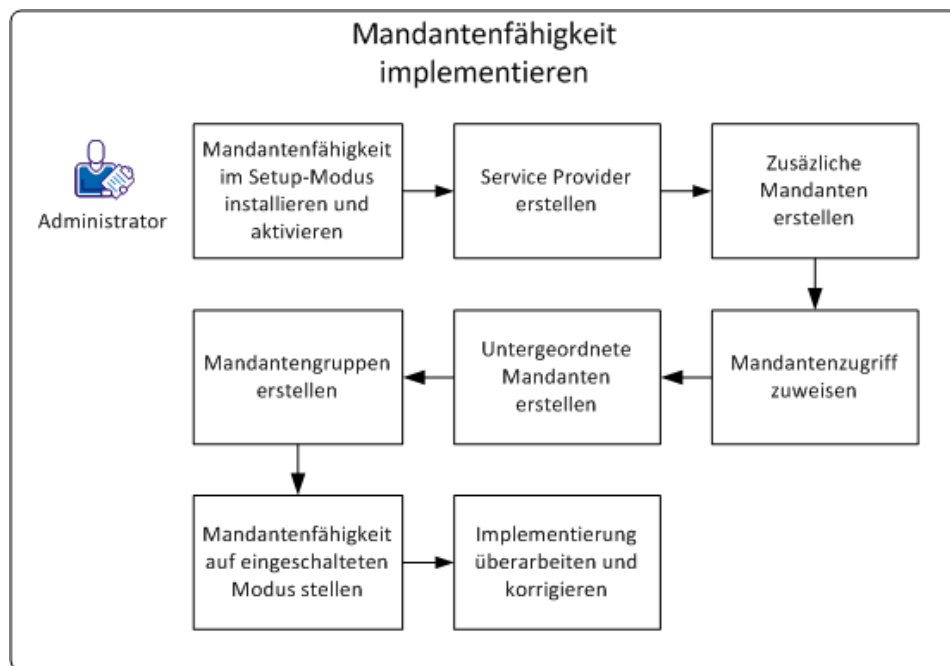
Im Beispiel verweisen die Pfeile auf Daten, auf die jeder Mandant folgendermaßen zugreifen kann:

- Mandant A-Anwender können auf die Daten von Mandant A und auf öffentliche Daten zugreifen.
- Mandant B und seine untergeordneten Mandantenanwender können auf Daten von Mandant B und auf öffentliche Daten zugreifen.
- Mandant C-Anwender können auf die Daten von Mandant C und auf öffentliche Daten zugreifen.
- Weil Mandant B, seine untergeordneten Mandanten und Mandant C zu einer Mandantengruppe gehören, können Anwender Mandant B, Mandant C und öffentlich Daten anzeigen.

Implementieren der Mandantenfähigkeit

Das folgende Diagramm beschreibt, wie ein Administrator als berechtigter CA SDM-Anwender das erste Mal mehrere Mandanten implementiert. Von Start bis zum Ende ändert sich die CA SDM-Implementierung folgendermaßen:

1. Ein einzelner Client verwendet eine einzelne Implementierung.
2. Mehrere unabhängige Clients (Mandanten) und ihre Anwender nutzen eine einzelne Implementierung *gemeinsam*. Jedem Mandanten wird die Implementierung ausschließlich für die eigene Verwendung angezeigt.



Als Administrator verwenden Sie die CA SDM-Administrationsschnittstelle, um diese Schritte auszuführen:

1. [Installieren und Aktivieren von mehreren Mandanten im Setup-Modus](#) (siehe Seite 317).
2. [Erstellen eines Service Provider-Mandanten](#) (siehe Seite 318).
3. [Erstellen von zusätzlichen Mandanten](#) (siehe Seite 320).
4. [Zuweisen des Mandantenzugriffs für eine Rolle](#) (siehe Seite 322).
5. [Erstellen von untergeordneten Mandanten](#) (siehe Seite 324).
6. [Erstellen von Mandantengruppen](#) (siehe Seite 325).
7. [Ändern von mehreren Mandanten in den "an"-Modus](#) (siehe Seite 327) und Neustarten von Services.
8. [Überprüfen der Implementierung und Beheben](#) (siehe Seite 328) von Problemen.

Installieren und Aktivieren von mehreren Mandanten

Sie aktivieren mehrere Mandanten, indem Sie eine Option für mehrere Mandanten im Produkt installieren und anschließend den Setup-Modus aktivieren. Der Setup-Modus gibt an, dass die Funktionen für mehrere Mandanten für Administratoren gelten. Dieser Modus ermöglicht es Ihnen, mandantenbezogene Objekte und Attribute anzuzeigen und zu bearbeiten. Das Produkt setzt allerdings keine Mandantenbeschränkung durch, und Anwender ohne Administratorrechte sehen keine Änderungen. Mit diesem Modus können Sie mehrere Mandanten vorbereiten, indem Sie Aufgaben ausführen, wie z. B. Mandanten definieren oder Mandanten zu Rollen zuzuweisen, ohne dabei den normalen Gebrauch des Produkts zu beeinträchtigen.

Wichtig! Wenn sich mehrere Mandanten im Setup-Modus befinden, sind Web-Schnittstellenänderungen für Service Provider-Administratoren aktiv. Dieses Verhalten ermöglicht es Ihnen, mandantenbezogene Objekte und Daten auf der Web-Schnittstelle anzuzeigen und zu bearbeiten. Einschränkungen der Mandantenfähigkeit werden jedoch nicht durchgesetzt, und andere Anwender (außer Service Provider-Administratoren) können Änderungen der Produktschnittstelle nicht sehen. Deswegen können Sie das Produkt weiterhin verwenden, während Sie mehrere Mandanten implementieren.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei CA SDM als Administrator an, und klicken Sie auf die Registerkarte "Administration".
2. Klicken Sie in der Baumstruktur auf der linken Seite auf "Optionsmanager" > "Mandantenfähigkeit".
Die Seite "Option - Liste" wird geöffnet.
3. Klicken Sie auf "Mandantenfähigkeit".
Die Seite mit den Optionsdetails zur Mandantenfähigkeit wird angezeigt.
4. Klicken Sie auf "Bearbeiten".
Die Seite "Optionen aktualisieren" wird angezeigt.
5. Wählen Sie "Setup" aus der Drop-Down-Liste "Optionswert" aus.
6. Klicken Sie auf "Installieren".
Die Option "Mandantenfähigkeit" wird jetzt installiert.
7. Klicken Sie auf "Aktualisieren".
Die Seite zeigt Ihre Änderungen.
8. Schließen Sie das Fenster.
Die Seite "Optionen – Liste" wird wieder angezeigt.
9. Starten Sie die Dienste neu.
Mehrere Mandanten können nun im Setup-Modus implementiert werden.

Erstellen eines Service Provider-Mandanten

Sie verwenden das Produkt, um den Service Provider-Mandanten zu erstellen. Wenn Sie den ersten Mandanten erstellen, tritt Folgendes ein:

1. Der erste Mandant wird immer der Service Provider.

Wichtig! Sie können diese Zuordnung nicht ändern: Auf der Seite "Neuen Mandanten erstellen" sind das Kontrollkästchen "Service Provider" und das Feld "Datensatzstatus" schreibgeschützt.

2. Das Produkt ordnet den privilegierten Anwender (normalerweise "ServiceDesk" unter Windows oder "srvcdesk" unter Linux/UNIX) dem Mandanten "Service Provider" zu. Das Produkt legt alle Systemkontakte (wie z. B. System_AHD_Generated) fest, die dem neuen Service Provider-Mandanten angehören.

Hinweis: Windows gibt einen Administrator-Systemanwender an. Der privilegierte Anwender muss dem Administratoranwender einen Mandanten manuell zuweisen.

Gehen Sie wie folgt vor:

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 mehrere Mandanten im Setup- oder im an-Modus installiert sind.

2. Klicken Sie auf "Neu erstellen".

Die Seite "Neuer Mandant" wird angezeigt.

3. Füllen Sie die folgenden Felder aus:

Name

Zeigt den Namen des Mandanten an.

Service Provider

Gibt an, dass dieser Mandant der Service Provider ist.

Mandantennummer

(Nur zur Information) Zeigt die Mandantennummer an. CA SDM verwendet diese Option nicht.

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, in der Sie eine Lokation angeben können.

Kontakt

Zeigt die Seite zur Suche von Kontakten an, in der Sie einen Kontakt angeben können.

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".

Das Produkt erstellt den Service Provider-Mandanten.

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 Service Provider-Mandanten an.
7. Melden Sie sich bei CA SDM ab.

Erstellen von Mandanten

Sie verwenden das Produkt, um zusätzliche Mandanten zu erstellen. Sie können beliebig viele Mandanten erstellen, um mehrere getrennte Unternehmen zu verwalten, die Clients unterstützen.

Gehen Sie wie folgt vor:

1. Melden Sie in der Administratorschnittstelle als Service Provider-Mitglied an. Eine einfache Möglichkeit für diese Anmeldung ist das Anmelden als berechtigter Anwender (zum Beispiel "ServiceDesk"). Dieser Anwender gehört automatisch zum Service Provider-Mandanten.

2. 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 mehrere Mandanten im Setup- oder im an-Modus installiert sind.

3. Klicken Sie auf "Neu erstellen".

Die Seite "Neuer Mandant" wird angezeigt.

4. Füllen Sie die Felder wie folgt aus:

Name

Zeigt den Namen des Mandanten an.

Service Provider

Gibt an, ob der Mandant ein Service Provider ist. Der erste erstellte Mandant ist immer der Service Provider. Danach ist dieses Kontrollkästchen schreibgeschützt.

Mandantennummer

(Nur zur Information) Zeigt die Mandantennummer an. CA SDM verwendet diese Option nicht.

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, in der Sie eine Lokation angeben können.

Kontakt

Zeigt die Seite zur Suche von Kontakten an, in der Sie einen Kontakt angeben können.

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

5. Klicken Sie auf "Speichern".

Das Produkt erstellt den Mandanten.

6. Schließen Sie das Fenster.

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

Die Mandantenliste wird aktualisiert und zeigt den erstellten Mandanten an.

8. (Optional) Wiederholen Sie die Schritte 3 bis 6 für jeden Mandanten, den Sie erstellen möchten.

Zuweisen des Mandantenzugriffs für eine Rolle

Die Rolle eines CA SDM-Anwenders bestimmt sowohl die Zugriffsautorisierung als auch die Anwenderschnittstelle. Die Rollen, die Anwendern zur Verfügung stehen, hängen von deren Zugriffstyp ab. Mit Mandantenfähigkeit können Sie den Mandanten oder die Mandantengruppe steuern, auf die ein Anwender innerhalb der Rolle zugreifen darf. Wenn mehrere Mandanten installiert sind, enthält die Seite "Rolle - Detail" zusätzliche Optionen, mit denen Sie den Mandantenzugriff zuweisen oder bearbeiten können.

Hinweis: Sie können Mandantenanwendern auch den Zugriff auf Daten von anderen gewähren. Mandanten-Analysten, die keine Service Provider sind, haben nur Zugriff auf ihre eigenen und auf untergeordnete Mandanten. Allerdings können Sie ihren Funktionszugriff aktualisieren, um den Mandanten des Analysten einzuschließen. Zum Beispiel können Sie eine Rolle definieren, um separaten Schreib- und Lesezugriff auf bestimmte Mandantengruppen für Anwender innerhalb dieser Rolle festzulegen.

Gehen Sie wie folgt vor:

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

Die Rollenliste wird angezeigt.

2. Klicken Sie auf die Rolle, für die Sie den Mandantenzugriff zuweisen möchten.

Die Seite "Rolle - Detail" wird angezeigt und verfügt über die Drop-down-Listen "Mandantenzugriff" und "Mandanten-Schreibzugriff" auf der Registerkarte "Autorisierung". "Mandantenzugriff" ist schreibgeschützt, und "Mandanten-Schreibzugriff" ermöglicht zusätzlich die Erstellung und Aktualisierung.

3. Klicken Sie auf "Bearbeiten".

Die Seite "Rolle aktualisieren" wird angezeigt.

4. Wählen Sie die Optionen für "Mandantenzugriff" und "Mandanten-Schreibzugriff" aus:

Gleich dem Mandantenzugriff

Legt fest, dass der Zugriff und die Einstellung "Mandantenzugriff" identisch sind. Dieser Wert ist der Standardwert für die Drop-down-Liste "Mandanten-Schreibzugriff" und ist nur für die Option "Mandanten-Schreibzugriff" verfügbar.

Alle Mandanten

Entfernt Mandanteneinschränkungen. Ein Anwender in einer Rolle mit diesem Zugriff kann folgende Aktionen durchführen:

- Anzeigen von Objekten in der Datenbank an (Lesezugriff).
- Erstellen und Aktualisieren (Schreibzugriff) von Mandantenobjekten in der Datenbank.

Wenn ein Anwender mit dem Zugriff "Alle Mandanten" ein Objekt erstellt, muss der Anwender den Mandanten des neuen Objekts auswählen.

Einzelner Mandant

Legt den Mandantenzugriff für eine Rolle auf einen genannten Mandanten fest. Wenn Sie diese Option auswählen, wird ein anderes Feld angezeigt, mit dem Sie einen bestimmten Mandanten auswählen können. Ein Anwender in dieser Rolle kann nur auf die Objekte zugreifen, die dem genannten Mandanten zugeordnet sind.

Mandantengruppe

Legt den Mandantenzugriff einer Rolle auf eine anwenderspezifische oder vom System gepflegte Mandantengruppe fest. Nachdem Sie diese Option auswählen, wird ein anderes Feld angezeigt, mit dem Sie eine bestimmte Mandantengruppe auswählen können. Ein Anwender in dieser Rolle kann nur auf die Objekte zugreifen, die einem Mandanten in dieser Gruppe zugeordnet sind. Wenn ein Anwender mit dem Zugriff "Mandantengruppe" ein Objekt erstellt, muss der Anwender den Mandanten für das neue Objekt auswählen.

Mandant des Kontakts

Legt den Mandantenzugriff einer Rolle auf den Mandanten des benutzenden Kontakts fest. Ein Anwender in dieser Rolle kann nur auf die Objekte zugreifen, die dem eigenen Mandanten zugeordnet sind.

Mandantengruppe des Kontakts

Legt den Rollenzugriff für eine Analystenrolle auf die Mandantengruppe fest, mit der der Analyst arbeitet, wie auf dem Kontaktdatensatz für den Analysten angegeben. Wenn der Anwender mit der Rolle kein Analyst ist, hat diese Auswahl die gleiche Wirkung wie Mandant des Kontakts. Diese Option steht nur für Analysten zur Verfügung.

Untergeordnete Mandantengruppe des Kontakts

Legt den Mandantenzugriff einer Rolle auf die untergeordnete Mandantengruppe des benutzenden Kontakts fest. Ein Anwender in dieser Rolle kann nur auf die Objekte zugreifen, die der eigenen untergeordneten Mandantengruppe zugeordnet sind.

Untergeordnete Mandantengruppe des Kontakts

Legt den Mandantenzugriff einer Rolle auf die übergeordnete Mandantengruppe des benutzenden Kontakts fest. Ein Anwender in dieser Rolle kann nur auf die Objekte zugreifen, die der eigenen übergeordneten Mandantengruppe zugeordnet sind.

Verwandte Mandantengruppe des Kontakts

Legt den Mandantenzugriff einer Rolle auf die verwandte Mandantengruppe des benutzenden Kontakts fest. Ein Anwender in dieser Rolle kann nur auf die Objekte zugreifen, die der eigenen verwandten Mandantengruppe zugeordnet sind.

'Öffentlich' aktualisieren?

Diese Option steuert, ob ein Anwender des Service Providers in der Rolle öffentliche Daten erstellen oder aktualisieren darf. Alle Anwender können öffentliche Daten anzeigen, unabhängig von den Zugriffsrechten für die aktuelle Rolle. Mandantenanwender (Anwender, die einem anderen Mandanten angehören als dem Service Provider) können unabhängig von ihrer Rolle keine öffentlichen Daten aktualisieren.

Klicken Sie auf "Speichern".

Mandantenzugriff ist für die Rolle zugewiesen. Wenn ein Anwender die Datenbank abfragt, schränkt das Produkt die Ergebnisse auf Objekte ein, die zu Mandanten gehören, die der Rolle des Anwenders zugeordnet sind.

Erstellen von untergeordneten Mandanten

Untergeordnete Mandanten ermöglichen Ihnen das Definieren und Ändern von Mandantenstrukturen zu organisatorischen Zwecken und zur gemeinsamen Datenverwendung. Um einen Mandanten in eine Mandantenstruktur aufzunehmen, weisen Sie den Mandanten einen übergeordneten Mandanten zu.

Gehen Sie wie folgt vor:

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

Die Mandantenliste wird angezeigt.

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

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

Die Seite "Mandant - Detail" wird angezeigt, auf der Sie erforderliche Daten oder Änderungen eingeben können.

3. Wählen Sie einen übergeordneten Mandanten aus.

Hinweis: Die Drop-down-Liste "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 der untergeordneten Mandantengruppe des übergeordneten Mandanten an. Der übergeordnete Mandant verbindet sich mit der übergeordneten Mandantengruppe des untergeordneten Mandanten. Alle Mandanten verbinden sich mit der verwandten Mandantengruppe des anderen Mandanten.

Erstellen von Mandantengruppen

Eine Mandantengruppe ist eine Sammlung von Mandanten, die den Zugriff auf CA SDM-Objekte gemeinsam nutzen. Mandantengruppen ermöglichen es Ihnen, den Zugriff auf Mandanten zu klassifizieren, zu verwalten und zu steuern. Sie können eine Rolle einem Mandanten oder einer Mandantengruppe zuweisen. Wenn mehrere Mandanten aktiv sind, ordnet das Produkt jede Rolle zu mit: alle Mandanten (Öffentlich), einem einzelnen Mandanten oder einer einzelnen Mandantengruppe. Verwenden Sie Mandantengruppen, wenn eine Rolle den Zugriff auf mehr als einen Mandanten benötigt. Zum Beispiel können Sie Analysten zu einer Mandantengruppe zuweisen, die Mandanten enthält, die zu einer bestimmten geografischen Lokation gehören.

Das Produkt 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)

Sie verwenden systemverwaltete Mandantengruppen, wie z. B. anwenderspezifische Mandantengruppen. Allerdings können Sie nur die Namen und Beschreibungen der systemverwalteten Mandantengruppen ändern.

Beispiel: Eine Rolle benötigt den Zugriff auf Mandant A, Mandant B und Mandant J

Anstatt jedem Mandanten die Rolle separat zuzuweisen, können Sie folgendermaßen vorgehen:

1. Erstellen Sie eine Mandantengruppe, und fügen Sie Mandant A, Mandant B und Mandant J zu der Gruppe hinzu.
2. Weisen Sie Rolle A dieser Mandantengruppe zu.

Anwender (Kontakte), die der Rolle A zugewiesen sind, können auf die Mandantengruppe zugreifen, die aus den Mandanten A, B und J besteht.

Gehen Sie wie folgt vor:

1. Melden Sie sich als Service Provider an, klicken Sie auf die Registerkarte "Administration", und wählen Sie "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", und fügen Sie der Gruppe Mandantenmitglieder hinzu.
9. (Optional) Wiederholen Sie die Schritte 3 bis 6 für jede Mandantengruppe, die Sie erstellen möchten.

Ändern von mehreren Mandanten in den "an"-Modus

Sie ändern die Option "Mehrere Mandanten" in den "an"-Modus, um die Implementierungsfunktion für mehrere Mandanten zu vervollständigen. Jeder Mandant zeigt dann die Implementierung ausschließlich für die eigene Verwendung an. Jeder Mandant kann die Daten eines anderen Mandanten nicht aktualisieren oder anzeigen.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei CA SDM als Administrator an, und klicken Sie auf die Registerkarte "Administration".
2. Klicken Sie in der Baumstruktur auf der linken Seite auf "Optionsmanager" > "Mandantenfähigkeit".
Die Seite "Option - Liste" wird geöffnet.
3. Klicken Sie auf "Mandantenfähigkeit".
Die Seite mit den Optionsdetails zur Mandantenfähigkeit wird angezeigt.
4. Klicken Sie auf "Bearbeiten".
Die Seite "Optionen aktualisieren" wird angezeigt.
5. Wählen Sie "Setup" aus der Drop-Down-Liste "Optionswert" aus.
6. Klicken Sie auf "Bearbeiten".
Die Seite "Optionen aktualisieren" wird angezeigt.
7. Wählen Sie "an" (der Standard) aus den folgenden Werten in der Drop-Down-Liste "Optionswert" aus:

ein

(Standard) Deaktiviert das Einchecken in eine mandantenabhängige Tabelle, wenn der Mandant ungültig ist und eine SREL zu einer Tabelle mit einem Mandanten nicht verfügbar ist.

an(Warnung)

Protokolliert einen Fehler, lässt jedoch das Einchecken zu, wenn ein mandantenabhängiges Objekt mit einem ungültigen Mandanten erstellt oder aktualisiert wird.

an(erlauben)

Protokolliert eine Warnung, lässt jedoch das Einchecken zu, wenn ein mandantenabhängiges Objekt mit einem ungültigen Mandanten erstellt oder aktualisiert wird.

8. Klicken Sie auf "Speichern" und anschließend auf "Aktualisieren".

Die Seite zeigt Ihre Änderungen.

9. Schließen Sie das Fenster.

Die Seite "Optionen – Liste" wird wieder angezeigt.

10. Starten Sie die Dienste neu.

Mehrere Mandanten sind nun voll funktionsfähig.

Überprüfen und Korrigieren der Implementierung

Überprüfen der Implementierung von mehreren Mandanten und Beheben von Problemen.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei CA SDM mit dem Anmeldenamen des Anwenders mit Administratorrechten an (in der Regel ServiceDesk).
2. Klicken Sie auf die Registerkarte "Administration", und navigieren Sie zur Mandantenliste.

Der Provider zeigt für den berechtigten Anwender im Mandantennamen "Ja" an.

3. Stellen Sie sicher, dass Ihre Einschränkungen von mehreren Mandanten durchgesetzt werden, indem Sie zu einer Kontaktliste navigieren.

Wenn mandantenabhängige Tabellen fälschlicherweise Daten ohne Mandanten in einem System mit mehreren Mandanten enthalten, wird folgende Meldung in der Kontaktliste angezeigt:

AHD05358 nn aktive Kontaktobjekte ohne Mandant waren beim Start von Service Desk vorhanden.

Wichtig! Wenn sich Daten ohne Mandanten in der Datenbank befinden, können Sie die Option für mehrere Mandanten auf "an(Warnung)" oder "an(erlauben)" festlegen. Mit diesen Modi können Sie mandantenabhängige Tabellen mit einem ungültigen Mandanten aktualisieren. Diese Methode verhindert Datenverlust, wenn ein Service Level Agreement (SLA) oder ein angehängtes Event für ein Ticket ausgeführt wird, das keinen Mandanten enthält.

4. (Optional) Deaktivieren Sie mehrere Mandanten, wenn Probleme auftreten, und führen Sie folgende Schritte aus:
 - a. Stellen Sie die Tabellen "Domain_Constraint" und "usp_role" wieder her.
 - b. Legen Sie die Option "Mehrere Mandanten" in den Setup-Modus fest.
 - c. Führen Sie eine Zurückführung des Systems durch.

Am Standort können vorherige Vorgänge wieder aufgenommen werden, während Sie beliebige Issues korrigieren.

Aktivieren von Multi-Tenancy

Mit diesem Produkt können Sie die Mandantenfähigkeit aktivieren.

So aktivieren Sie die Mandantenfähigkeit:

1. Klicken Sie auf die Registerkarte "Administration".
2. Klicken Sie in der Baumstruktur auf der linken Seite auf "Optionsmanager" > "Mandantenfähigkeit".

Die Seite "Option - Liste" wird geöffnet.
3. Klicken Sie auf "Mandantenfähigkeit".

Die Seite mit den Optionsdetails zur Mandantenfähigkeit wird angezeigt.
4. Klicken Sie auf "Bearbeiten".

Die Seite "Optionen aktualisieren" wird angezeigt.
5. Wählen Sie in der Dropdownliste "Optionswert" *eine* der folgenden Optionen aus:

aus

Deaktiviert die Funktion der Mandantenfähigkeit.

Setup

Aktiviert die Mandantenfähigkeit im Setup-Modus. In diesem Modus zeigt CA SDM bearbeitbare mandantenbezogene Objekte und Attribute für Administratoren von Service Providern. Es werden jedoch keine Anforderungen für mehrere Mandanten erzwungen. Andere Benutzer können mit ihrer Arbeit fortfahren, als ob Mandantenfähigkeit nicht installiert wurde.

ein

Aktiviert die Mandantenfähigkeiten-Option in vollem Funktionsumfang.
Folgende Optionen stehen zur Auswahl:

- **strict:** (Standardwert) CA SDM kann das Einchecken in eine mandantenabhängige Tabelle nicht ausführen, wenn der Mandant null ist und das Produkt ihn nicht standardmäßig aus einer SREL in eine Tabelle mit Mandanten übernehmen kann.
- **warn:** CA SDM protokolliert einen Fehler, lässt jedoch das Einchecken zu, wenn ein mandantenabhängiges Objekt mit einem ungültigen Mandanten erstellt oder aktualisiert wird.
- **allow:** CA SDM protokolliert eine Warnung, lässt jedoch das Einchecken zu, wenn ein mandantenabhängiges Objekt mit einem ungültigen Mandanten erstellt oder aktualisiert wird.

Hinweis: Wenn Sie die Tabelle "ca_tenant" noch nicht mit Daten gefüllt haben, wählen Sie "Setup" aus der Dropdownliste "Optionswert" aus. Wenn Sie die Mandantenfähigkeit neu implementieren möchten, wählen Sie "Setup".

6. Klicken Sie auf "Installieren".

Die Option "Mandantenfähigkeit" wird jetzt installiert.

7. Klicken Sie auf "Aktualisieren".

Die Seite zeigt Ihre Änderungen.

8. Schließen Sie das Fenster.

Die Seite "Optionen – Liste" wird wieder angezeigt.

9. Starten Sie die Dienste neu.

Initialisieren eines neuen Mandanten

Als Service Provider möchten Sie für einen neuen Mandanten vielleicht Standarddatensätze wie Kategorien, Datenpartitionen, Ticket-Vorlagen usw. erstellen. Diese Aufgabe wird in einer "pdm_userload"-Eingabedatei durchgeführt, die Sie mit "pdm_extract" oder "pdm_tenant_extract" erstellen und die gewünschten Daten enthält.

Gegebenenfalls können Sie diese Datei mit einem beliebigen Texteditor bearbeiten. Sie kann dann mit "pdm_userload" und dem Argument "-t" in die Datenbank geladen werden. Die Spalte "Mandant" wird dadurch auf den neuen Mandanten gesetzt. Informationen zu weiteren Argumenten von "pdm_userload" finden Sie im *Administrationshandbuch*.

So initialisieren Sie einen neuen Mandanten:

1. Erstellen Sie den Mandanten in der Tabelle "ca_tenant".
Verwenden Sie dazu die Online-Seite [Mandant erstellen](#) (siehe Seite 333).
2. Laden Sie die Standarddaten wie zuvor beschrieben.
Legen Sie mit "pdm_userload -t" den Mandanten fest.
3. Erstellen Sie Kontaktdatensätze für den neuen Mandanten.
Laden Sie externe Daten, oder verwenden Sie "pdm_userload -t".

Konvertieren einer vorhandenen Mandanten-Implementierung in das Mandantenobjekt

Möglicherweise haben Sie für einige Funktionen bisher Datenpartitionen und ein anderes CA SDM-Objekt verwendet. Nun wird diese Funktionalität durch die Mandantenfähigkeit bereitgestellt. Wenn Sie eine Implementierung für mehrere Mandanten bereitstellen wollen, müssen Sie in einem ersten Schritt die Daten in dem zuvor verwendeten Objekt dem neuen Mandantenobjekt zuordnen. Das zuvor verwendete Objekt wird als *vorgeordnetes* Objekt bezeichnet. Für die meisten Standorte mit diesen Anforderungen ist das org-Objekt (Organisation) das vorgeordnete Mandantenobjekt, doch der nachfolgende Ansatz gilt für alle vorgeordneten Mandantenobjekte.

1. Handelt es sich bei dem vorgeordneten Objekt nicht um "org", überprüfen Sie, ob in der Objektdefinition "Majic" TENANT_REQUIRED angegeben ist.
2. Überprüfen Sie die Attributzuordnungen vom vorgeordneten Mandantenobjekt zum neuen Mandantenobjekt in der Datei "buildtenant.xml" im folgenden Verzeichnis:

\$NX_ROOT/samples/multi_tenancy

Hinweis: Sie müssen "buildtenant.xml" in das Verzeichnis "\$NX_ROOT/site/cfg" kopieren. Darüber hinaus muss sich "buildtenant.xsd" im selben Verzeichnis befinden wie "buildtenant.xml", anderenfalls erhalten Sie einen Fehler. Wenn Sie das Produkt installieren, befindet sich "buildtenant.xsd" im Verzeichnis "\$NX_ROOT/site/cfg", so dass Sie diese Datei nicht kopieren müssen.

Die Standardeinstellungen basieren auf "org". Wenn das vorgeordnete Mandantenobjekt nicht "org" lautet, müssen Sie die Datei bearbeiten.

3. [Führen Sie pdm_buildtenant -f aus](#) (siehe Seite 341).
Für jedes vorgeordnete Mandantenobjekt wird ein neuer Mandant erstellt und das Attribut "Mandant" im Mandantenobjekt verweist dann auf den neuen Mandanten.
4. Melden Sie sich bei CA SDM an, und überprüfen Sie sowohl das Mandantenobjekt als auch das vorgeordnete Mandantenobjekt.

Hinweis: In manchen Fällen werden Sie mehrere vorgeordnete Mandantenobjekte nur einem Mandantenobjekt zuordnen wollen. Dazu aktualisieren Sie die betroffenen vorgeordneten Mandantenobjekte manuell und löschen oder deaktivieren dann die nicht verwendeten Mandanten.

Füllen des Attributs "Mandant" in Tabellen

Das Attribut "Mandant" können Sie in der gesamten Tabelle oder einem Tabellenteil mit dem Dienstprogramm *pdm_settenant* füllen. Dieses Dienstprogramm verwendet eine Konfigurationsdatei, um die mandantenspezifischen Objekte auszuwählen und anzugeben, woher der Mandant für die Objekte stammen soll. Sie können einen bestimmten Mandanten angeben oder bestimmen, dass der Mandant aus einer SREL-Referenz im entsprechenden Objekt abgeleitet werden soll.

So füllen Sie das Attribut "Mandant" in Ihren Tabellen mit "pdm_settenant":

1. Erstellen oder bearbeiten Sie eine Konfigurationsdatei.

Die Konfigurationsdatei wählt die Zeilen für das Attribut "Mandant" aus und gibt eine Quelle für seinen Wert an. Im folgenden Verzeichnis finden Sie eine Beispieldatei für "settenant.xml":

`$NX_ROOT/samples/multi_tenancy`

Hinweis: Sie können die Beispieldatei "settenant.xml" ändern oder eine neue Datei erstellen und in das Verzeichnis "\$NX_ROOT/site/cfg" kopieren. Darüber hinaus muss sich settenant.xsd im selben Verzeichnis befinden wie settenant.xml, anderenfalls erhalten Sie einen Fehler. Wenn Sie das Produkt installieren, befindet sich "settenant.xsd" im Verzeichnis "\$NX_ROOT/site/cfg", so dass Sie diese Datei nicht kopieren müssen.

2. [Führen Sie "pdm_settenant -f \[Konfigurationsdatei\] -r" aus.](#) (siehe Seite 343)

Das Dienstprogramm *pdm_settenant* liest die Konfigurationsdatei und verarbeitet jede definierte Regel nacheinander.

Es wird empfohlen, dass Sie zuerst das Attribut "Mandant" im Objekt "cnt" (Kontakt) mit Hilfe des Dienstprogramms füllen und dann das cnt-Objekt als Quelle zum Füllen des Attributs in anderen Objekten verwenden.

Sobald das cnt-Objekt alle gewünschten Mandanten enthält, dient es als Basis für die Mandanten in anderen Tabellen. Dazu führen Sie die folgenden Schritte aus.

- a. Geben Sie in der Konfigurationsdatei eine Mandantenregel (TenantRule) mit "type=SREL" für ein Attribut ein, das auf das cnt-Objekt verweist, um "Mandant" in anderen Tabellen festzulegen.
 - b. (Optional) Geben Sie eine Mandantenregel (TenantRule) mit "type="Name" <Mandantenname >" an, um "Mandant" nur in bestimmten Tabellen festzulegen.
3. Führen Sie "pdm_settenant" mit einer neuen Konfigurationsdatei aus.
 4. Führen Sie "pdm_settenant" erneut aus, falls erforderlich.

Nachdem Sie die Spalte "Mandant" in einem Objekt gefüllt haben, können Sie SREL für dieses Objekt verwenden. Dieses dient als Basis einer SREL-Mandantenregel, um "Mandant" in anderen Objekten festzulegen.

Beispiel: Syntax für SREL

Die SREL-Syntax sucht nach cnt-Objekten, die keinen Mandantenwert enthalten und verwendet denjenigen aus dem verknüpften org-Objekt:

```
<Object name="cnt">  
<TenantRule type="SREL">organization</TenantRule>  
<Where>tenant is null</Where>  
</Object>
```

Beispiel: Syntax für Name

Die Namensyntax sucht nach org-Objekten, die keinen Mandantenwert enthalten und setzt das Feld "Mandant" auf den Namen eines aktuellen Mandantenobjekts:

```
<Object name="org">  
<TenantRule type="Name">Mandant A</TenantRule>  
<Where>tenant is null</Where>  
</Object>
```

Erstellen eines Mandanten

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

So erstellen Sie einen Mandanten:

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

Die Seite "Mandanten - Liste" wird angezeigt.

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

2. Klicken Sie auf "Neu erstellen".

Die Seite "Neuer Mandant" wird angezeigt.

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

Name

Zeigt den Namen des Mandanten an.

Service Provider

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

Mandantennummer

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

Datensatzstatus

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

Übergeordneter Mandant

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

Untergeordnete Mandanten zulässig

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

Mandantentiefe

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

Übergeordnete Mandantengruppe

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

Untergeordnete Mandantengruppe

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

Fremde Schlüsselgruppe

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

Verwandte Mandantengruppe

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

Nutzungsbedingungen

Legt die Nutzungsbedingungen für den Mandanten fest.

Logo

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

Standort

Zeigt die Seite zur Suche von Lokationen an.

Kontakt

Zeigt die Seite zur Suche von Kontakten an.

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

4. Klicken Sie auf "Speichern".

Der Mandant wurde erstellt.

5. Schließen Sie das Fenster.

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

Die Mandantenliste wird aktualisiert und zeigt den erstellten Mandanten an.

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

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.

Mandantenhierarchien

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

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

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

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

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

Erstellen von untergeordneten Mandanten

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

So erstellen Sie einen untergeordneten Mandanten:

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

Die Mandantenliste wird angezeigt.

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

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

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

3. Wählen Sie einen übergeordneten Mandanten aus.

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

4. Klicken Sie auf "Speichern".

Der Mandant ist ein untergeordneter Mandant des übergeordneten Mandanten.

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

Systemverwaltete Mandantengruppen

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

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

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

Exportieren und Importieren von Mandantendaten

Der Service Provider kann Mandantendaten aus einer vorhandenen Implementierung für mehrere Mandanten extrahieren und in ein neues System importieren.

Hinweis: Abhängig vom Datenvolumen kann der Extrahierungsprozess bis zu einigen Stunden dauern. Die Extrahierungs- und Importschritte müssen Sie eventuell wie folgt in mehreren Phasen durchführen:

Beginn

Es wird ein Basisvolumen extrahiert und eine Kontrolldatei für die nachfolgenden Phasen erstellt.

Update

Anhand der Kontrolldatei werden nur solche Daten extrahiert, die seit der vorherigen Ausführung geändert wurden.

Final

Es werden die gleichen Schritte wie beim Aktualisieren durchgeführt, doch werden außerdem auch Animationen extrahiert. Animationen bleiben in den Anfangs- und Aktualisierungsphasen unberücksichtigt.

So extrahieren Sie Daten aus einer Datenbank und importieren diese in eine andere Datenbank:

1. Führen Sie in der Anfangsphase [pdm_tenant_extract](#) (siehe Seite 347) aus, um die Basisdaten zu extrahieren. Dadurch wird die Kontrolldatei erstellt, die in den nachfolgenden Phasen verwendet wird.
2. Bereiten Sie eine neue, leere MDB für die extrahierten Daten vor.

Wichtig! Das Ergebnis aus der Anfangsphase *muss* in eine Datenbank geladen werden, die zuvor noch nie für das Produkt oder ein anderes Produkt genutzt worden ist. Jede Tabelle, die mit Daten aus der Anfangsphase geladen wird, wird vor dem Laden abgeschnitten. Wenn die Datenbank bereits verwendet wird, könnte dies zu Datenverlust führen.

3. Um zu verhindern, dass Dubletten für berechtigte Kontakte ins neue System gelangen, müssen Sie die berechtigten Kontakte deaktivieren. Melden Sie sich bei CA SDM an, und ändern Sie den Status dieser Kontakte in "Inaktiv", bevor Sie die extrahierten Daten laden.
4. Um Probleme mit Referenzen beim Laden der Daten zu vermeiden, führen Sie das entsprechende Skript zum Entfernen von Einschränkungen aus:
 - (Oracle) Führen Sie Folgendes aus:
\$NX_ROOT/samples/views/Oracle/OracleDropConstraints.sql
 - (SQL Server) Führen Sie Folgendes aus:
\$NX_ROOT/samples/views/SQLServer/SQLDropConstraints.sql
5. Laden Sie die Daten aus der Anfangsphase mit Hilfe von [pdm_userload](#) (siehe Seite 349) in die leere MDB, die Sie in den Schritten 2 und 3 vorbereitet haben.
6. Führen Sie "pdm_tenant_extract" zum Aktualisieren und für die Schlussphase aus, um weitere Daten zu laden, die seit der vorausgegangenen Phase erstellt oder geändert wurden. "Pdm_tenant_extract" verwendet die in Schritt 1 erstellte Kontrolldatei, um die bereits in der vorherigen Phase verarbeiteten Daten zu bestimmen.
7. Laden Sie die in Schritt 5 extrahierten Daten mit "pdm_userload" in dieselbe MDB, die die zuvor geladenen Daten enthält.

Hinweis: Weitere Informationen über dieses Dienstprogramm finden Sie unter [pdm_userload](#) (siehe Seite 349).

8. Wiederholen Sie nach Bedarf die Schritte 5 und 6, bis alle Daten in die neue Datenbank importiert worden sind. Die letzte Ausführung findet in der Schlussphase statt.
9. Um die Integrität der neuen Datenbank zu schützen, stellen Sie die in Schritt 3 entfernten Einschränkungen wieder her, indem Sie das entsprechende Skript zum Hinzufügen der Einschränkungen ausführen:
 - (Oracle) Führen Sie Folgendes aus:
\$NX_ROOT/samples/views/Oracle/OracleAddConstraints.sql
 - (SQL Server) Führen Sie Folgendes aus:
\$NX_ROOT/samples/views/SQLServer/SQLAddConstraints.sql
10. Löschen Sie mit Hilfe von [pdm_tenant_delete](#) (siehe Seite 346) die extrahierten Daten aus der ursprünglichen Datenbank.
11. Stellen Sie sicher, dass alle den extrahierten Mandanten zugeordneten Repositories in die Zieleinstellungen kopiert werden.

Umgang mit Anhängen und Repositories

Anhänge werden in Repositories gespeichert. Alle Repositories, die extrahierten Mandanten zugeordnet sind, müssen in das Zielsystem kopiert werden, einschließlich der öffentlichen Repositories. Dieser Prozess wird hauptsächlich manuell ausgeführt und umfasst die folgenden Schritte:

1. Definieren Sie speicherortspezifischen Informationen für alle Repositories neu, nachdem das erste Laden der Daten in das Zielsystem beendet ist. Dafür müssen die folgenden Werte geändert werden:
 - Servername
 - Upload-Pfad
 - Servlet-Pfad
 - Archivpfad
2. Erstellen Sie manuell alle erforderlichen Verzeichnisse und Ordner.
3. Kopieren Sie alle Dateianhänge vom bisherigen Speicherort in den neuen Repository-Speicherort, nachdem (oder während) die Daten der letzten Phase geladen wurden.

Nach dem Ausführen dieser Schritte sollten alle Verweise auf Anhänge im Zielsystem erfolgreich sein. Allerdings bleiben Kopien der Anhänge auf dem Quellsystem. [Verwenden Sie das Dienstprogramm "pdm_clean_attachments.pl"](#) (siehe Seite 343), um diese redundanten Anhänge zu löschen.

Dienstprogramme für mehrere Mandanten

Dieser Abschnitt beschreibt Dienstprogramme, die zur Verwaltung einer Umgebung mit mehreren Mandanten verwendet werden.

Hinweis: Erforderliche Parameter werden in "{}" eingeschlossen, während optionale Parameter zwischen "[]" stehen.

Weitere Informationen:

[pdm_buildtenant – Erstellen von Mandanten aus einem anderen Objekt](#) (siehe Seite 341)

["pdm_clean_attachments" - Löschen redundanter Anhänge nach dem Importieren von Mandantendaten](#) (siehe Seite 343)

[pdm_settenant: Zuweisen von Mandanten zu Objekten](#) (siehe Seite 343)

["pdm_tenant_delete" - Löschen von Mandantendaten aus einer Datenbank](#) (siehe Seite 346)

[pdm_tenant_extract: Extrahieren von Mandantendaten](#) (siehe Seite 347)

[pdm_userload: Laden von Mandantendaten](#) (siehe Seite 349)

pdm_buildtenant – Erstellen von Mandanten aus einem anderen Objekt

Mit dem Hilfsprogramm *pdm_buildtenant* können Mandanten aus einem anderen Objekt erstellt werden. Eventuell haben Sie Datenaufteilungen und ein weiteres CA SDM-Objekt verwendet, um einen Teil der Funktionalität zu erreichen, die jetzt mit der Mandantenfähigkeit möglich ist. Wenn Sie eine Implementierung in Mandantenfähigkeit konvertieren möchten, müssen Sie als Erstes mit Hilfe von "pdm_buildtenant" die Daten im zuvor verwendeten Objekt dem neuen Mandantenobjekt zuordnen.

Wichtig! Bevor Sie "pdm_buildtenant" ausführen, *müssen* Sie den Service Provider konfigurieren.

In diesem Abschnitt wird das Objekt, das Mandanteninformationen enthält, als vorgeordnetes Mandantenobjekt bezeichnet. An den meisten Standorten mit diesen Anforderungen ist das org-Objekt ("organization") das Vormandantenobjekt, die folgende Methode kann jedoch für jedes Vormandantenobjekt verwendet werden.

Das Hilfsprogramm "pdm_buildtenant" erstellt die Mandantenobjekte aus Vormandantenobjekten. Diese Anwendung erstellt für jedes Vormandantenobjekt einen neuen Mandanten und konfiguriert das Mandantenattribut im Vormandantenobjekt so, dass es den neuen Mandanten referenziert. Die Syntax für dieses Hilfsprogramm lautet:

```
pdm_buildtenant [-h] | [-f [configuration_file]
```

-f configuration_file

(Optional) Gibt den Speicherort einer Konfigurationsdatei an, die die Regeln für das Erstellen von Mandanten aus dem Vormandantenobjekt vorgibt. Wenn dieses Argument nicht enthalten ist, verwendet "pdm_buildtenant" die Konfigurationsdatei aus dem Verzeichnis "\$NX_ROOT/site/cfg". Diese Datei geht davon aus, dass das vorgeordnete Mandantenobjekt "org" ist. Wenn dies nicht der Fall ist, *müssen* Sie die Konfigurationsdatei bearbeiten, bevor Sie "pdm_buildtenant" verwenden.

Hinweis: Sie *müssen* "buildtenant.xml" in das Verzeichnis "\$NX_ROOT/site/cfg" kopieren. Darüber hinaus muss sich "buildtenant.xsd" im selben Verzeichnis befinden wie "buildtenant.xml", anderenfalls erhalten Sie eine Fehlermeldung. Wenn Sie das Produkt installieren, befindet sich "buildtenant.xsd" im Verzeichnis "\$NX_ROOT/site/cfg", so dass Sie diese Datei nicht kopieren müssen.

-h

Zeigt Informationen zur Verwendung für "pdm_buildtenant" an.

Die Konfigurationsdatei hat folgendes Format:

```
<?xml version="1.0" encoding="utf-8" ?>
<BuildTenant>
  <Object from="MajicObjectName">
    <Attribute from="sourceAttribute1" to="tenantAttribute1" />
    <Attribute from="sourceAttribute2" to="tenantAttribute2" />
  </Object>
</BuildTenant>
```

Das Attribut "*from*" in der Objektmarkierung identifiziert das vorgeordnete Mandantenobjekt. Jedes Attribute-Tag identifiziert ein Attribut, das aus dem Vormandantenobjekt in ein Attribut des neuen Mandanten kopiert werden soll.

Wichtig! Bei UNIX-Implementierungen der Mandantenfähigkeit *müssen* Sie vor dem Ausführen der Dienstprogramme "pdm_settenant" und "pdm_buildtenant" das Programm "pdm_task" ausführen, um LIBPATH zu exportieren. Sie müssen die Funktion "pdm_task" vor diesen Dienstprogrammen ausführen, anderenfalls erhalten Sie Systemfehlermeldungen. Verwenden Sie "../pdm_task", um den Befehl auszuführen.

"pdm_clean_attachments" - Löschen redundanter Anhänge nach dem Importieren von Mandantendaten

Nach dem Importieren von Mandantendaten sollten Sie redundante Anhänge löschen. Dieses Dienstprogramm verfügt über folgende Syntax:

```
pdm_perl pdm_clean_attachments.pl [-h] | [-n repository_name] | [-S|-K]
```

-h

Gibt an, dass die Befehlszeilenhilfe angezeigt wird.

-n repository_name

Gibt den Namen des zu verarbeitenden Repository an. Wenn er nicht angegeben wird, werden alle Repositories verarbeitet.

-S

Gibt an, dass nur CA SDM-Repositories verarbeitet werden.

-K

Gibt an, dass nur Repositories für Knowledge Management und eingebettete Bilder verarbeitet werden.

Hinweis: Wenn der Befehl "pdm_clean_attachments.pl" ohne Argumente ausgeführt wird, werden alle Repositories verarbeitet.

Wichtig! Bei UNIX muss der LIBPATH vor der Ausführung mehrerer CA SDM-Dienstprogramme festgelegt werden. Verwenden Sie *pdm_task*, um den LIBPATH vor der Ausführung eines Dienstprogramms festzulegen. Geben Sie zum Beispiel "pdm_task pdm_clean_attachments ..." ein.

pdm_settenant: Zuweisen von Mandanten zu Objekten

Nachdem Sie Mandanten definiert haben, müssen Sie die Spalte "Mandant" mit dem Dienstprogramm *pdm_settenant* in anderen Objekten festlegen. Dieses Dienstprogramm verfügt über folgende Syntax:

```
pdm_settenant [-h] | {-f [configuration_file] | -r} [-d domsrvr]
```

-d domsrvr

(Optional) Gibt einen zu verwendenden domsrvr an. Wenn dieses Argument nicht angegeben ist, verwendet "pdm_settenant" den standardmäßigen domsrvr.

-f configuration_file

(Optional) Gibt das Verzeichnis der Konfigurationsdatei an, welche die zu aktualisierenden Daten sowie die entsprechenden Aktualisierungsregeln festlegt. Wenn dieses Argument nicht angegeben ist, verwendet "pdm_settenant" die Konfigurationsdatei aus dem Verzeichnis "\$NX_ROOT/site/cfg" (nach dem Kopieren der Konfigurationsdatei in den Ordner "\$NX_ROOT/site/cfg").

Hinweis: Sie können die Beispieldatei "settenant.xml" ändern oder eine neue Datei erstellen und in das Verzeichnis "\$NX_ROOT/site/cfg" kopieren. Darüber hinaus muss sich settenant.xsd im selben Verzeichnis befinden wie settenant.xml, anderenfalls erhalten Sie einen Fehler. Wenn Sie das Produkt installieren, befindet sich "settenant.xsd" im Verzeichnis "\$NX_ROOT/site/cfg", so dass Sie diese Datei nicht kopieren müssen.

Der folgende XML-Beispielcode beschreibt das Format dieser Datei:

```
<?xml version="1.0" encoding="utf-8" ?>
<SetTenant>
  <Object name="MajicObjectName">
    <TenantRule type="SREL">MajicColumnName</TenantRule>
    <Where>tenant is null</Where>
  </Object>
  <Object name="MajicObjectName">
    <TenantRule type="Name">TenantName</TenantRule>
    <Where>tenant is null</Where>
  </Object>
</SetTenant>
```

Jedes Objekt-Tag gibt ein CA SDM-Mandantenobjekt an. Das TenantRule-Tag gibt an, wie "pdm_settenant" den Mandanten bestimmen soll, und das Where-Tag wählt die Objekte für die Mandanten aus. Es gibt zwei Arten des Tags TenantRule:

- type="Name"
Gibt einen bestimmten Mandanten nach dem Namen an.
- type="SREL"
Gibt ein SREL-Attribut im Objekt an. "Pdm_settenant" kopiert den Mandanten des Objekts, das durch SREL referenziert wird.

-h

Zeigt Benutzerinformationen für "pdm_settenant" an.

-r

Gibt einen Bericht aus, der die Gesamtzahl der Zeilen in jeder mandantenabhängigen Tabelle anzeigt und wie viele einen Nullwert in der Spalte "Mandant" aufweisen.

Hinweis: Bei Angabe der beiden Argumente "-f" und "-r" gibt "pdm_settenant" nach der Aktualisierung einen Bericht aus. Wenn Sie nur das Argument "-r" angeben, gibt "pdm_settenant" einen Bericht aus, aktualisiert jedoch keine Daten.

Wird "pdm_settenant" ohne Argumente ausgeführt, so werden Benutzerinformationen angezeigt. Um "pdm_settenant" mit der Standardkonfigurationsdatei auszuführen, geben Sie das Argument "-f" ohne das Argument "configuration_file" an. Das Dienstprogramm pdm_settenant liest die Konfigurationsdatei und verarbeitet jede definierte Regel nacheinander. Die Ausgabe wird in die Datei "pdm_settenant.log" im Verzeichnis "\$NX_ROOT/log" geschrieben.

Sie können das Dienstprogramm so oft ausführen, wie dies erforderlich ist. Der erste Durchlauf kann sehr viel Zeit in Anspruch nehmen (bei großen Standorten bis zu mehreren Stunden). Nachfolgende Durchgänge werden schneller ausgeführt, da nur die Zeilen verarbeitet werden müssen, die nicht aktualisiert wurden. Damit wird die Datenbank vor dem Installieren der Mandantenfähigkeiten-Option vorbereitet.

Wichtig! Für die Mandantenfähigkeit unter UNIX müssen Sie zuerst "pdm_task" zum Exportieren von LIBPATH ausführen, bevor Sie die Dienstprogramme "pdm_settenant" und "pdm_buildtenant" ausführen. Sie müssen die Funktion pdm_task vor diesen Dienstprogrammen ausführen, anderenfalls erhalten Sie Systemfehler. Führen Sie den Befehl mit ../pdm_task aus.

Hinweise zum Zuweisen von Mandanten zu Objekten

Nach dem Definieren von Mandanten können Sie das Dienstprogramm "pdm_settenant" (Zuweisen von Mandanten zu Objekten) verwenden, um die Mandantenspalte in anderen Objekten festzulegen. Wenn Sie den Mandanten für ein Objekt ändern, müssen Sie ermitteln, ob die Mandantenfähigkeit für zugehörige Mandantenobjekte geändert werden muss, um die Datenintegrität beizubehalten. Werden diese Objekte nicht synchronisiert, so können Daten scheinbar in CIs, Beziehungen, MDRs, Version usw. fehlen. Die folgenden CA CMDB-Objekte sind als Mandantenobjekte ausgelegt:

- nr – CI-Definitionen
- nr_com – Protokolleinträge, die mit einem CI verknüpft sind
- bmhier – Beziehungen, die mit CIs verknüpft sind
- MDR_idmap – MDR-Providerdefinitionen
- ci_mdr_idmap – Föderierte CI-/MDR-Zuordnungen

Führen Sie für jedes CI die folgenden Schritte zum Synchronisieren der Daten aus, wenn Sie die Mandantenfähigkeit mit "pdm_settenant" ändern:

- Geben Sie "nr" als Name für das CI-Objekt an.
- Ändern Sie die Protokolleinträge, die mit dem CI in "nr_com" verknüpft sind, damit Sie die Protokolleinträge für den neuen Mandanten anzeigen können.

Hinweis: Informationen über den Befehl "pdm_settenant" finden Sie im *Administrationshandbuch*.

Beispiel: XML-Code zum Ändern des Mandanten und des Protokolls

Der folgende XML-Code ändert den Mandanten für ein CI mit der Bezeichnung "CITest" in "T2" und ändert auch die entsprechenden Protokolleinträge in "nr_com":

```
<TenantRule type="Name">T2</TenantRule>
<Where>name = 'CITest'</Where>
</Object>
<Object name="nr_com">
<TenantRule type="Name">T2</TenantRule>
<Where>asset_id.name = 'CITest'</Where>
\</Object>
```

"pdm_tenant_delete" - Löschen von Mandantendaten aus einer Datenbank

Mit dem Dienstprogramm "pdm_tenant_delete" werden alle Daten für einen bestimmten Mandanten aus der Datenbank entfernt.

Wichtig! Die referenziellen Einschränkungen für "ca_tables" müssen vor dem Ausführen von "pdm_tenant_delete" aufgehoben und danach wiederhergestellt werden.

Dieses Dienstprogramm verfügt über folgende Syntax:

```
pdm_tenant_delete -h|-t tenant_name [-C|-R] [-Q]
```

-h

Zeigt die Verwendungsinformationen für "pdm_tenant_delete" an.

-t tenant_name

Gibt den Namen des Mandanten an, dessen Daten gelöscht werden.

Hinweis: Der Mandant muss als inaktiv gekennzeichnet werden, bevor Sie dieses Dienstprogramm zum Löschen der Daten verwenden können.

-C

Gibt an, dass alle Kontakte für einen Mandanten als inaktiv gekennzeichnet werden. Da Kontakte unter Produkten gemeinsam genutzt werden können, sollte über die Standardlogik keine Sammel Löschung oder Sammelinaktivierung von Kontakten erfolgen, sofern dies nicht ausdrücklich gefordert wird.

Hinweis: Diese Option wird ignoriert, wenn die Option "-R" angegeben ist.

-R

Gibt an, dass alle Zeilen in allen Mandantentabellen, die in "ddict.sch" als "CA_COMMON" gekennzeichnet sind, gelöscht werden, einschließlich des Mandantenobjekts selbst.

Wichtig! Diese Tabellen werden von zahlreichen Produkten gemeinsam genutzt; setzen Sie diese Option also mit Vorsicht ein.

-Q

Gibt Verarbeitung im Ad-hoc-Abfragemodus an, damit Datenbankabfragen so schnell wie möglich durchgeführt werden. Wenn dieses Argument nicht angegeben wird, verwendet das Dienstprogramm die Hintergrundverarbeitung, so dass Abfragen nur ausgeführt werden, wenn das System sonst inaktiv ist. Dieses Argument verbessert die Ausführungszeit auf Kosten einer stärkeren Auslastung eines aktiven Systems.

Wichtig! Bei UNIX muss der LIBPATH vor der Ausführung mehrerer CA SDM-Dienstprogramme festgelegt werden. Verwenden Sie *pdm_task*, um den LIBPATH vor der Ausführung eines Dienstprogramms festzulegen. Geben Sie zum Beispiel "pdm_task pdm_clean_attachments ..." ein.

pdm_tenant_extract: Extrahieren von Mandantendaten

Das Dienstprogramm *pdm_tenant_extract* extrahiert alle Daten für einen angegebenen Mandanten aus der Datenbank. Die Daten werden im "pdm_userload"-Format extrahiert, so dass sie bequem in eine andere Datenbank geladen werden können. Dieses Dienstprogramm verfügt über folgende Syntax:

```
pdm_tenant_extract -h | -c control_file [-d domsrvr] [-g yes|no] [-o output_file]
                    -p phase [[-t tenant_name]...] [-Q] [table1 [table2...]]
```

-h

Zeigt Benutzerinformationen für "pdm_tenant_extract" an.

-c control_file

Gibt das Verzeichnis der Kontrolldatei für diesen Mandantenextrakt an. In der Anfangsphase wird die Datei im angegebenen Verzeichnis erstellt (sie darf nicht bereits vorhanden sein). Die Datei muss für die Aktualisierungs- und die Schlussphase vorhanden sein.

-d domsrvr

(Optional) Gibt einen zu verwendenden domsrvr an.

-g yes|no

(Optional) Gibt an, ob öffentliche Daten in die Ausgabedatei eingeschlossen werden sollen. Ist dieses Argument nicht angegeben, werden öffentliche Daten aus allen Tabellen eingeschlossen.

-o output_file

(Optional) Gibt das Verzeichnis der Ausgabedatei an. Ist dieses Argument nicht angegeben, wird die Ausgabe in "stdout" geleitet.

-p phase

Gibt die Phase des Extrakts an. Verwenden Sie einen der folgenden Werte:

I – Initial

U – Update

F – Final

-t tenant_name

Gibt den Namen eines zu extrahierenden Mandanten an. Dieses Argument wird für die Anfangsphase benötigt und kann für mehrere Mandanten wiederholt werden. In der Aktualisierungs- und Schlussphase ist es nicht zulässig.

-Q

Gibt Verarbeitung im Ad-hoc-Abfragemodus an, damit Datenbankabfragen so schnell wie möglich durchgeführt werden. Wenn dieses Argument nicht angegeben ist, werden Abfragen im Hintergrund verarbeitet, d. h. nur dann, wenn das System im Leerlauf ist.

table1 [table2...]

(Optional) Gibt die zu extrahierenden Tabellen an. Ohne dieses Argument werden alle Tabellen extrahiert.

Wichtig! Die Ergebnisse aus der Anfangsphase müssen in eine Datenbank geladen werden, die noch nicht für CA SDM oder für andere Produkte verwendet worden ist. Jede Tabelle, die mit Daten aus der Anfangsphase geladen wird, wird vor dem Laden abgeschnitten. Wenn die Datenbank bereits verwendet wird, könnte dies zu Datenverlust führen.

Hinweis: Um Probleme mit Referenzen beim Laden der Daten zu vermeiden, führen Sie das entsprechende Skript zum Entfernen von Einschränkungen aus: (\$NX_ROOT/samples/views/Oracle/OracleDropConstraints.sql oder \$NX_ROOT/samples/views/SQLServer/SQLDropConstraints.sql). Nachdem der Ladevorgang abgeschlossen ist, übernehmen Sie die Einschränkungen mit dem entsprechenden Skript "xxxAddConstraints.sql" im selben Verzeichnis erneut.

Wichtig! Bei UNIX muss der LIBPATH vor der Ausführung mehrerer CA SDM-Dienstprogramme festgelegt werden. Verwenden Sie *pdm_task*, um den LIBPATH vor der Ausführung eines Dienstprogramms festzulegen. Geben Sie zum Beispiel "pdm_task pdm_clean_attachments ..." ein.

Weitere Informationen:

[Exportieren und Importieren von Mandantendaten](#) (siehe Seite 338)

pdm_userload: Laden von Mandantendaten

Das Dienstprogramm *pdm_userload* dient zum Laden der Daten in eine CA SDM-Datenbank. Dieses Dienstprogramm ist auch dann verfügbar, wenn die Mandantenfähigkeit nicht installiert ist. Die Mandantenfähigkeit stellt ein weiteres Argument (-t) bereit. Dieses gibt den Namen eines Mandanten an, dessen ID in die Spalte "Mandant" aller eingefügten oder aktualisierten Zeilen in einer mandantenabhängigen Tabelle eingefügt werden muss. Der angegebene Mandant muss bereits in der Datenbank sein.

Führen Sie beim Extrahieren von Daten die folgenden Schritte aus, um Fehler in "stdlog" zu vermeiden:

1. Fahren Sie CA SDM zuerst herunter, und starten Sie dann das Produkt wie folgt neu im DBADMIN-Modus, bevor Sie den Ladevorgang beginnen:

Windows

Führen Sie "pdm_d_mgr -s DBADMIN" aus.

UNIX

Führen Sie "pdm_init -s DBADMIN" aus.

2. Nachdem die Daten geladen sind, halten Sie CA SDM mit dem Befehl "pdm_halt" an.
3. Starten Sie CA SDM im Normalmodus.

Hinweis: Weitere Informationen zum Hilfsprogramm "pdm_userload" finden Sie im *Administrationshandbuch*.

So aktivieren Sie Auto-Failover

Die Server-Systemüberwachung beobachtet, wie ein Server auf die Betriebslast reagiert und verfolgt dessen Reaktionsfähigkeit auf Client-Anfragen. Mit dieser Überwachung sollen Serverfehler verhindert werden, indem sichergestellt wird, dass der Server immer über ausreichende Kapazitäten verfügt, um die angeforderten Aufgaben durchzuführen. Die meisten der standardmäßigen Systemüberwachungstools unterstützen Remote-Server-Monitoring durch die HTTP und HTTPS-Protokolle.

Die automatische Failover-Funktion von CA SDM stellt die folgenden HTTP-basierten Standardschnittstellen bereit:

- Health Monitoring Interface: HTTP(S)-Schnittstelle zur Überwachung des Zustands des Hintergrundservers. Sie trifft darüber hinaus verlässliche Failover-Entscheidungen, um ein Failover auf einem ausgewählten Standby-Server zu initiieren, falls der Hintergrundserver nicht verfügbar ist oder wenn er die angeforderten Aufgaben nicht ausführen kann.
- Failover Initiating Interface: HTTP(S)-Schnittstelle, um den gewählten Standby-Server nahtlos als neuen Hintergrundserver einzusetzen, ohne dabei eine Serviceunterbrechung zu verursachen.

Gehen Sie wie folgt vor:

1. Installieren Sie Apache Tomcat auf dem Hintergrundserver und allen Standby-Servern.

Hinweis: Stellen Sie sicher, dass Tomcat JRE 1.7 verwendet und dass Tomcat nicht die Portnummer verwendet, die für die CA SDM-Komponenten konfiguriert ist.
2. (Optional) Konfigurieren Sie SSL auf den installierten Tomcat-Servern. Weitere Informationen zur Konfiguration von SSL finden Sie im Szenario *So konfigurieren Sie die SSL-Authentifizierung* oder im *Administrationshandbuch*.
3. Melden Sie sich am Hintergrundserver an.
4. Stellen Sie das Health-Servlet bereit. Führen Sie die folgenden Schritte aus:
 - a. Kopieren Sie die HealthServlet.war-Datei vom Ordner "`$NX_ROOT/samples/HealthServlet`" in den Ordner "`TOMCAT_HOME/webapps`".
 - b. Starten Sie Tomcat neu.

Die Datei "HealthServlet.war" wird im Ordner "webapps" bereitgestellt. Um die Bereitstellung zu bestätigen, verifizieren Sie, dass der HealthServlet-Ordner im gleichen webapps-Ordner erstellt wird.

Nach der erfolgreichen Bereitstellung ist das Health-Servlet bereit, die Zustandsüberprüfungen auszuführen. Dazu gehört auch die Prüfung des Status des SLUMP und des Zustands der CA SDM-Prozesse, die in der health.xml-Datei definiert werden. Suchen Sie die Datei "health.xml" im folgenden Speicherort:

`TOMCAT_HOME/webapps/HealthServlet/WEB-INF/classes`

5. (Optional) Passen Sie "health.xml" basierend auf den Anforderungen Ihrer Organisation an. Zum Beispiel möchten Sie den Webengine-Prozess überwachen. Fügen Sie den Prozess der health.xml-Datei mit dem richtigen Tagnamen, wie in CA SDM definiert, hinzu. Führen Sie die folgenden Schritte aus, um den Tagnamen zu finden:
 - a. Öffnen Sie die pdm_startup.i- und pdm_startup-Dateien vom \$NX_ROOT/pdmconf-Verzeichnis.
 - b. Suchen Sie in beiden Dateien nach dem Prozess, den Sie überwachen wollen.
 - c. Finden Sie das entsprechenden Tagnamen, indem Sie die Variablen in beiden Dateien abstimmen.

Zum Beispiel wird Webengine-Prozess in der pdm_startup.i-Datei folgendermaßen definiert:

```
#define WEBENGINE(_TAG,_HOST,_SLUMP_NAME,_DOMSRVR, _CFG, _WEBDIRECTOR, _RPC_NAME)
```

Der Webengine-Prozess wird in der pdm_startup-Datei folgendermaßen definiert:

```
WEBENGINE(webengine, $NX_LOCAL_HOST, web:local, domsrvr, $NX_ROOT/bopcfg/www/web.cfg, "", "rpc_srvr:%h")
```

Anhand dieses Beispiels können wir feststellen, dass das Tagname für den Webengine-Prozess "webengine" ist.

Wichtig! Wenn Sie einen neuen Prozess erstellen, wird der vorhandene Prozess in der pdm_startup-Datei mit Kommentarzeichen versehen, und neue Einträge werden erstellt. Stellen Sie sicher, dass Sie in den neuen Prozesseinträgen nach dem Tagnamen suchen.

Wichtig! Wenn Sie health.xml ändern, stellen Sie sicher, dass der XML-Code keine Fehler aufweist und dass Sie Tomcat neu starten, damit die Änderungen übernommen werden.

6. Führen Sie Schritte 4 und 5 für alle Standby-Server aus.
7. Konfigurieren Sie das gewählte Drittanbieter-Tool, um den Zustand des Hintergrundservers in regelmäßigen Intervallen zu überwachen. Verwenden Sie dazu die folgende HTTP URL:

`http://Background_server_name: port_number/HealthServlet/GetHealth`

8. Konfigurieren Sie das gewählte Drittanbieter-Tool, um eine Failover-Logik zu initiieren, wenn sich der Zustand des Hintergrundservers verschlechtert. Wir empfehlen, die Failover-Logik so zu konfigurieren, dass der Standby-Server als neuer Hintergrundserver hochgestuft wird. Verwenden Sie das folgende Failover-Servlet in der Failover-Logik:

Wichtig! Wir empfehlen, das Failover-Servlet auf SSL mit Zugriffsberechtigungen zu konfigurieren, die nur bestimmten Anwendern gegeben worden sind. Dies trifft auch auf die Konfiguration von Drittanbieter-Tool zur Failover-Initiierung zu.

`http(s)://Standby_server_name:port_number/HealthServlet/FailoverServlet`

Sie haben Auto-Failover aktiviert.

9. Nach der erfolgreichen Konfiguration beginnt das Drittanbieter-Tool mit der Überwachung des Zustands des Hintergrundservers unter Verwendung der Health-Servlet-URL.
 - Jeder Servertyp hat eine eigene Reihe von Prozessen. Wenn der SLUMP und alle CA SDM-Prozesse richtig funktionieren, erhält das Drittanbieter-Tool vom Hintergrundserver eine HTTP 200-Antwort mit vordefinierten Daten:

EV-Server-Status: All OK!

EV-Server-Role: BG
 - Wenn ein SLUMP oder einer der CA SDM-Prozesse (in health.xml aufgeführt) nicht länger arbeitet und nicht neu gestartet werden kann, erhält das Drittanbieter-Tool vom Hintergrundserver eine HTTP 503-Antwort mit folgenden Daten:

EV-Server-Status: NOT OK!

EV-Server-Role: BG
10. Bei Eingang einer HTTP 503-Antwort initiiert das Drittanbieter-Tool automatisch die Failover-Logik.

Kapitel 6: Anpassung

Dieses Kapitel enthält folgende Themen:

[Anpassung – Übersicht](#) (siehe Seite 355)

[So verschieben Sie das Authentifizierungsmodul zu einem externen Server](#) (siehe Seite 356)

[Anpassen der Benachrichtigungsmethode](#) (siehe Seite 364)

[Anpassen von Abfragen und Meldungen](#) (siehe Seite 373)

[Anpassen der Webschnittstelle](#) (siehe Seite 388)

[Anpassung der Event-Protokoll-Datenspeicherung](#) (siehe Seite 509)

[Anpassen von CA Business Intelligence-Berichten](#) (siehe Seite 511)

[Anpassen von Legacy-Berichten](#) (siehe Seite 529)

Kapitel 7: Anpassung – Übersicht

Mit CA SDM können Sie verschiedene IT-Service-Management-Funktionen erfüllen. Das Produkt stellt umfassende Funktionen und verschiedene Dokumente zur Best Practice bereit, mit denen die Anforderungen Ihres Service Management umgesetzt werden können.

Obwohl die Standardimplementierung von CA SDM weitestgehend mit den Prozessen und der Terminologie der meisten IT-Unternehmen übereinstimmt, können Sie das Produkt anpassen, um mit den individuellen Aspekten Ihres Betriebs zu arbeiten. Das Produkt enthält folgende Möglichkeiten zur Produktanpassung, um Ihren jeweiligen Anforderungen gerecht zu werden:

- Personalisierung von Endanwendern
- Systemweite Konfiguration
- Tool-basierte Anpassung
- Anpassung auf Codeebene

Für die Anpassung des Produktes stehen verschiedene Möglichkeiten zur Verfügung.

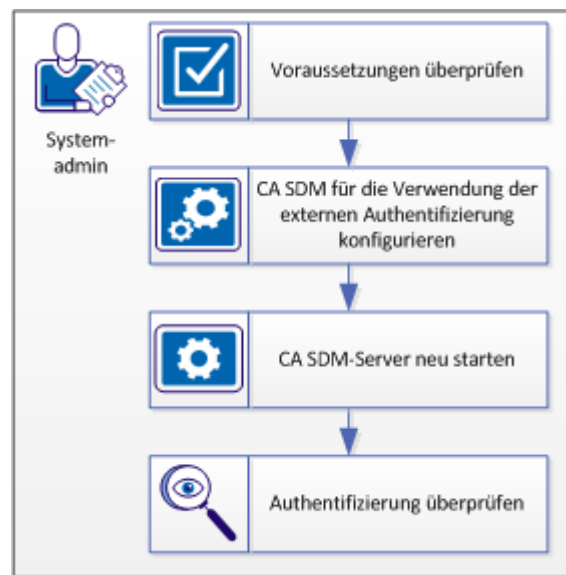
So verschieben Sie das Authentifizierungsmodul zu einem externen Server

Das Authentifizierungsmodul in CA SDM ist ein Singleton-Daemon, der für die Anwenderauthentifizierung verantwortlich ist. Das Authentifizierungsmodul wird auf dem Primärserver für die konventionelle Konfiguration und auf dem Hintergrundserver für die Konfiguration für erweiterte Verfügbarkeit ausgeführt. Sie verschieben das Authentifizierungsmodul zu einem externen Server, wenn folgende Szenarien auftreten:

- Konventionelle Konfiguration:
 - Der Primärserver befindet sich auf einer UNIX- oder Linux-Plattform, und Sie benötigen eine Windows-Authentifizierung. Sie verschieben das Authentifizierungsmodul zu einem Windows-Sekundärserver.
 - Der Primärserver befindet sich auf einer Solaris-Plattform, und Sie benötigen die CA EEM-Authentifizierung. Sie verschieben das Authentifizierungsmodul zum Sekundärserver, da CA SDM die CA EEM-Integration unter Solaris nicht unterstützt.
- Konfiguration für erweiterte Verfügbarkeit:
 - Der Hintergrundserver befindet sich auf einer UNIX- oder Linux-Plattform, und Sie benötigen eine Windows-Authentifizierung. Sie verschieben das Authentifizierungsmodul zu einem Windows-Anwendungsserver.
 - Der Hintergrundserver befindet sich auf einer Solaris-Plattform, und Sie benötigen die CA EEM-Integration. Sie verschieben das Authentifizierungsmodul zu einem Anwendungsserver, da CA SDM die CA EEM-Integration unter Solaris nicht unterstützt.

Hinweis: Auf dem ausgewählten externen Server muss CA SDM installiert sein. Wenn Sie das Authentifizierungsmodul zu einem externen Server verschieben, wird dies zu einer Fehlerquelle. Wenn Sie zum Beispiel das Authentifizierungsmodul zu einem Anwendungsserver verschieben, dann können sich Anwender nicht mehr anmelden, wenn dieser Anwendungsserver ausfällt.

Folgendes Diagramm veranschaulicht, wie das Authentifizierungsmodul verschoben wird:



Um das Authentifizierungsmodul zu einem externen Server zu verschieben, gehen Sie folgendermaßen vor:

1. Überprüfen Sie die Voraussetzungen.
2. [Konfigurieren Sie CA SDM für das Verschieben des Authentifizierungsmoduls.](#) (siehe Seite 359)
3. [Starten Sie die CA SDM-Server neu](#) (siehe Seite 360)
4. [Überprüfen der Authentifizierung.](#) (siehe Seite 363)

Überprüfen der Voraussetzungen

Die Analyse der CA SDM-Server-Plattformen hilft Ihnen dabei, zu entscheiden, wie Sie das Authentifizierungsmodul zu einem externen Server verschieben.

Gehen Sie wie folgt vor:

- Identifizieren Sie das Betriebssystem des folgenden Servers, der auf dem Konfigurationstyp basiert:
 - Konventionell: Primärserver.
 - Erweiterte Verfügbarkeit: Anwendungsserver.
- Identifizieren Sie den Typ der erforderlichen Authentifizierung von den folgenden Modellen:
 - Windows-Authentifizierung für die CA SDM-Implementierung unter UNIX oder Linux.
 - CA EEM-Authentifizierung für die CA SDM-Implementierung unter Solaris.
- Stellen Sie sicher, dass CA SDM auf dem ausgewählten externen Server installiert ist.

Konfigurieren von CA SDM für die Verwendung der externen Authentifizierung

Um die Authentifizierungs-Requests an einen externen Server umzuleiten, müssen Sie den Hostnamen des Zielservers angeben, auf dem sich das Authentifizierungsmodul befindet. Der Konfigurationsprozess von CA SDM für das Verschieben des Authentifizierungsmoduls ist für die konventionelle Konfiguration und für die Konfiguration für erweiterte Verfügbarkeit von CA SDM unterschiedlich.

Konventionelle Konfiguration

Gehen Sie wie folgt vor:

1. Melden Sie sich als Administrator beim Primärserver an.
2. Ändern Sie über die Eingabeaufforderung das Verzeichnis auf "samples\pdmconf" unter "NX_ROOT", und führen Sie "pdm_perlpdm_edit.pl" aus.
3. Wählen Sie im Hauptmenü von "pdm_edit.pl" die Option "U" aus, und drücken Sie die EINGABETASTE.
Das Untermenü für Anwendervalidierungsserver wird angezeigt.
4. Geben Sie "E" ein, um den Hostnamen des externen Servers anzugeben, und drücken Sie die EINGABETASTE.
5. Geben Sie primär für den Primärserver oder den Hostnamen des Sekundärservers ein.

Sie haben die Umleitung der Authentifizierungs-Requests zu einem externen Server konfiguriert.

Konfiguration für erweiterte Verfügbarkeit

Gehen Sie wie folgt vor:

1. Melden Sie sich als Administrator bei der Web-Schnittstelle des Hintergrundservers an.
2. Klicken Sie auf die Registerkarte "Administration".
3. Blenden Sie "Optionsmanager", "Sicherheit" ein.
4. Klicken Sie auf den Eintrag "bopauth_nxd_host" in der Optionsliste.
Die Seite "Optionen - Detail: bopauth_nxd_host" wird angezeigt.
5. Klicken Sie auf "Bearbeiten".
6. Wählen Sie den Hostnamen des Zielservers aus der Dropdown-Liste "Optionswert" aus.
7. Klicken Sie auf "Speichern".

Hinweis: Standardmäßig wird das Authentifizierungsmodul auf dem Hintergrundserver ausgeführt.

Sie haben die Umleitung der Authentifizierungs-Requests zu einem externen Server konfiguriert.

So starten Sie die CA SDM-Server neu

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

- [Starten Sie die CA SDM-Server in konventioneller Konfiguration neu](#) (siehe Seite 360).
- [Starten Sie die CA SDM-Server in der Konfiguration für erweiterte Verfügbarkeit neu](#) (siehe Seite 360).

Neustarten der CA SDM-Server in konventioneller Konfiguration

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

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

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

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

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

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

1. Starten Sie alle Standby-Server neu.
2. [Stufen Sie den Standby-Server als neuen Hintergrundserver hoch](#) (siehe Seite 361).
3. Starten Sie den alten Hintergrundserver.

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

4. [Wählen Sie einen Anwendungsserver aus, der wenig aktiv ist](#) (siehe Seite 362).
5. Starten Sie den Anwendungsserver neu, der wenig aktiv ist.
6. [Halten Sie den anderen Anwendungsserver an](#) (siehe Seite 362).
7. Starten Sie den Anwendungsserver.
8. Führen Sie die Schritte 6 und 7 für die anderen Anwendungsserver aus.

Hochstufen des Standby-Servers als neuen Hintergrundserver

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

Gehen Sie wie folgt vor:

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

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

-h

Zeigt die Hilfeseite an.

-q seconds

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

-c

Diese Option bricht einen zuvor gesendeten Request zur Stilllegung ab.

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

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

```
pdm_server_control -b
```

-b

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

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

Auswählen des Anwendungsservers, der wenig aktiv ist

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

```
pdm_webstat
```

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

Anhalten der anderen Anwendungsserver

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

Gehen Sie wie folgt vor:

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

3. Führen Sie folgenden Befehl auf dem Anwendungsserver aus:

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

-h

Zeigt die Hilfeseite an.

-q *interval* -s *server_name*

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

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

Der Anwendungsserver wird erfolgreich angehalten.

Überprüfen der Authentifizierung

Überprüfen Sie die Authentifizierung mit einer Anwender-ID, die einen entsprechenden Kontaktdatensatz in Windows oder CA EEM hat, basierend auf dem Authentifizierungstyp. Eine erfolgreiche Anmeldung zeigt an, dass Sie das Authentifizierungsmodul erfolgreich verschoben haben.

Gehen Sie wie folgt vor:

1. Starten Sie den Browser, und geben Sie die CA SDM-URL ein.
2. Melden Sie sich bei CA SDM mit einem Anwendernamen an, der einen entsprechenden Kontaktdatensatz in Windows oder CA EEM hat, basierend auf dem Authentifizierungstyp.

Wenn das Modul erfolgreich verschoben wurde, wird die Service Desk-Startseite geöffnet.

Anpassen der Benachrichtigungsmethode

Die automatischen Benachrichtigungsmethoden von CA SDM benachrichtigen Mitarbeiter an wichtigen Punkten im Service Desk-Managementprozess. Die Standardbenachrichtigungsmethoden werden wie folgt angezeigt:

- E-Mail
- Benachrichtigung (Protokoll)
- Pager_Email

Sie können angepasste Benachrichtigungsmethoden definieren, um eine neue Methode der Übertragung anzugeben (z. B. Sprachmeldungen, Bildschirmanzeigen oder bestimmte Drucker). Sie können auch Daten aus einer anderen Anwendung abrufen und sie in die Benachrichtigung einschließen.

Benachrichtigungsprozess

Ticket-Benachrichtigungen (die für Issues, Changes und Anfragen verwendet werden können) werden bearbeitet, wenn das Ticket gespeichert wird, wie nachfolgend beschrieben:

- Wenn für die Benachrichtigungsmethode etwas anderes als "Benachrichtigung" (z. B. "E-Mail") eingestellt ist, führt der Benachrichtigungsprozess die Benachrichtigungsmethode für jeden Kontakt in der Liste aus. Bei dieser Methode handelt es sich typischerweise um eine ausführbare Datei oder ein Shell-Skript, die bzw. das in einem neuen Prozess ausgeführt wird. Details über die Benachrichtigung werden in Umgebungsvariablen gespeichert, damit die ausführbare Datei bzw. das Skript problemlos darauf zugreifen kann.
- Der Benachrichtigungsprozessor stellt die Umgebungsvariablen `NX_NTF_MESSAGE` und `NX_NTF_SUMMARY` für jede angeforderte Benachrichtigung ein, indem der Titel der Benachrichtigungsmeldung und der Benachrichtigungstext verwendet werden, die in der Notizbuchseite „Meldungsvorlage“ des Fensters „Aktivitätsbenachrichtigungen – Detail“ angegeben sind. Wenn der Empfänger ein gültiger Kontakt ist, werden weitere Umgebungsvariablen aus den Informationen des entsprechenden Kontaktdetail-Datensatzes erstellt.
- Wenn die Option „In Datei schreiben“ für die Benachrichtigung ausgewählt ist, wird eine Textdatei mit zusätzlichen Informationen erstellt, die von der Benachrichtigungsmethode verwendet werden kann, um weitere, detaillierte Informationen abzurufen.
- Eine Liste der Kontakte, die diese Benachrichtigung erhalten, wird auf Grundlage der Informationen in den Notizbuchseiten „Objekte“, „Kontakte“ und „Umfrage“ des Fensters „Aktivitätsbenachrichtigung – Detail“ erstellt. Für die Kontakte, bei denen die Benachrichtigungsebene und die installierte Optionsmanager-Option „log_all_notify“ mit der Benachrichtigungsmethode übereinstimmt, wird eine Benachrichtigung vor dem Benachrichtigungsprotokoll erstellt.

Variablen der Benachrichtigungsmethode

Für die Benachrichtigungsmethode werden zwei Variablensätze erstellt und zur Verfügung gestellt.

Grundlegende Umgebungsvariablen

Der erste Variablensatz wird unabhängig davon, ob die Option „In Datei schreiben“ für die Benachrichtigung eingestellt ist, für jede gesendete Benachrichtigung erstellt. Sie werden als Umgebungsvariablen in die Umgebung geschrieben, auf die die Benachrichtigungsmethode standardmäßig zugreifen kann. Wenn Sie die Option "In Datei schreiben" für die Benachrichtigungsmethode wählen, werden diese Variablen auch in die Benachrichtigungsdatei im Benachrichtigungsbereich geschrieben.

Die folgenden Umgebungsvariablen liefern Ihnen grundlegende Informationen über die Benachrichtigung. Sie sind immer definiert, selbst wenn der entsprechende Wert leer ist:

Umgebungsvariable	Beschreibung
NX_NTF_MESSAGE	Der vollständige Text der Meldungsvorlage, einschließlich der vollständigen Erweiterung von allen Variablen
NX_NTF_SUMMARY	Der vollständige Kopf der Meldungsvorlage, einschließlich der vollständigen Erweiterung von allen Variablen
NX_NTF_URGENCY	Die Dringlichkeit der Benachrichtigung (1 entspricht einer niedrigen Dringlichkeit, 4 einer hohen)

Die folgenden Umgebungsvariablen werden nur geschaffen, wenn der Empfänger ein gültiger CA SDM-Kontakt ist. In diesem Fall werden sie mit Werten aus dem Kontaktdatensatz des Empfängers eingestellt, wie in der folgenden Tabelle gezeigt:

Variable	Felder im Fenster „Kontakt – Detail“
NX_NTF_BEEPER_PHONE	Pager-Nummer
NX_NTF_COMBO_NAME	Nachname, Vorname, Zweiter Vorname
NX_NTF_CONTACT	ID kontaktieren
NX_NTF_EMAIL_ADDRESS	E-Mail- oder Pager-E-Mail-Adresse (in Abhängigkeit vom Benachrichtigungstyp)
NX_NTF_FAX_PHONE	Faxnummer

Variable	Felder im Fenster „Kontakt – Detail“
NX_NTF_PUBLIC_PHONE	Telefonnummer
NX_NTF_USERID	Benutzer-ID
NX_NTF_VOICE_PHONE	Alt. Telefonnummer

Hinweis: Diese Variablen werden nicht erstellt, wenn die entsprechenden Werte leer sind (mit Ausnahme der Variablen "NX_NTF_CONTACT", die nicht leer sein kann).

Attributvariablen

Der zweite Variablensatz, die sogenannten Attributvariablen, steht nur zur Verfügung, wenn Sie beim Definieren der Benachrichtigungsmethode die Option "In Datei schreiben" wählen. Sie werden nur in die Benachrichtigungsdatei geschrieben, nicht in die Umgebung. Sie weisen folgendes Format auf:

NX_NTF_attribute[.secondary_attribute]=value

Dabei gilt:

Attribut

Der Name des Attributs, dessen Wert Sie abrufen möchten. Dies ist der Attributname, wie er für das Objekt definiert wurde. Eine vollständige Liste aller Attributnamen für alle Objekte finden Sie im *Technischen Referenzhandbuch zu CA SDM*. Die gebräuchlichsten Objekte, die Benachrichtigungen zugeordnet sind, sind Tickets. Sie verfügen über einen Objektnamen, der vom Typ des Tickets (z. B. "cr" für Anfragen) abhängig ist, und den Kontakt, der den Empfänger angibt und den Objektnamen "cnt" aufweist. Die Umgebungsvariable des Beschreibungsattributs eines Tickets kann in der Benachrichtigungsdatei beispielsweise folgendermaßen aussehen:

NX_NTF_DESCRIPTION=This is a sample description.

secondary_attribute

Wenn das erste *Attribut* ein internes Kennzeichen für ein anderes Objekt ist, wird häufig unter Verwendung der Punktnotation ein sekundäres Attribut angehängt, um aussagekräftigere Informationen zu vermitteln. In Bezug auf Datenbanken stellen Attribute keinen einfachen Datenwert dar, sondern einen Fremdschlüssel, der auf eine Zeile in einer anderen Tabelle verweist. Die direkte Verwendung des Schlüsselwerts hätte wahrscheinlich keine Bedeutung. Damit Sie weniger Aufwand haben, werden viele dieser Feldtypen aufgelöst oder referenziert. Wenn dies der Fall ist, entspricht *secondary_attribute* dem Wert in der referenzierten Tabelle. Anstatt z. B. den Wert für das assignee-Attribut zu schreiben, das als eindeutige ID des Kontaktdatensatzes für den Zuständigen gespeichert ist, wird der kombinierte Name des Zuständigen geschrieben, der auf das Attribut "combo_name" für das Kontaktobjekt verweist, wie in diesem Beispiel dargestellt:

```
NX_NTF_ASSIGNEE.COMBO_NAME=Armstrong, Beth
```

Wenn ein Attribut über keinen Wert verfügt, ist der entsprechende Wert normalerweise (NULL) oder leer. Beispiel:

```
NX_NTF_CALL_BACK_DATE=(NULL)
```

```
NX_NTF_GROUP.COMBO_NAME=
```

Hinweis: Eine Attributvariable, die sowohl für das Ticket als auch den Empfänger existiert, ist *NX_NTF_ID* (das ID-Attribut). Diese Variable entspricht der eindeutigen Datenbank-ID des Objekts.

Benachrichtigungsdatei

Wenn Sie bei der Definition der Benachrichtigungsmethode die Option "In Datei schreiben" wählen, werden grundlegende Umgebungs- und Attributvariablen in eine Textdatei geschrieben, die vor der Ausführung des Skripts bzw. Programms der Benachrichtigungsmethode geschlossen wird. Diese Benachrichtigungsdatei wird immer dann geschrieben, wenn die Benachrichtigungsmethode für einen Kontakt aufgerufen wird. Sie stellt einen handlichen Mechanismus für das Übergeben von relevanten Informationen an das Benachrichtigungsskript dar, die andernfalls in der Umgebung nicht verfügbar sind.

Der vollständige Pfad der Benachrichtigungsdatei ist in der Umgebungsvariablen `NX_NTF_FILENAME` festgelegt, die für den Prozess der Benachrichtigungsmethode zur Verfügung steht. Der Dateiname wird auch am Ende des Wertes hinzugefügt, den Sie während der Definition der Benachrichtigungsmethode in das Feld „Benachrichtigungsmethode“ eingeben. Wenn die Benachrichtigungsmethode z. B. `"pdm_perl -w mymethod"` lautet, führt der eigentliche Prozess `"pdm_perl -w mymethod.pl unique_notification_file_name"` aus.

Wichtig! Der Administrator kann die Benachrichtigungsdateien löschen. Dies ist für Standorte mit einem hohen Durchsatz von Tausenden von Benachrichtigungen am Tag besonders wichtig. Die Dateien befinden sich im standardmäßigen temporären Verzeichnis (TEMP unter Windows und TMP unter UNIX). Ein Vorschlag besteht darin, die Dateien am Ende der Ausführung des Skripts bzw. Programms der Benachrichtigungsmethode zu löschen.

Bei der Benachrichtigungsdatei handelt es sich um eine Standard-Textdatei, die in Abschnitte geteilt ist. Jede Zeile enthält entweder ein Attribut/Wert-Paar oder eine Abschnittsmarkierung. Jede Benachrichtigungsdatei hat drei Abschnitte, die im Folgenden beschrieben sind. Alle Abschnitte beginnen mit „-----“ gefolgt von einer neuen Zeile.

SECTION=obj, wobei obj den Objekttyp des Tickets angibt

Iss

Liefert Informationen über das Issue.

Chg

Liefert Informationen über den Change.

Cr

Liefert Informationen über die Anfrage.

SECTION=cnt

Liefert Informationen über den Empfänger.

SECTION=notification

Gibt dieselben Informationen an, die auch als grundlegende Umgebungsvariablen verfügbar sind.

Hinweis: Die Abschnittsnamen für das Ticket und den Empfänger entsprechen den Objektnamen für die Attribute in dem Abschnitt. Eine vollständige Liste aller Attributnamen für alle Objekte finden Sie im *Technischen Referenzhandbuch von CA SDM*.

In jedem Abschnitt sind mehrere Zeilen mit Attribut/Wert-Paaren enthalten, von denen jedes ein Attribut des entsprechenden Objekts darstellt. Unter "Attributvariablen" finden Sie in diesem Abschnitt ausführliche Informationen dazu, wie diese Zeilen formatiert werden und was sie bedeuten.

Zeilenumbrüche in einem Attributwert werden als neue Zeilen in der Benachrichtigungsdatei reproduziert. Ihr Prozess der Benachrichtigungsmethode kann nur die Attribut- oder Wertzeilen verwenden, die mit NX_NTF und Abschnittmarkierungen beginnen. Erzeugen Sie eine Beispieldatei, und schauen Sie sich ihren Inhalt an, bevor Sie mit einer Benachrichtigungsdatei in Ihrem Prozess der Benachrichtigungsmethode arbeiten.

Weitere Informationen:

[Attributvariablen](#) (siehe Seite 366)

[Grundlegende Umgebungsvariablen](#) (siehe Seite 365)

Verwenden von Perl-Skripten

Die meisten Benachrichtigungsmethoden rufen eine ausführbare Datei oder ein Shell-Skript auf, um die Umgebungsvariablen zu lesen und die Nachricht zu senden. Dies funktioniert auf den meisten UNIX-Servern, doch auf einem Windows-Server treten mitunter Probleme beim Lesen der Umgebungsvariablen auf.

Sie können ein Perl-Skript verwenden, um dieses Problem unter Windows zu umgehen. CA SDM umfasst eine einsatzbereite Installation des Perl-Interpreters "pdm_perl". Perl-Skripts, die mit pdm_perl als Benachrichtigungsmethode aufgerufen werden, können die Umgebungsvariablen zuverlässig abrufen. Perl-Skripts können die Werte von Umgebungsvariablen lesen und formatieren und anschließend mit den restlichen Benachrichtigungen fortfahren, indem z. B. ein Pager ausgelöst oder ein E-Mail gesendet wird.

Für Windows-basierte Server können Sie das Hilfsprogramm launchit verwenden. Eine der Funktionen dieses Dienstprogramms besteht darin, Ihre Skripts oder Programme ähnlich wie bei der Verwendung der Eingabeaufforderung in einer Shell-Umgebung aufzurufen, während die Umgebungsvariablen korrekt eingestellt sind.

Wenn Sie z. B. das Perl-Skript „read_env.pl“ schreiben, das mehrere der hier beschriebenen Umgebungsvariablen lesen soll, können Sie es für eine Benachrichtigung aufrufen, indem Sie im Fenster „Benachrichtigungsmethode – Detail“ Folgendes in das Feld „Benachrichtigungsmethode“ eingeben:

```
pdm_perl script_path/read_env.pl
```

Mit dieser Benachrichtigungsmethode wird der Perl-Interpreter gestartet, und die Anweisungen im Skript "read_env.pl" werden ausgeführt.

Erstellen einer angepassten Benachrichtigungsmethode

So erstellen Sie eine angepasste Benachrichtigungsmethode:

1. Erstellen Sie ein Skript, um die Meldungsvorlage zu bearbeiten und an den Empfänger zu übermitteln. Bei dem Skript kann es sich in Abhängigkeit von der Plattform um eine beliebige ausführbare Datei handeln. Domäneninterpreter von anderen Herstellern bzw. öffentliche Domäneninterpreter können ebenfalls verwendet werden. Üblicherweise werden Bourne-Shell-Skripte unter UNIX und .bat-Dateien unter Windows verwendet. Wenn für Ihr Skript eine spezielle Vorlage erforderlich ist, müssen Sie sie erstellen.
2. Fügen Sie die neue Benachrichtigungsmethode mit Hilfe der Web-Schnittstelle Ihrem Standort hinzu.

Weitere Informationen:

[Erstellen eines Skripts](#) (siehe Seite 370)

[Hinzufügen der Benachrichtigungsmethode](#) (siehe Seite 370)

Erstellen eines Skripts

Führen Sie die folgenden Schritte aus, um ein Skript für die Benachrichtigungsmethode zu erstellen:

1. Legen Sie fest, wie die Benachrichtigung übermittelt werden soll (z. B. durch Drucken mit einem bestimmten Drucker).
2. Legen Sie den Inhalt der Benachrichtigungsmeldung fest.
3. Geben Sie an, welche Informationen aus der Meldungsvorlage in die Benachrichtigung eingeschlossen werden sollen.
4. Richten Sie ein Skript ein, mit dem die Benachrichtigung übertragen wird.
5. Fügen Sie das Skript in eine ausführbare Datei im Pfad des CA SDM-Servers ein.

Hinzufügen der Benachrichtigungsmethode

Nachdem Sie ein Skript erstellt haben, müssen Sie die neue Benachrichtigungsmethode für CA SDM definieren. Eine Benachrichtigungsmethode können Sie auf zweierlei Arten hinzufügen:

- Über die Web-Schnittstelle
- Mit Hilfe eines UNIX-Shell-Skripts

Weitere Informationen:

[Hinzufügen einer Benachrichtigungsmethode über die Web-Schnittstelle](#) (siehe Seite 371)

[Hinzufügen einer Benachrichtigungsmethode über ein UNIX-Shell-Skript](#) (siehe Seite 372)

Hinzufügen einer Benachrichtigungsmethode über die Web-Schnittstelle

Verwenden Sie die Web-Schnittstelle, um eine Benachrichtigungsmethode hinzuzufügen.

So fügen Sie eine Benachrichtigungsmethode über die Web-Schnittstelle hinzu

1. Wählen Sie im Fenster "Administrationsschnittstelle" unter "Benachrichtigungen" die Option "Benachrichtigungsmethoden" aus.

Das Fenster „Benachrichtigungsmethode – Liste“ wird angezeigt.

2. Klicken Sie auf die Schaltfläche „Neu erstellen“.

Das Fenster „Neue Benachrichtigungsmethode erstellen“ wird angezeigt.

3. Geben Sie Daten in den folgenden Feldern ein:

Symbol

(Erforderlich) Bestimmen Sie die Benachrichtigungsmethode.

In Datei schreiben

Aktivieren Sie dieses Kontrollkästchen, um Kontextinformationen der Benachrichtigungsmethode in eine Datei zu schreiben.

Beschreibung

Beschreiben Sie die Benachrichtigungsmethode.

Benachrichtigungsmethode

Geben Sie den vollständigen Pfad des ausführbaren Skripts für die Benachrichtigungsmethode an. Wenn das Skript oder Programm mit Hilfe des Systempfads aufgelöst werden kann, müssen Sie den vollen Pfad nicht angeben. Ziehen Sie bei einem Windows-Server in Betracht, das Dienstprogramm "launchit.exe" zu verwenden, um das Skript bzw. Programm aufzurufen.

Hinweis: Weitere Informationen über das Dienstprogramm "launchit" finden Sie in der *Online-Hilfe*.

Hinweis: Da die Benachrichtigungsmethode vom CA SDM-Server ausgeführt wird, müssen Sie das Skript der Benachrichtigungsmethode in ein Verzeichnis verschieben auf das über den Pfad vom Server aus zugegriffen werden kann. Geben Sie anderenfalls den vollständigen Pfad zum Skript an. Unter UNIX können Sie dies in Abhängigkeit vom ausgeführten Skript überprüfen, indem Sie den folgenden Befehl ausführen:

```
which pathname_to_script
```

Wenn mit der Benachrichtigungsmethode ein Problem auftritt, überprüfen Sie die Protokolle im Verzeichnis "\$NX_ROOT/log" (unter UNIX) bzw. im Verzeichnis "\$NX_ROOT\log" (unter Windows).

Hinzufügen einer Benachrichtigungsmethode über ein UNIX-Shell-Skript

Mit den folgenden Schritten wird ein Shell-Skript für eine Benachrichtigungsmethode erstellt, das die Benachrichtigungsmeldung an den Service Desk-Drucker SDPR2 sendet. In diesem Beispiel besteht die Benachrichtigungsmeldung aus dem Meldungskopf und dem Meldungstext aus der Meldungsvorlage:

1. Richten Sie das Shell-Skript so ein, dass es den Benachrichtigungstext zusammenstellt und die Benachrichtigung überträgt:

```
#!/bin/sh

echo "

TO:      $NX_NTF_USERID
SUBJECT:  $NX_NTF_SUMMARY
MESSAGE:

$NX_NTF_MESSAGE" |lp -dSDPR2
```

2. Nennen Sie die ausführbare Datei "sd_print", und speichern Sie sie in einem beliebigen Verzeichnis, das an Ihrem Standort für gemeinsam verwendete Skripts verwendet wird (z.B. /usr/local/netbin).
3. Definieren Sie das Shell-Skript mit chmod als ausführbare Datei.
4. Wählen Sie im Fenster "Administrationsschnittstelle" unter "Benachrichtigungen" die Option "Benachrichtigungsmethoden" aus.
5. Wählen Sie im Menü "Datei" die Option "Neu" aus.

6. Geben Sie Daten in die folgenden Felder ein:

Symbol

SDPR2

Beschreibung

Senden Sie Sicherungsbenachrichtigungen an Service Desk-Drucker SDPR2

Benachrichtigungsmethode

/usr/local/netbin/sd_print

7. Klicken Sie auf die Schaltfläche „Speichern“, um den neuen Datensatz zu speichern. Klicken Sie anschließend auf „Fenster schließen“, um das Detailfenster zu schließen.

Anpassen von Abfragen und Meldungen

In CA SDM stehen eine Reihe von Funktionen zur Verfügung, mit denen Sie den Schwerpunkt von Informationen begrenzen können, damit Sie sich auf Requests, Changes und Issues konzentrieren können, die unmittelbar gelten. Eine dieser Funktionen speichert Abfragen, die Sie verwenden können, um wichtige Informationen auf dem Scoreboard in der Administrations- oder Web-Schnittstelle anzuzeigen. Eine andere lässt Sie die Meldungen anpassen, die Mitarbeiter in Schlüsselpositionen über Ticket-Aktivitäten informieren.

Gespeicherte Abfragen können sich auf Tickets des angemeldeten Anwenders beziehen und die Zählerfelder im Scoreboard-Bereich der Administrations- und Web-Schnittstellen anpassen. Sie können Aktivitätsbenachrichtigungen so anpassen, dass Attribute aus dem Aktivitätsprotokoll-Objekt und Informationen zu bestimmten Tickets enthalten sind.

Weitere Informationen:

[Scoreboard-Abfragen](#) (siehe Seite 374)

[ITIL-spezifische Abfragen](#) (siehe Seite 381)

[Anpassen der Meldung für Aktivitätsbenachrichtigungen](#) (siehe Seite 381)

Scoreboard-Abfragen

Eine der Tabellen in der Datenbank Cr_Stored_Queries definiert gespeicherte Abfragen. Diese gespeicherten Abfragen sind den SQL-Abfragen sehr ähnlich und können verwendet werden, um die Zählerfelder auf Knoten im Scoreboard-Bereich in Administrations- und Web-Schnittstellen anzupassen. Die Zählerfelder geben an, wie viele Datensätze der Abfrage entsprechen. Sie können beispielsweise angeben, wie viele Anfragen unterschiedlichen Typs dem angemeldeten Benutzer zugeordnet wurden.

Jeder Benutzer kann die auf seinem Scoreboard angezeigten Zählerfelder anpassen (dies wird in der Online-Hilfe erläutert). Allerdings muss der Systemadministrator zuerst die verschiedenen Anfragetypen, die in diesen Zählerfeldern gezählt werden können, als gespeicherte Abfragen definieren. Informationen zu Scoreboard-Abfragen finden Sie im *Administrationshandbuch*.

Hinweis: Scoreboard-Zählungen sind falsch, wenn die Werte von Datenbankabfragen gleich NULL sind. Wenn die Scoreboard-Abfrage beispielsweise angibt, dass assignee.organization = xyz, während für einen Datensatz ein Feld "Bevollmächtigter" leer (NULL) ist, ist dieser Datensatz nicht in der Scoreboard-Zählung enthalten.

Gespeicherte Abfragen für angemeldete Benutzer

Zwei der Felder, die im Fenster „Gespeicherte Abfrage – Detail“ definiert werden müssen, sind „Where-Klausel“ und „Beschriftung“. Beide Felder können Ausdrücke enthalten, die für den angemeldeten Benutzer angepasst sind. Gespeicherte Abfragen beziehen sich nicht auf Tabellennamen und Spalten, sondern auf Objekte und Attribute. Eine gespeicherte Abfrage, die für den angemeldeten Benutzer angepasst ist, besteht aus den folgenden zwei Teilen:

Das Objekt (z.B. "cr" für eine Anfrage)

Dies ist für gewöhnlich links vom Gleichheitszeichen (=) angegeben. Die Syntax für diesen Teil der gespeicherten Abfrage ist:

```
att_name[.att_name...].SREL_att_name
```

Eine gespeicherte Abfrage weist immer einen Typ auf, der dem Namen des Objekts entspricht, für das die Abfrage ausgeführt wird, und der den Kontext für die Abfrage liefert. In der oben angegebenen Syntax muss das erste att_name der Attributname des Kontextobjekts sein.

Der angemeldete Benutzer (die Instanz des "cnt"-Objekts für diesen Benutzer)

Dies muss rechts vom Gleichheitszeichen (=) angegeben sein, wenn die Tickets abhängig vom Attribut des angemeldeten Benutzers auszuwählen sind. Die Syntax für diesen Teil der gespeicherten Abfrage ist:

```
@att_name[.att_name...].SREL_att_name
```

Hinweis: Weitere Informationen zu Objekten und Attributen finden Sie im *Technischen Referenzhandbuch von CA SDM*.

Syntax des „cr“-Objekts

Verwenden Sie die folgende Syntax, wenn auf das Anforderungsobjekt (cr) verwiesen wird:

att_name[.att_name...].SREL_att_name

In diesem Beispiel wird die Position der Person identifiziert, die für die Verarbeitung dieses Tickets zugeordnet wurde. In diesem Beispiel ist der Objektname ausgelassen, da der Typ der gespeicherten Abfrage das „cr“-Objekt impliziert:

`assignee.location=@cnt.location AND active=1`

Verantwortlicher

Das Attribut im Anforderungsobjekt, das dem Feld „Bevollmächtigter“ in der entsprechenden Tabelle zugeordnet ist. Das assignee-Attribut ist z. B. im „cr“-Objekt als „SREL agt“ definiert, was bedeutet, dass es sich auf die agt-Factory bezieht. Die agt-Factory ist Teil der „cnt“-Objektdefinition.

Standort

Das Attribut im „cnt“-Objekt, das dem Feld „c_l_id“ in der Tabelle „Contact“ zugeordnet ist. Das location-Attribut ist im „cnt“-Objekt mit „SREL loc“ definiert, was bedeutet, dass es sich auf das „loc“-Objekt bezieht.

WHERE-Klausel

Das folgende Beispiel veranschaulicht einen Wert, den Sie in einer WHERE-Klausel codieren können:

`assignee.location=@cnt.location AND active=1`

Wenn die gespeicherte Abfrage eine Anforderung ist, wählt diese Abfrage alle aktiven Anforderungen aus, in denen die Position des Zuständigen der Position des angemeldeten-Benutzers entspricht.

Beschriftung

Attribute im „cnt“-Objekt können in Beschriftungen auf dieselbe Weise eingeschlossen werden, wie in WHERE-Klauseln. Im Folgenden ist ein Beispiel für die Verwendung eines Attributs im „cnt“-Objekt in einer Beschriftung angegeben:

`@cnt.location.name-Aufrufe`

Diese Beschriftung schließt den Namen einer Lokation (z.B. Phoenix) ein, wobei @cnt.location.name durch Phoenix ersetzt wird, wenn die Beschriftung in einem Fenster angezeigt wird. Die Beschriftung wird als „Phoenix-Aufrufe“ angezeigt.

Das IN-Schlüsselwort

Mit Hilfe des IN-Schlüsselworts kann eine gespeicherte Abfrage auf zwei (oder mehr) Tabellen verweisen, ohne dass eine Kombination erzeugt wird. Dies kann die Effizienz bei der Ausführung der Abfrage erheblich steigern. Es wird folgendermaßen codiert:

```
SREL_att_name IN ( value1 [, value2 [,...]] )
```

Anfrageabfragen können z. B. folgendermaßen codiert werden:

```
category.sym IN (\'Soft%\', \'Email\')
```

Dies resultiert in der folgenden SQL WHERE-Klausel:

```
category IN (SELECT persid FROM prob_ctg WHERE sym LIKE \'Soft\' OR sym = \'Email\')
```

Ein Verwendungszweck von IN besteht in der Vermeidung kartesischer Produkte. Die folgende Abfrage z. B. führt zu einem kartesischen Produkt und ist äußerst ineffizient:

```
assignee.last_name LIKE \'MIS%\' OR group.last_name LIKE \'MIS%\'
```

Durch die Verwendung des IN-Schlüsselworts führt die Abfrage zu keinem kartesischen Produkt. Es werden in der Tat gar keine Verbindungen geschaffen, wie durch das folgende Beispiel veranschaulicht wird:

```
assignee.last_name IN \'MIS%\' OR group.last_name IN \'MIS%\'
```

Hinweis: Die Klammern, die normalerweise die Werteliste auf der rechten Seite von IN umschließen, können weggelassen werden, wenn nur ein Wert in der Liste vorhanden ist. Genauso sollten Sie Verbindungen in Datenaufteilungen vermeiden, indem Sie Datenaufteilungen konvertieren, wie im Folgenden dargestellt:

```
assignee.last_name LIKE \'Smith\'
```

in:

```
assignee = U'374683AA82ACE34AB999A042F3A0BA2E'
```

Dabei gilt:

U

angibt, dass der Wert eine UUID ist.

'374683AA82ACE34AB999A042F3A0BA2E'

Die 32 Zeichen in einfachen Anführungszeichen entsprechen der Zeichenfolgendarstellung der eigentlichen UUID.

Somit werden Joins vermieden, es kommt aber auch zu einem Verlust an Klarheit. Durch Verwendung von IN kann die gleiche Aufteilung (siehe folgendes Beispiel) mit der Klarheit der ersten Version sowie nahezu der gleichen Effizienz wie die zweite Version wie folgt geschrieben werden:

```
assignee.last_name IN 'Smith'
```

CA SDM unterstützt die IN-Klausel, wenn sie auf QREL- oder BREL-Listen angewendet wird. Wenn Sie z. B. alle Anfragen mit Assets finden möchten, die einem anderen spezifischen Asset (mit ID 374683AA82ACE34AB999A042F3A0BA2E) übergeordnet sind, lautet die entsprechende WHERE-Klausel folgendermaßen:

```
affected_resource.[parent]child_hier.child IN  
(U'374683AA82ACE34AB999A042F3A0BA2E')
```

Der erste Teil der Klausel "*Betroffene_Ressource*" ist eine SREL (ein Fremdschlüssel) des "cr"-Objekts (Anfrage), das auf die Tabelle "Network_Resource" verweist. Der Teil „*child_hier*“ entspricht einer Liste mit „*hier*“-Objekten, die auf hierarchische Beziehungen verweisen. Der letzte Teil „*child*“ bildet den ersten Teil der WHERE-Klausel für die untergeordnete IN-Abfrage. Der Teil „374683AA82ACE34AB999A042F3A0BA2E“ entspricht dem Fremdschlüsselwert, der mit *child* übereinstimmen soll. *[parent]* gibt die Rückgabe der Unterabfrage an. Da der ID-Wert eine Zeichenfolgendarstellung einer UUID ist, muss er als solcher angegeben und wie folgt geschrieben werden: U'374683AA82ACE34AB999A042F3A0BA2E'.

Nachfolgend ist ein Beispiel für den eigentlich generierten SQL-Code angegeben, der alle Anfragen liefert, bei denen das Asset einem bestimmten Asset übergeordnet ist:

```
SELECT Call_Req.id FROM Call_Req WHERE Call_Req.affected_rc IN (SELECT hier_parent  
FROM Asset_Assignment WHERE hier_child = U'374683AA82ACE34AB999A042F3A0BA2E')
```

Um mehrere übergeordnete Assets abzufragen, können Sie in dem Teil in Klammern () des SQL-Codes eine durch Kommas getrennte Liste angeben, wie im folgenden Beispiel gezeigt:

```
affected_resource.[parent]child_hier.child IN  
(U'374683AA82ACE34AB999A042F3A0BA2E', U'374683AA82ACE34AB999A042F3A0BA2E')
```

Der Attributname in eckigen Klammern ([]) wird verwendet, um den SELECT-Teil der Unterabfrage zu bilden. Die Klammernnotation wird nicht für die Gruppe "Gespeicherte Abfragen" verwendet, die zum Lieferumfang von Service Desk 6.0 gehört, wie im folgenden Beispiel dargestellt:

```
(assignee = @cnt.id OR group.group_list.member IN (@cnt.id)) AND active = 1
```

Hinweis: Wenn die Klammernnotation nicht verwendet wird, geht das SQL-Subsystem davon aus, dass es sich um den Attributnamen des ersten Symbols in der Punktnotation handelt. In diesem Fall funktioniert es eher zufällig, dass das Objekt „group_list“ über das Attribut „group“ verfügt. Wenn dieses Attribut einen anderen Namen aufweisen würde, könnte die WHERE-Klausel nicht analysiert werden. Die entsprechende Klausel mit Klammern lautet folgendermaßen:

```
(assignee = @cnt.id OR group.[group]group_list.member IN (@cnt.id)) AND active = 1
```

Hinweis: Sie können die Punktnotation nicht erweitern. Folgendes funktioniert beispielsweise nicht:

```
affected_resource.[parent]child_hier.child.name IN ('chicago1')
```

Prioritätsbasierte Abfragen

Die Tabelle "Priorität" in der Datenbank verfügt über die Spalten "sym" und "enum". Bei den Werten, die dem Benutzer angezeigt werden, handelt es sich um die „sym“-Werte. Die Anwendung sieht die „sym“-Werte jedoch auf Basis der „enum“-Werte. Derzeit entsprechen die „enum“-Werte der Umkehrung der standardmäßigen „sym“-Werte 1 bis 5.

Beispiel

Symbol	Aufzählung
1	5
2	4
3	3
4	2
5	1

Wenn Sie beim Schreiben einer gespeicherten Abfrage auf den Wert 5 verweisen, suchen Sie daher tatsächlich nach Priorität 1, solange Sie nicht mit .sym angeben, welches Attribut angezeigt werden soll.

Wichtig! Sie dürfen die vom Produkt zugewiesenen Standardwerte für "enum" nicht ändern. Wenn Sie neue "sym"-Werte hinzufügen, fahren Sie einfach nach dem höchsten "enum"-Wert fort.

Zeitbasierte Abfragen

Zeitspannen können verwendet werden, um zeitbasierte gespeicherte Abfragen zu erstellen. Eine Zeitspanne definiert eine Zeitperiode, die relativ zum aktuellen Datum sein kann. Eine Zeitspanne kann sich z. B. auf heute, gestern, letzte Woche oder letzten Monat beziehen. Eine Zeitspanne hat einen Namen, wie z. B. HEUTE oder GESTERN. Sie beziehen sich auf eine Zeitspanne in einer gespeicherten Abfrage, indem Sie eine der folgenden integrierten Funktionen verwenden:

StartAtTime (Name der Zeitspanne)

Dies bezieht sich auf den Beginn der Periode, die von der Zeitspanne beschrieben wird.

EndAtTime (Name der Zeitspanne)

Dies bezieht sich auf das Ende der Periode, die von der Zeitspanne beschrieben wird.

Die Syntaxregeln für gespeicherte Abfragen erfordern, dass der Name der Zeitspanne von einfachen Anführungszeichen eingeschlossen wird, wobei dem Anführungszeichen ein Backslash-Zeichen vorangestellt ist. Um sich z. B. auf den Beginn der vergangenen Woche zu beziehen, geben Sie Folgendes an:

```
StartAtTime(\'PAST_WEEK\')
```

Durch den Zeitablauf ist es erforderlich, gespeicherte Abfragen, die einen Verweis auf eine Zeitspanne enthalten, in regelmäßigen Abständen zu aktualisieren. So ändert sich beispielsweise das Intervall, das durch „gestern“ beschrieben wird, um Mitternacht. Im Fenster „Zeitspanne – Detail“ geben Sie die Startzeit, Endzeit und Auslöser-Zeit für Aktualisierungen an.

Startzeit

Die Startzeit gibt den Anfang einer Zeitspanne absolut oder relativ an. Im Folgenden werden die Felder im Bereich „Startzeit“ des Fensters „Zeitspanne – Detail“ erläutert:

Jahr

Ein explizites Jahr (z. B. 2000) oder ein relatives Jahr (z. B. +1 (nächstes Jahr) oder -1 (letztes Jahr))

Monat

Ein expliziter Monat von 1 (Januar) bis 12 (Dezember) oder ein relativer Monat (z. B. +1 (nächster Monat) oder -1 (letzten Monat))

Tag

Ein expliziter Tag von 1 bis 31 oder ein relativer Tag (z. B. +1 (morgen) oder -1 (gestern))

Stunde

Eine explizite Stunde von 0 bis 24 oder eine relative Stunde (z. B. +1 (nächste Stunde) oder -1 (letzte Stunde))

Minute

Eine explizite Minute von 0 bis 59 oder eine relative Minute (z. B. +1 oder -1)

Endzeit

Die Endzeit gibt das Ende einer Zeitspanne absolut oder relativ an. Die Endzeitfelder im Fenster „Zeitspanne – Detail“ entsprechen den Startzeitfeldern im Fenster „Zeitspanne – Detail“.

Auslöser-Zeit

Das Feld „Auslöser-Zeit“ gibt an, wann eine WHERE-Klausel einer gespeicherten Abfrage, die einen Verweis auf eine Zeitspanne enthält, erneut erstellt und die gespeicherte Abfrage aktualisiert wird. Die Auslöser-Zeit muss relativ zur aktuellen Uhrzeit sein, wie im Folgenden beschrieben:

Jahr

Muss ein relatives Jahr von -1 (letztes Jahr) bis +36 (36 Jahre ab jetzt) sein.

Monat

Muss ein relativer Monat von -1 (letzter Monat) bis +11 (11 Monate ab jetzt) sein.

Tag

Muss ein relativer Tag von -1 (gestern) bis +31 (31 Tage ab jetzt) sein.

Stunde

Muss eine relative Stunde von -1 (letzte Stunde) bis +23 (23 Stunden ab jetzt) sein.

Minute

Muss eine relative Minute von +9 (9 Minuten ab jetzt) bis +59 (59 Minuten ab jetzt) sein.

ITIL-spezifische Abfragen

Probleme und Incidents sind Anfragen mit einem bestimmten Wert im Attribut *type*: "I" für Incidents und "P" für Probleme.

Die folgende gespeicherte Abfrage listet alle Incidents auf, in denen die Organisation des Zuständigen bzw. der Gruppe mit der Organisation des angemeldeten Analysten identisch ist:

```
assignee.organization IN @cnt.organization OR group.organization IN  
@cnt.organization) AND active = 1 AND type = \'I\'
```

Die Abfrage für Probleme ist mit Ausnahme des Typs = \'P\' identisch.

Anpassen der Meldung für Aktivitätsbenachrichtigungen

Benachrichtigungen können automatisch gesendet werden, wenn Anfrageaktivitäten stattfinden.

Hinweis: Informationen zu Benachrichtigungsmeldungen und Anweisungen zum Definieren von Aktivitätsbenachrichtigungen finden Sie im *Administrationshandbuch*.

Zwei der Felder, die im Fenster „Aktivitätsbenachrichtigungen – Detail“ definiert werden müssen, sind „Titel der Benachrichtigungsmeldung“ und „Benachrichtigungstext“. Diese beiden Felder können Attribute des Aktivitätsprotokollobjekts enthalten ("alg" für Anfragen/Incidents/Probleme, "chgalg" für Changes und "issalg" für Issues. Diese drei Aktivitätsprotokollobjekte sind fast identisch) und können die spezifische Anfrage identifizieren, die sich auf die Aktivität bezieht.

Formatieren von Attributen für Aktivitätsbenachrichtigungen

Das optionale Formatieren und Umwandeln von individuellen Attributen kann mit den unten aufgeführten Eigenschaften erzielt werden. Dies kann hilfreich sein, insbesondere wenn eine HTML-Benachrichtigung formatiert wird, in der die Daten im Attribut möglicherweise umgewandelt werden müssen, um dem HTML-Standard zu entsprechen.

Verwenden Sie zum Einschließen von Formatierungen die folgende Syntax:

```
@{property=value property=value:attribute_name}
```

Paare von Eigenschaftswerten werden durch mindestens ein Leerzeichen getrennt. Bei ihnen muss die Groß-/Kleinschreibung nicht beachtet werden. Ein Doppelpunkt trennt die Formatierungseigenschaften vom Attributnamen. Wenn keine Eigenschaften aufgeführt sind, wird das Attribut weder formatiert noch umgewandelt.

In der folgenden Tabelle sind die verfügbaren Formatierungseigenschaften aufgeführt:

Property	Beschreibung
DATE_FMT	Gibt das Datumsformat für Attribut an. Gültige Werte sind: TT/MM/JJJJ MM-TT-JJJJ TT/MM/JJJJ TT-MM-JJJJ JJJJ/MM/TT JJJJ-MM-TT Gültig nur für Datumsattribute. Daten, die in Zeichenfolgen eingebettet sind, sind nicht betroffen.

Property	Beschreibung
ESC_STYLE=NONE HTML URL	Gibt den Umwandlungstyp des formatierten Texts an. Gültige Werte sind: NONE Standardeinstellung. Gibt an, dass für kein Zeichen im Textkörper eine besondere Behandlung erforderlich ist. HTML Folgende Zeichen sind in HTML-Text von besonderer Bedeutung und erfordern daher eine besondere Behandlung: ■ & wird &amp; ■ " wird &quot; ■ < wird &lt; ■ > wird &gt; URL Übersetzen Sie alle Zeichen, die keine Buchstaben oder Ziffern sind, sowie '@*-_.#' bis '%xx', wobei xx eine hexadezimale Kodierung des übersetzten Zeichens ist.
JUSTIFY=LEFT CENTER RIGHT TRUNCATE WRAP LINE	Gibt die Ausrichtung des formatierten Textes an. Gültige Werte lauten: TRUNCATE (Standardwert, wenn formatiert) Kürzt Text entsprechend dem Eigenschaftswert WIDTH ab, wenn eine positive Ganzzahl angegeben ist. Wenn ESC_STYLE=HTML, wird die HTML-Formatierung durch Ersetzen von "<" und ">" durch "&lt;" und "&gt;" eliminiert (siehe auch KEEPLINKS und KEEPTAGS). LEFT CENTER RIGHT Stellt genau die durch das Argument WIDTH angegebene Breite an Zeichen her, je nach Bedarf gekürzt oder mit Leerzeichen aufgefüllt, wobei eingebettete neue Zeilen durch ein Leerzeichen ersetzt werden. Wenn ESC_STYLE=HTML, wird der Ausgabertext durch die Tags <pre> und </pre> begrenzt. Das Argument WIDTH muss als positive Ganzzahl angegeben werden. WRAP Gleiche Eigenschaft wie LEFT, mit Ausnahme dass beim Textumbruch Wörter berücksichtigt werden (d. h. kein Zeilenumbruch innerhalb eines Worts). LINE Entspricht TRUNCATE mit der Ausnahme, dass alle eingebetteten Zeilenumbrüche durch das Tag
 ersetzt werden, wenn ESC_STYLE=HTML.
KEEPLINKS=YES NO	Wenn KEEPLINKS=YES angegeben ist, wird die Aktion JUSTIFY=LINE oder JUSTIFY=TRUNCATE geändert, um die HTML-Anchor-Tags (Aktion:) zu bewahren, während alle anderen „<“- und „>“-Zeichen konvertiert werden. Gegenseitig austauschbar mit KEEPTAGS. Nur gültig, wenn ESC_STYLE=HTML.

Property	Beschreibung
KEEPNL=YES NO	Die normale Aktion von PDM_FMT soll alle eingebetteten Zeilenvorschübe und alle folgenden Leerzeichen in ein einzelnes Leerzeichen umwandeln. Wenn KEEPNL=YES angegeben ist, werden eingebettete Zeilenvorschübe beibehalten. Dieses Argument wird für JUSTIFY=LINE ignoriert.
KEEPTAGS=YES NO	Wenn KEEPTAGS=YES angegeben ist, wird die Aktion JUSTIFY=LINE oder JUSTIFY=TRUNCATE modifiziert, sodass alle HTML-Tags zu beibehalten werden. Gegenseitig austauschbar mit KEEPLINKS. Nur gültig, wenn ESC_STYLE=HTML.
PAD=YES NO	Wenn PAD=NO angegeben ist, wandelt PDM_FMT leere Zeichenfolgen nicht zu einem einzelnen Leerzeichen um. Dies ist die normale Aktion, wenn WIDTH nicht null ist, oder JUSTIFY TRUNCATE oder WRAP ist.
WIDTH=nn	Wenn diese Eigenschaft nicht null ist, gibt sie an, dass der Text genau auf die für WIDTH angegeben Zeichen formatiert werden soll.

Um z. B. die Anfragebeschreibung einer HTML-Benachrichtigung durch Umwandeln von HTML-spezifischen Zeichen umzuwandeln, indem
-Tags für Zeilenumbrüche hinzugefügt und HTML-Links als Verknüpfungen beibehalten werden, geben Sie Folgendes ein:

```
@{ESC_STYLE=HTML JUSTIFY=LINE KEEPLINKS=YES:call_req_id.description}
```

Um das Öffnungsdatum einer Anfrage im europäischen Format zu formatieren, geben Sie Folgendes ein:

```
@{DATE_FMT=DD-MM-YYYY:call_req_id.open_date}
```

Attribute des Aktivitätsprotokollobjekts

Um ein Attribut vom Aktivitätsprotokollobjekt einzuschließen, schließen Sie dies im Feld „Titel der Benachrichtigungsmeldung“ oder „Benachrichtigungstext“ ein:

```
@{Attributname}
```

Der Name des Objekts ("alg", "chgalg" oder "issalg") ist der Standardwert und muss nicht angegeben werden. Um z. B. den Typ der Aktivität in den Titel der Meldung einzuschließen, geben Sie diesen in das Feld „Titel der Benachrichtigungsmeldung“ ein (zusammen mit dem, was noch im Titel angezeigt werden soll):

```
@{Typ}
```

Um eine Beschreibung der Aktivität in den Text der Meldung einzuschließen, geben Sie diesen in das Feld „Benachrichtigungstext“ ein (zusammen mit dem, was noch im Text angezeigt werden soll):

```
@{Beschreibung}
```


Informationen zu bestimmten Changes

Bei Meldungen, die Informationen zu einem bestimmten Change liefern, der die Benachrichtigung ausgelöst hat, muss das Feld "Titel der Benachrichtigungsmeldung" oder "Benachrichtigungstext" ein Attribut im Aktivitätsprotokollobjekt enthalten, das auf das Change-Objekt verweist. Geben Sie die Referenz in diesem Format ein:

`@{change_id.chg_att_name}`

Für diese Referenz gilt Folgendes:

@

Zeigt an, dass dieser Ausdruck ersetzt werden soll.

change_id

Das Attribut im Aktivitätsprotokollobjekt, das den Ausdruck mit einer bestimmten Instanzierung des Change-Objekts (chg) verknüpft.

chg_att_name

Ein beliebiges Attribut im „chg“-Objekt.

Um z. B. die Priorität des Change im Titel der Meldung einzuschließen, geben Sie Folgendes in das Feld "Titel der Benachrichtigungsmeldung" ein (zusammen mit dem, was noch im Titel angezeigt werden soll):

`@{change_id.priority.sym}`

Um im Text der Meldung zu identifizieren, wer den Change (betroffener Endbenutzer) berichtet hat, geben Sie Folgendes im Feld "Benachrichtigungstext" ein (zusammen mit dem, was noch im Text angezeigt werden soll):

`@{change_id.requestor.combo_name}`

Wenn Sie einen bestimmten Change anhand der Nummer erneut öffnen, können Sie die Meldung entsprechend mit folgender Syntax anzeigen:

Change @{change_id.chg_ref_num} erneut öffnen

Hinweis: Bei Meldungen, die Informationen zu einem bestimmten Issue liefern, der die Benachrichtigung ausgelöst hat, muss das Feld "Titel der Benachrichtigungsmeldung" oder "Text der Benachrichtigungsmeldung" ein Attribut "iss" im Aktivitätsprotokollobjekt enthalten, das auf den Issue verweist. Die in diesem Abschnitt enthaltenen Informationen zu Anfragen und Changes sowie die Informationen zu Objekten und Attributen im *Technischen Referenzhandbuch zu CA SDM* helfen Ihnen dabei, dies zu erreichen.

Um z. B. die Priorität des Issue im Titel der Meldung einzuschließen, geben Sie Folgendes in das Feld "Titel der Benachrichtigungsmeldung" ein (zusammen mit dem, was noch im Titel angezeigt werden soll):

@{issue_id.priority.sym}

Informationen zu bestimmten Anfragen

Bei Meldungen, die Informationen zu einer bestimmten Anfrage liefern, welche die Benachrichtigung ausgelöst hat, muss das Feld "Titel der Benachrichtigungsmeldung" oder "Benachrichtigungstext" ein Attribut im Aktivitätsprotokollobjekt enthalten, das auf das Anfrageobjekt verweist. Geben Sie den Verweis in folgendem Format ein:

`@{call_req_id.cr_att_name}`

@

Zeigt an, dass dieser Ausdruck ersetzt werden soll.

call_req_id

Das Attribut im Aktivitätsprotokollobjekt, das den Ausdruck mit einer bestimmten Instanzierung des Anfrageobjekts (cr) verknüpft.

cr_att_name

Ein beliebiges Attribut im „cr“-Objekt.

Um z. B. die Auswirkung der Anfrage im Titel der Meldung einzuschließen, geben Sie diese in das Feld "Titel der Benachrichtigungsmeldung" ein (zusammen mit dem, was noch im Titel angezeigt werden soll):

`@{call_req_id.impact.sym}`

Um die betroffene Ressource im Text der Meldung zu identifizieren, geben Sie diese in das Feld „Benachrichtigungstext“ ein (zusammen mit dem, was noch im Text angezeigt werden soll):

`@{call_req_id.affected_resource.name}`

Wenn Sie eine bestimmte Anfrage anhand der Nummer erneut öffnen möchten, können Sie die Meldung mit folgender Syntax anzeigen:

Anfrage `@{call_req_id.ref_num}` erneut öffnen

Es gibt zahlreiche weitere Mechanismen, mit denen Meldungen gesendet werden können, die sich im Kontext der Anfrage selbst (oder eines Change oder Issue) befinden. Wenn der Kontext die Anfrage selbst ist, müssen (und können) Sie den Teil "call_req_id" der Referenz nicht verwenden. In diesen Fällen müssen Sie Folgendes verwenden:

„@{ref_num}“ anstelle von „@{call_req_id.ref_num}“

Anpassen der Webschnittstelle

Die CA SDM-Web-Schnittstelle (auch als Browserschnittstelle bezeichnet) stellt Ihnen Funktionen von CA SDM über das Internet bereit. Diese Funktionen umfassen das Öffnen, Aktualisieren oder Schließen von Tickets, das Anzeigen und Bereitstellen von Ankündigungen und sowie das Zugreifen auf unterstützende Datentabellen. Sie ermöglichen das unabhängige Durchsuchen der Knowledge Base, wodurch die Anzahl der Anrufe beim Service Desk verringert und die Lösungszeiten verkürzt werden können. Die Web-Schnittstelle kann vollständig angepasst und mit vielen häufig genutzten Webbrowsern verwendet werden.

Nachdem Sie die Web-Schnittstelle installiert und konfiguriert haben, können Sie diese in Ihre vorhandene Web-Schnittstelle integrieren und an Ihre Bedürfnisse anpassen. Voraussetzung dafür ist, dass Sie mit HTML und dem an Ihrem Standort verwendeten Webbrowser vertraut sind.

Hinweis: In der WSP-Design-Ansicht können CA SDM-Steuerelemente (PDM_MACROs) verwendet werden. Wenn Sie Formulare bearbeiten, die keine CA SDM-Steuerelemente enthalten, können Sie nur die Registerkarte "Quellcode" verwenden. Die Webformulare "Kunde" und "Mitarbeiter" enthalten keine CA SDM-Steuerelemente und werden deshalb nicht in der Registerkarte "Design", sondern in der Registerkarte "Quellcode" angezeigt. Einige Formulare für Analysten enthalten keine CA SDM-Steuerelemente und werden deshalb auch nicht in der Registerkarte "Quellcode" angezeigt.

Wichtig! CA SDM r12.9 verwendet keine angepassten .mac-Dateien für "pdm_macro" im Verzeichnis "\$NX_ROOT\$\site\mods\www\macro" mehr. Sie können keine Makros anpassen.

Wichtig! Der Technische Support bietet keine Unterstützung für Design und Fehlerbehebung von Anpassungen (dies gilt auch für Dokumentation und Online-Hilfe). Es werden jedoch allgemeine Informationen zur Anpassung der Web-Schnittstelle von CA SDM zur Verfügung gestellt. Sie sollten sich bewusst sein, dass Sie für Ihre Anpassungen selbst verantwortlich sind. Der Technische Support für CA SDM kann Ihnen helfen, die Informationen zur Anpassung richtig zu interpretieren und zu verstehen.

Die Unterstützung für die Anpassungsverfahren stellt ebenfalls sicher, dass die Verfahren und Einrichtungen wie dokumentiert ausgeführt werden. Achten Sie darauf, dass sie keine nicht dokumentierten Funktionen nutzen bzw. keine dokumentierten Funktionen über die beschriebenen Leistungen hinaus verwenden. Eine derartige Nutzung wird nicht unterstützt und kann zu Systemproblemen oder Instabilität führen, die keinen Bezug zur Anpassung aufweisen. Aus diesem Grund können Support-Mitarbeiter Sie darum bitten, Anpassungen zu entfernen und Probleme danach zu reproduzieren. Standorte sollten sich hierauf vorbereiten, indem sie sorgfältig die Richtlinien zum Platzieren von Änderungen in der Baumstruktur mit dem Verzeichnis "site mods" befolgen und Änderungsprotokolle verwalten. Standorte, an denen häufig komplexe oder umfassende Änderungen durchgeführt werden, sollten die CA SDM-Anpassung als Projekt zur Entwicklung von Software mit disziplinierter Quellcodeverwaltung, Quellcodetests und gesteuerten Freigaben an die Produktion.

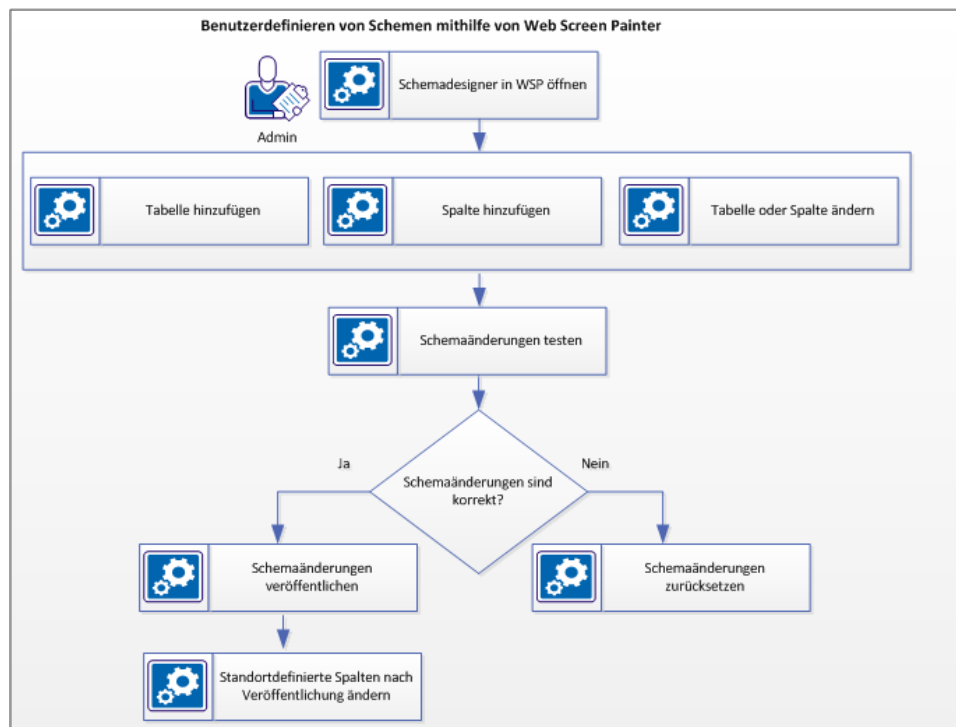
Die Migration der Anpassungen zwischen verschiedenen Versionen kann mit besonderen Herausforderungen verbunden sein. Bei der Entwicklung des Produkts wurde besonders darauf geachtet, dass der in die Anpassung investierte Aufwand erhalten bleibt. Grundsätzlich wird jedoch davon ausgegangen, dass Anpassungen des Produkts nur nach den in diesem Handbuch dokumentierten Anleitungen erfolgt sind. Dies gilt insbesondere für die Einordnung aller Anpassungen in der Baumstruktur "site mods". Darüber hinaus werden Patches, die vom Support der zweiten Ebene bereitgestellt werden, unter denselben Voraussetzungen geschrieben. Patches und Aktualisierungen eines Systems mit ungeregelten Anpassungen stellen ein riskantes Unternehmen dar, das häufig kostenintensive Systemausfallzeiten nach sich zieht. Diese Ausfallzeiten können Sie vermeiden, indem Sie die Anweisungen in diesem Handbuch befolgen und die soliden Software-Engineering-Richtlinien beachten.

Hinweis: Informationen zum Sichern und Konfigurieren der Web-Schnittstelle finden Sie im *Administrationshandbuch*.

So passen Sie das Schema mithilfe von Web Screen Painter an

Verwenden Sie den Schemadesigner von Web Screen Painter, um das Datenbankschema von CA SDM zu ändern. Der Schemadesigner bietet eine grafische Anwenderschnittstelle zum Überprüfen und Ändern dieses Schemas.

Folgendes Diagramm zeigt, wie ein Schema mithilfe von Web Screen Painter angepasst wird:



Gehen Sie wie folgt vor:

1. [Überprüfen Sie die Hinweise zu Web Screen Painter](#) (siehe Seite 390).
2. [Öffnen Sie den Schemadesigner in WSP](#) (siehe Seite 391).
3. [Fügen Sie eine Tabelle hinzu](#) (siehe Seite 391) oder [fügen Sie eine Spalte hinzu](#) (siehe Seite 394) oder [ändern Sie die Tabelle oder Spalte](#) (siehe Seite 399).
4. Testen Sie die Schemaänderungen. Beispiel: Erstellen, aktualisieren und zeigen Sie Webformulare an, die Sie verwenden, bevor Sie Änderungen an der physischen Datenbank vornehmen. Weitere Informationen über das Erstellen von Webformularen finden Sie unter dem Thema "[So passen Sie die Web-Schnittstelle mithilfe von WSP an](#)" (siehe Seite 408).
 - Wenn die Schemaänderungen richtig sind, [veröffentlichen Sie die Schemaänderungen](#) (siehe Seite 400).
 - Wenn die Schemaänderungen nicht richtig sind, [kehren Sie die Schemaänderungen um](#) (siehe Seite 405).
5. (Im Bedarfsfall) [Ändern Sie standortdefinierte Spalten nach der Veröffentlichung](#) (siehe Seite 406).

Überprüfen Sie die Hinweise zu Web Screen Painter

Beachten Sie folgende Informationen, bevor Sie Web Screen Painter verwenden:

- Sie können WSP nicht verwenden, um die Länge von vorhandenen Spalten zu ändern. Es wird empfohlen, dass Sie auch *keine* anderen Tools hierfür verwenden. Die Änderung der Länge von vorhandenen Spalten wird nicht unterstützt. Dies könnte dazu führen, dass der Zugriff von anderen Anwendungen auf die CA SDM-Datenbank fehlschlägt.

Wichtig! Kürzen oder löschen Sie kein vorhandenes Feld, denn dadurch könnten Fehler in CA SDM auftreten.
- Gehen Sie beim Hinzufügen von Spalten zu einer vorhandenen Tabelle sorgfältig vor, da Sie unbeabsichtigt die mögliche Datensatzlänge der zugrunde liegenden Datenbank überschreiten können. Prüfen Sie die Spezifikationen für die Datenbank, die Sie mit CA SDM verwenden, und nehmen Sie Änderungen innerhalb der Grenzen dieser Datenbank vor.
- Das Veröffentlichen von Änderungen am Datenbankschema könnte je nach den durchgeführten Änderungen und dem Leistungsvermögen der zugrunde liegenden Datenbank begrenzte oder beträchtliche Ausfallzeiten erfordern.

- Wenn Sie ein neuer Anwender von CA SDM sind, ist es einfacher, alle Änderungen während des Testens durchzuführen, anstatt bis zur Produktion zu warten.
- Überprüfen Sie allgemeinen Verfahren, die Sie vor und nach dem Ändern des Datenbankschemas durchführen müssen.
- Verwenden Sie zum Anpassen des Schemas spezifische Verfahren. Für die meisten dieser Verfahren sind Beispiele für eine Änderung angegeben, die Sie möglicherweise am Standarddatenbankschema vornehmen möchten.

Öffnen Sie den Schemadesigner in WSP

Um mit dem Schemadesigner zu arbeiten, stellen Sie sicher, dass WSP auf dem CA SDM-Server installiert ist. Hinweis: Weitere Informationen zur WSP-Installation finden Sie im *Implementierungshandbuch*.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei folgendem CA SDM-Server an, wo WSP abhängig von Ihrer CA SDM-Konfiguration installiert ist:
 - Konventionell: Primärserver
 - Erweiterte Verfügbarkeit: Hintergrundserver
2. Starten Sie WSP, indem Sie eine der folgenden Aktionen durchführen, abhängig vom Betriebssystem, das auf dem CA SDM-Server installiert ist:
 - (Windows) Wählen Sie im Startmenü die Option "Programme", "CA", "CA SDM", "Web Screen Painter" aus.
 - (UNIX) Geben Sie den Befehl "pdm_wsp" mit "\$NX_ROOT/bin" in Ihren Pfad ein.

Das Web Screen Painter-Anmeldefenster wird geöffnet.

3. Geben Sie Ihre Anmeldeinformationen ein.
4. Wählen Sie "Extras", "Schemadesigner" aus.

Das Fenster "Schemadesigner" wird geöffnet. Im Fenster "Schemadesigner" wird auf der linken Seite die CA SDM-Datenbank im Baumstrukturformat angezeigt. Die Tabellen und Spalten werden nach Objektnamen angezeigt. Wenn der Anzeigename vom Objektnamen einer Tabelle oder Spalte abweicht, wird der Anzeigename in Klammern mit dem Objektnamen angezeigt.

Hinzufügen einer Tabelle

Verwenden Sie den Schemadesigner, um der Datenbank eine Tabelle hinzuzufügen.

Gehen Sie wie folgt vor:

1. Wählen Sie "Bearbeiten", "Tabelle hinzufügen" aus.

Das Dialogfeld "Neue Tabelle hinzufügen" wird geöffnet.

2. Geben Sie den Tabellennamen in das Feld "Neuer Tabellename" ein, und klicken Sie auf "OK". Stellen Sie sicher, dass der Name der standortdefinierten Tabelle mit dem Buchstaben "z" beginnt, um Konflikte mit möglichen zukünftigen Standardtabellen zu verhindern.

Wenn Sie kein "z" hinzufügen, dann WSP fügt ein "z" an den Anfang des Tabellennamens hinzu.

3. Füllen Sie folgende Felder nach Wunsch aus:

Name

(Schreibgeschützt) Gibt den Objektnamen der Tabelle an. Der Objektnamen der cr-Tabelle lautet z. B. "cr".

Anzeigename

Gibt den anwenderfreundlichen Namen für die Tabelle an. Der Anzeigename der cr-Tabelle lautet z. B. "Request". Sie können den Anzeigename einer Tabelle ändern, indem Sie einen neuen Namen in dieses Feld eingeben.

Schemaname:

(Schreibgeschützt für standardmäßige Tabellen) Gibt den Namen, der verwendet wird, um auf die Tabelle in CA SDM-Hilfsprogrammen zu verweisen, wie z. B. "pdm_userload". Bei standortdefinierten Tabellen entspricht der Schemaname standardmäßig dem Objektnamen. Sie können den Schemanamen durch Eingabe eines neuen Werts in diesem Feld ändern.

DBMS-Name:

Gibt den Namen der Tabelle im physischen DBMS an. Dieses Feld ist bei allen Standardtabellen schreibgeschützt. Für standortdefinierte Tabellen entspricht dieser Name immer dem Schemanamen.

Standardanzeigefeld (allgemeiner Name)

Gibt die Spalte an, die in der Anwenderschnittstelle für ein Feld angezeigt wird, das auf diese Tabelle verweist. Zum Beispiel bildet das Feld "Bevollmächtigter" eines Request einen Verweis zur Tabelle "Contact". Da der allgemeine Name der Tabelle "Contact" "combo_name" (Nachname, Vorname zweiter Vorname) lautet, wird der kombinierte Name des entsprechenden Kontakts als Zuständiger angezeigt. Der Wert des allgemeinen Namens kann nicht geändert werden.

Fremdes Schlüsselfeld (rel. Attr.)

Gibt die Spalte an, die in der Datenbank für ein Feld gespeichert ist, das auf diese Tabelle verweist. Zum Beispiel bildet das Feld "Bevollmächtigter" eines Request einen Verweis zur Tabelle "Contact". Da das relative Attribut der Tabelle "Kontakt" ID lautet, enthält die Spalte "Zuständiger" in einer Request die ID des referenzierten Kontakts. Der Wert von "rel attr." kann nicht geändert werden.

Funktionsgruppe

Gibt den Namen der Gruppe ein, die die Zugriffsebene steuert, über die Anwender für den Zugriff auf Datensätze in dieser Tabelle verfügen. Der Zugriffstyp jedes Kontakts gibt an, ob der Kontakt über Lesezugriff, Bearbeitungsrechte oder keinen Zugriff auf die Daten in Tabellen in jeder Funktionsgruppe verfügt. Sie können den Wert von „rel attr“ ändern, indem Sie einen anderen Wert in der Dropdownliste wählen.

Wichtig! Der Schemadesigner enthält die Registerkarte "Erweitert". Die Informationen zu diesen Registerkarten sind für Support-Mitarbeiter von CA Technologies und technische Fachkräfte gedacht. Bei der Verwendung des Schemadesigners werden diese Registerkarten in der Regel nicht benötigt und werden deshalb in diesem Handbuch nicht weiter erläutert.

4. Führen Sie eine der folgenden Aktionen aus, um die Tabelle zu speichern:
 - Wenn Sie im Testsystem arbeiten, wählen Sie "Datei", "Speichern" aus.
 - Wenn Sie im Produktionssystem arbeiten, wählen Sie "Datei", "Speichern" aus, und legen Sie den Testmodus fest.

Daraufhin werden Ihre Änderungen in der Datenbank gespeichert und eine Datei (wsptest.mods) auf dem Server erstellt, in der die Änderungen für die Objekt-Engine definiert werden. Diese Datei wird im Unterverzeichnis "site/mods/majic" des CA SDM-Installationsverzeichnis gespeichert. Nachdem die Datei "wsptest.mods" erstellt wurde, aktualisiert WSP die Objekt-Engine, sodass sie die neuen Änderungen verwendet. In Abhängigkeit von der Komplexität Ihres Schemas kann dies von ein paar Sekunden bis zu ein paar Minuten dauern.

Eine Meldung wird angezeigt. Klicken Sie zum Fortsetzen auf "Ja". Die Datei "wsptest.mods" wirkt sich nur auf die Objekt-Engine aus, die von der Option "wsp_domsrvr" angegeben ist. Andere Objekt-Engines auf demselben Server verarbeiten die Datei nicht, und die Datei wird nicht über andere Server verteilt. Darüber hinaus werden im Testmodus neue Tabellen und Spalten für die Objekt-Engine als lokale Objekte definiert. Dies bedeutet, dass die Objekt-Engine über sie informiert ist, und Sie sie in Webformularen verwenden können. Sie existieren jedoch nicht in der Datenbank und wirken sich nicht auf andere Anwender aus. Normale CA SDM-Anwender verwenden die Objekt-Engine von WSP nicht und sind deshalb nicht von den Schemaänderungen betroffen, die Sie testen.

Die Tabelle wird hinzugefügt.

Hinzufügen einer Spalte

Verwenden Sie den Schemadesigner, um der Datenbank eine Spalte hinzuzufügen.

Gehen Sie wie folgt vor:

1. Wählen Sie die Tabelle aus, für die Sie eine Spalte hinzufügen möchten (oder wählen Sie eine der vorhandenen Spalten aus).
2. Wählen Sie "Bearbeiten", "Spalte hinzufügen" aus.
Das Dialogfeld "Neue Spalte hinzufügen" wird geöffnet.
3. Geben Sie den Spaltennamen in das Feld "Neuer Spaltenname" ein, und klicken Sie auf "OK". Stellen Sie sicher, dass die Namen der standortdefinierten Tabelle mit dem Buchstaben "z" beginnen, um Konflikte mit möglichen zukünftigen Standardspalten zu verhindern.

WSP stellt sicher, dass Sie das Präfix hinzugefügt haben, aber fügt im Bedarfsfall ein "z" am Anfang des Spaltennamens hinzu.

4. Füllen Sie die folgenden Felder nach Wunsch aus:

Name

(Nur Anzeige) Gibt den Objektnamen der Spalte an. Der Objektname der Spalte "alt_phone" in der Tabelle "Kontakt" lautet "alt_phone".

Anzeigename

Gibt den anwenderfreundlichen Namen für die Spalte an. Sie können den Anzeigenamen einer Spalte ändern, indem Sie einen anderen Namen in dieses Feld eingeben. Der Anzeigename der Spalte "alt_phone" in der Tabelle "Kontakt" lautet "Alternative Telefonnummer".

Schemaname:

(Schreibgeschützt für standardmäßige Tabellen) Gibt den Namen, der verwendet wird, um auf die Spalten in CA SDM-Hilfsprogrammen zu verweisen, wie z. B. "pdm_userload". Bei standortdefinierten Tabellen entspricht der Schemaname standardmäßig dem Objektnamen. Sie können den Schemanamen durch Eingabe eines anderen Werts in diesem Feld ändern.

DBMS-Name:

(Schreibgeschützt für alle Tabellen) Gibt den Namen an, der verwendet wird, um auf die Tabelle im physischen DBMS zu verweisen. Für standortdefinierte Tabellen entspricht der DBMS-Name immer dem Schemanamen.

Beschreibung

Gibt eine kurze Beschreibung der Spalte an.

Feldtyp

(Schreibgeschützt für alle standardmäßigen Spalten in standardmäßigen Tabellen und gespeicherte standortdefinierte Spalten) Gibt den Datentyp der Spalte an. Sie können den Feldtyp von standortdefinierten Spalten angeben oder ändern, indem Sie einen Wert aus der Dropdown-Liste wählen. Folgende Liste beschreibt die verfügbaren Feldtypen:

INTEGER

Gibt einen numerischen Wert an.

STRING

Gibt eine Textzeichenfolge an. Das Feld "Zeichenfolgenlänge" gibt die Anzahl der Zeichen in einer Zeichenfolge an.

DATUM

Gibt ein Datum und eine Uhrzeit an. Der in der Datenbank gespeicherte Ganzzahlwert entspricht der Anzahl an Sekunden seit Mitternacht, dem 1. Januar 1970.

DAUER

Gibt eine Zeitspanne an. Der in der Datenbank gespeicherte Wert ist eine Ganzzahl, die einer Anzahl an Sekunden entspricht.

DOUBLE

Gibt eine reale Zahl (Gleitkomma) an.

SREL

Gibt eine Fremdschlüsselreferenz auf eine andere Tabelle an. Das Feld "SREL-Tabelle" gibt die referenzierte Tabelle an. Der in der Datenbank gespeicherte Wert entspricht dem zugehörigen Attribut der entsprechenden Tabelle. Hierbei kann es sich entweder um eine Ganzzahl oder eine Zeichenfolge handeln. Der im Produkt angezeigte Wert ist der allgemeine Name der entsprechenden Tabellenzeile. Informationen zum Festlegen von SREL-Attributen mit Fremdschlüsselwerten finden Sie im *Technischen Referenzhandbuch*.

BREL

Gibt eine virtuelle Spalte an, in der alle Objekte mit SREL auf diese Tabelle dargestellt sind. Es existiert nur in der Objekt-Engine und ist nicht physikalisch in der Datenbank gespeichert. Dieser Feldtyp sollte nur auf Anweisung eines Mitarbeiters von CA Technologies ausgewählt werden.

QREL

Gibt eine virtuelle Spalte an, in der eine Reihe von Objekten dargestellt ist, die von der Where-Klausel in der Registerkarte „Erweitert“ ausgewählt wird. Es existiert nur in der Objekt-Engine und ist nicht physikalisch in der Datenbank gespeichert. Dieser Feldtyp sollte nur auf Anweisung eines Mitarbeiters von CA Technologies ausgewählt werden.

DERIVED

Gibt eine virtuelle Spalte an, die von der Objekt-Engine mit den Werten von anderen Spalten erstellt wurde. Hierfür wurde die in der Registerkarte „Erweitert“ angegebene Formel verwendet. Es existiert nur in der Objekt-Engine und ist nicht physikalisch in der Datenbank gespeichert. Dieser Feldtyp sollte nur auf Anweisung eines Mitarbeiters von CA Technologies ausgewählt werden.

Zeichenfolgenlänge

Die Länge einer Zeichenfolge-Spalte. Dieses Feld ist für Nicht-String-Spalten leer. Es ist bei allen Standardspalten und bei gespeicherten standortdefinierten Spalten schreibgeschützt. Sie können die Länge von neuen standortdefinierten STRING-Spalten angeben oder ändern, indem Sie eine Ganzzahl zwischen 1 und 32767 in dieses Feld eingeben.

SRel-Tabelle

Die Tabelle, auf die eine SREL-Spalte verweist. Dieses Feld ist für Nicht-SREL-Spalten leer. Es ist bei allen Standardspalten und bei gespeicherten standortdefinierten Spalten schreibgeschützt. Sie können die Tabelle angeben, auf die von einer neuen standortdefinierten SREL verwiesen wird, indem Sie sie aus der Dropdownliste wählen.

Bei neuem Standardwert

Der Standardwert, der dieser Spalte zugeordnet ist, wenn eine neue Zeile der Tabelle definiert wird. Es muss sich um einen für den Feldtyp geeigneten Wert handeln. Einige Schlüsselwortwerte stehen für besondere Feldtypen zur Verfügung:

JETZT

Gibt das aktuelle Datum und die aktuelle Uhrzeit für die Spalte DATE an.

ANWENDER

Gibt den aktiven Anwender für eine SREL zur Tabelle "Contact" an.

Beim Speichern festgelegter Wert

Der Wert, der dieser Spalte zugeordnet ist, wenn eine Zeile der Tabelle aktualisiert wird. Es muss sich um einen für den Feldtyp geeigneten Wert handeln. Einige Schlüsselwortwerte stehen für besondere Feldtypen zur Verfügung:

JETZT

Gibt das aktuelle Datum und die aktuelle Uhrzeit für die Spalte DATE an.

ANWENDER

Gibt den aktiven Anwender für eine SREL zur Tabelle "Contact" an.

Erforderlich

Durch Aktivieren dieses Kontrollkästchen wird angegeben, dass ein Wert für die Spalte angegeben werden muss, bevor eine Zeile der Tabelle mit dieser Spalte gespeichert werden kann. Sie können diese Option für Standardspalten und standortdefinierte Spalten festlegen. Überdies können Sie festgelegte Optionen auch wieder deaktivieren. Sie können jedoch die Option einer Standardspalte nicht deaktivieren, sofern sie nicht durch Ihren Standort festgelegt wurde.

Nur bei neuem Eintrag aktualisierbar

Durch Aktivieren dieses Kontrollkästchens wird angegeben, dass ein Wert für diese Spalte nur angegeben werden kann, wenn eine Tabellenzeile neu erstellt wurde. Danach sind keine Änderungen mehr möglich. Sie können diese Option für Standardspalten und standortdefinierte Spalten festlegen. Überdies können Sie festgelegte Optionen auch wieder deaktivieren. Sie können jedoch die Option einer Standardspalte nicht deaktivieren, sofern sie nicht durch Ihren Standort festgelegt wurde.

Schlüssel für pdm_userload

Durch Aktivieren dieses Kontrollkästchens wird angegeben, dass diese Spalte zu den Spalten gehört, die mit pdm_userload getestet wurden, um zu überprüfen, ob die Eingabe eine Aktualisierung einer verfügbaren Zeile ist. Diese Option ist nur für STRING-Spalten verfügbar. Sie ist für alle Spalten in Standardtabellen schreibgeschützt.

DBMS-Indexoptionen

Diese Optionen geben Merkmale einer Spalte an, die ein Index der physischen DBMS ist. Sie sind nur für Spalten in standortdefinierten Tabellen verfügbar.

Einzel

Gibt an, dass die Spalte in der Tabelle einmalig ist, und dass keine zwei Zeilen über denselben Wert für die Spalte verfügen.

Aufsteigend

Gibt an, dass der DBMS-Index in dieser Spalte in aufsteigender Reihenfolge aufgeführt ist. Diese Option bewirkt das Gegenteil von "Absteigend".

descending

Gibt an, dass der DBMS-Index in dieser Spalte in absteigender Reihenfolge aufgeführt ist. Diese Option bewirkt das Gegenteil von "Aufsteigend".

Wichtig! Der Schemadesigner enthält die Registerkarte "Erweitert". Die Informationen zu diesen Registerkarten sind für Support-Mitarbeiter von CA Technologies und technische Fachkräfte gedacht. Bei der Verwendung des Schemadesigners werden diese Registerkarten in der Regel nicht benötigt und werden deshalb in diesem Handbuch nicht weiter erläutert.

5. Führen Sie eine der folgenden Aktionen aus, um die Spalte zu speichern:
 - Wenn Sie im Testsystem arbeiten, wählen Sie "Datei", "Speichern" aus.
 - Wenn Sie im Produktionssystem arbeiten, wählen Sie "Datei", "Speichern" aus, und legen Sie den Testmodus fest.

Daraufhin werden Ihre Änderungen in der Datenbank gespeichert und eine Datei (wsptest.mods) auf dem Server erstellt, in der die Änderungen für die Objekt-Engine definiert werden. Diese Datei wird im Unterverzeichnis "site/mods/majic" des CA SDM-Installationsverzeichnis gespeichert. Nachdem die Datei "wsptest.mods" erstellt wurde, aktualisiert WSP die Objekt-Engine, sodass sie die neuen Änderungen verwendet. In Abhängigkeit von der Komplexität Ihres Schemas kann dies von ein paar Sekunden bis zu ein paar Minuten dauern.

Eine Meldung wird angezeigt. Klicken Sie zum Fortsetzen auf "Ja". Die Datei "wsptest.mods" wirkt sich nur auf die Objekt-Engine aus, die von der Option "wsp_domsrvr" angegeben ist. Andere Objekt-Engines auf demselben Server verarbeiten die Datei nicht, und die Datei wird nicht über andere Server verteilt. Darüber hinaus werden im Testmodus neue Tabellen und Spalten für die Objekt-Engine als lokale Objekte definiert. Dies bedeutet, dass die Objekt-Engine über sie informiert ist, und Sie sie in Webformularen verwenden können. Sie existieren jedoch nicht in der Datenbank und wirken sich nicht auf andere Anwender aus. Normale CA SDM-Anwender verwenden die Objekt-Engine von WSP nicht und sind deshalb nicht von den Schemaänderungen betroffen, die Sie testen.

Die Spalte wird zur Bereichstabelle hinzugefügt.

Ändern von Tabellen oder Spalten

Sie können Informationen über eine Tabelle oder Spalte im Schemadesigner ändern. Klicken Sie dazu auf die Tabelle oder Spalte, und geben Sie die neuen Informationen in die entsprechenden Felder ein. Welche Informationen Sie ändern können, hängt vom Status der Tabelle oder Spalte ab:

Standardtabellen

Ermöglicht es Ihnen, die Felder "Anzeigename", "Beschreibung" und "Funktionsgruppe" zu ändern.

Standardspalten

Ermöglicht es Ihnen, die Felder "Anzeigename" und "Beschreibung" sowie "Bei neuem Standardwert" und "Bei Speichern festgelegter Wert" zu ändern. Darüber hinaus können Sie die Kontrollkästchen „Erforderlich“ und „Nur bei neuem Eintrag aktualisierbar“ aktivieren, wenn diese nicht aktiviert sind. Wenn diese Optionen standardmäßig definiert sind, können Sie sie nicht deaktivieren. Sie können jedoch Ihre eigenen Änderungen umkehren.

Standortdefinierte Tabelle

Wenn die Tabelle nicht veröffentlicht wurde, können Sie alle Felder mit Ausnahme des Feldes "Name" bearbeiten. Dieses kann nach dem Speichern der Tabelle nicht mehr geändert werden. Nachdem eine standortdefinierte Tabelle veröffentlicht wurde, können Sie nur die Felder "Anzeigename", "Beschreibung" und "Funktionsgruppe" ändern.

Standortdefinierte Spalte

Wenn die Spalte nicht veröffentlicht wurde, können Sie alle Felder mit Ausnahme des Feldes "Name" bearbeiten. Dieses kann nach dem Speichern der neuen Spalte nicht mehr geändert werden. Nachdem eine standortdefinierte Spalte veröffentlicht wurde, können Sie nur die Felder "Anzeigename" und "Beschreibung" sowie "Bei neuem Standardwert" und "Bei Speichern festgelegter Wert" ändern. Außerdem können Sie die Kontrollkästchen "Erforderlich", "Nur bei neuem Eintrag aktualisierbar" und "Schlüssel für pdm_userload" aktivieren sowie die DBMS-Indexoptionen verwenden.

Veröffentlichen von Schemaänderungen

Sobald Sie mit den Schemaänderungen zufrieden sind, können Sie sie für alle Anwender verfügbar machen, indem Sie sie veröffentlichen. WSP speichert Ihre neuen oder aktualisierten Tabellen und Spalten in den Tabellen "wsptbl" und "wspcol" der jeweiligen Datenbank.

Gehen Sie wie folgt vor:

1. Erstellen oder aktualisieren Sie Dateien, die das geänderte Schema für die Objekt-Engine und die Dienstprogramme von CA SDM beschreiben. WSP erstellt in der Web-Engine die folgenden Dateien, die von der Option "wsp_webengine" bestimmt werden (standardmäßig web:local):

wsp.mods

Beschreibt alle von Web Screen Painter verwalteten Schemaänderungen an der Objekt-Engine.

wsp_schema.sch

Beschreibt alle von Web Screen Painter verwalteten Tabellen und Spalten.

wsp_index.sch

Beschreibt DBMS-Indizes für die von Web Screen Painter verwalteten Tabellen.

wsp.altercol

Benennt neue Spalten, die in WSP erstellt, aber noch nicht für die DBMS definiert wurden.

wsp.altertbl

Benennt neue Tabellen, die in WSP erstellt, aber noch nicht für die DBMS definiert wurden. Darüber hinaus verteilt WSP die Datei "wsp.mods" an alle CA SDM-Server mit einer Objekt-Engine.

2. Wählen Sie "Datei", "Speichern" und "Veröffentlichen" aus.

Die erforderlichen Dateien werden auf CA SDM-Servern erstellt, aber nicht zurückgeführt. Folglich haben die neuen Dateien keine unmittelbare Auswirkung. Die erstellten Dateien werden jedoch nach dem nächsten Neustart der CA SDM-Services verwendet.

3. Wenn Sie die *konventionelle Konfiguration* verwenden, führen Sie folgende Schritte aus:

- Fahren Sie die CA SDM-Dienste auf dem Primärserver herunter, und führen Sie folgenden Befehl aus:

```
pdm_publish
```

Dieser Befehl ändert das physische DBMS, sodass sie Informationen über das neue Schema enthält.

Wichtig! Die Ausführung von "pdm_publish" hat umfassende Auswirkungen auf andere Anwender. Stellen Sie sicher, dass Sie bei der Veröffentlichung von Schemaänderungen äußerst sorgfältig vorgehen. Wir empfehlen, dass Sie CA SDM-Änderungsaufträge verwenden, um die Genehmigung für geplante Schemaveröffentlichungen zu erhalten.

4. Wenn Sie die *Konfiguration für erweiterte Verfügbarkeit* verwenden, führen Sie folgende Schritte aus:

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

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

-h

Zeigt die Hilfeseite an.

-q seconds

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

-c

Diese Option bricht einen zuvor gesendeten Request zur Stilllegung ab.

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

- b. Fahren Sie die CA SDM-Dienste auf dem Hintergrundserver herunter.

Wichtig! Starten Sie die CA SDM-Dienste auf Standby-Servern oder Anwendungsservern nicht neu, nachdem Sie "Speichern und veröffentlichen" über WSP ausgeführt haben. Diese Aktion beschädigt die Konfiguration für erweiterte Verfügbarkeit. Wenn die CA SDM-Dienste auf Standby-Servern oder Anwendungsservern angehalten werden und Sie die Dienste starten möchten, führen Sie den Befehl "pdm_server_control -v" auf den Servern aus, um die Versionskontrolle zu unterdrücken, bevor Sie die CA SDM-Dienste starten.

Wichtig! Wenn der Hintergrundserver während der Veröffentlichung fehlschlägt, stellen Sie sicher, dass Sie die WSP-Änderungen wiederherstellen. Weitere Informationen finden Sie im Abschnitt "[Wiederherstellen von WSP-Änderungen beim Fehlschlagen der Hintergrundserver](#)" (siehe Seite 404).

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

```
pdm_server_control -b
```

-b

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

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

- d. Führen Sie folgenden Befehl auf dem ursprünglichen Hintergrundserver (jetzt der Standby-Server) aus, um das DBMS mit den Schemaänderungen zu aktualisieren:

```
pdm_publish
```

Der Befehl "pdm_publish" erstellt eine Kontrolldatei, die zum nächsten CA SDM-Start führt, um das Synchronisieren des Standby-Servers mit dem Hintergrundserver zu unterdrücken. Diese Aktion ist notwendig, um die von "pdm_publish" durchgeführten Änderungen der Schemadatei beizubehalten. Dieser Befehl führt optional den zweiten Failover durch, nachdem die Schemaänderungen erfolgreich veröffentlicht wurden. Folgende Meldung wird dem Anwender am Ende der erfolgreichen Veröffentlichung angezeigt:

Möchten Sie, dass "pdm_publish" CA Service Desk Manager auf diesem Standby-Server startet und ein Failover durchführt (J/N)?

- Wenn Sie "J" eingeben, startet "pdm_publish" die CA SDM-Dienste auf dem Standby-Server und führt automatisch ein Failover durch. Fahren Sie mit Schritt "g" fort, um die Schemaänderungen auf allen Anwendungsservern anzuwenden.
 - Wenn Sie "N" eingeben, fahren Sie mit Schritt "e" fort.
- e. Starten Sie CA SDM-Dienste auf dem Standby-Server (ursprünglich der Hintergrundserver).

Beim Start wird die Kontrolldatei entdeckt, die von "pdm_publish" erstellt wurde. Jedoch wird der Standby-Server nicht mit dem Hintergrundserver synchronisiert. Da keine Synchronisierung durchgeführt wird, werden die von "pdm_publish" vorgenommenen Änderungen für diesen Start beibehalten.

Wichtig! Stellen Sie sicher, dass Sie diese Anweisungen genau befolgen, da ein Failover-Fehler zum ursprünglichen Hintergrundserver nach "pdm_publish" zu fehlerhaften Diensten führt.

- f. Führen Sie folgenden Befehl auf dem Standby-Server (ursprünglich der Hintergrundserver) aus, um den Server wieder als Hintergrundserver festzulegen:

```
pdm_server_control -b
```

Dieser Befehl löscht auch die Kontrolldatei, sodass die Versionskontrolle normal funktioniert, wenn dieser Server wieder als Standby-Server festgelegt wird.

- g. Führen Sie folgenden Befehl auf den Anwendungsservern aus:

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

-q interval -s server_name

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

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

- h. Starten Sie alle Standby-Server neu.

Wiederherstellen von WSP-Änderungen während des Ausfalls eines Hintergrundservers

Sie können die MDB-Schemaänderungen wiederherstellen, wenn der Hintergrundserver während der Veröffentlichung fehlschlägt.

Wichtig! Wir empfehlen Ihnen, die Wiederherstellungsschritte nicht direkt in der Produktionsumgebung auszuführen. Stellen Sie sicher, dass Sie sie zuerst in einer Test- oder Entwicklungsumgebung validieren.

Gehen Sie wie folgt vor:

- Wenn der Hintergrundserver vor der Veröffentlichung abgestürzt ist, werden die letzten gespeicherten Schemaänderungen in der MDB beibehalten. Sie melden sich beim neuen Hintergrundserver an und setzen Ihre Veröffentlichungen fort.

- Wenn der Hintergrundserver nach der Veröffentlichung abstürzt, führen Sie folgende Aktionen aus:
 - a. Halten Sie CA SDM-Dienste auf dem abgestürzten Hintergrundserver an.
 - b. Wählen Sie einen Standby-Server aus, den Sie als neuen Hintergrundserver hochstufen möchten.
 - c. Kopieren Sie folgende Dateien vom abgestürzten Hintergrundserver in den gleichen Speicherort auf dem Standby-Server:
 - "\$NX_ROOT\$/site/mods/majic/wsp.mods"
 - "\$NX_ROOT\$/site/mods/wsp.altertbl"
 - "\$NX_ROOT\$/site/mods/wsp.altercol"
 - "\$NX_ROOT\$/site/mods/wsp_index.sch"
 - "\$NX_ROOT\$/site/mods/wsp_schema.sch"
 - d. Führen Sie folgenden Befehl auf dem Standby-Server aus, um die Schemaänderungen zu veröffentlichen und um das automatische Failover auszuführen:


```
pdm_publish
```
 - e. Wählen Sie "J" in der Meldung aus, die nach der erfolgreichen Veröffentlichung von Schemaänderungen angezeigt wird.
Die CA SDM-Dienste werden auf dem Standby-Server gestartet.
Hinweis: Wenn das automatische Failover nicht ausgeführt wird, führen Sie den Befehl "pdm_server_control -b" auf dem Standby-Server aus, um den Server als neuen Hintergrundserver hochzustufen.
 - f. Legen Sie alle Anwendungsserver still, und führen Sie sie zurück. Starten Sie alle Standby-Server neu. Weitere Informationen finden Sie im Abschnitt ["Veröffentlichen von Schemaänderungen"](#) (siehe Seite 431)".

Umkehren von Schemaänderungen

Wenn Sie Ihre Meinung über Schemaänderungen geändert haben, nachdem Sie sie in den Textmodus gesetzt haben, können Sie die Änderungen bis zur veröffentlichten Version des Schemas rückgängig machen. Das Umkehren von Schemaänderungen hat möglicherweise Auswirkungen auf andere Anwender. Daher ist diese Option nur verfügbar, wenn sowohl die Option "wsp_domsrvr" als auch "wsp_webengine" installiert ist, um WSP eine Objekt-Engine und eine Web-Engine zuzuordnen.

Gehen Sie wie folgt vor:

1. Wählen Sie "Datei", "Aus Testmodus zurücksetzen" aus.
WSP löscht die Datei "wspstest.mods", woraufhin die WSP-Objekt-Engine das Schema auf die veröffentlichte Version zurücksetzt.

Nachdem die Datei "wsptest.mods" gelöscht ist, wird die Objekt-Engine von WSP neu gestartet, damit das interne Schema neu erstellt werden kann. In Abhängigkeit von der Komplexität Ihres Schemas kann dies von ein paar Sekunden bis zu ein paar Minuten dauern.

Nachdem die Aktualisierung der Objekt-Engine abgeschlossen ist, entspricht das aktive Schema wieder der veröffentlichten Version.

Hinweis: Webformulare, die geändert wurden, damit sie mit dem neuen Schema funktionieren, werden nicht automatisch zurückgesetzt. Deshalb funktionieren sie bei Verwendung des veröffentlichten Schemas möglicherweise nicht korrekt.

Ändern von standortdefinierten Spalten nach der Veröffentlichung

Nachdem standortdefinierte Schemaänderungen veröffentlicht wurden, behandelt WSP sie ähnlich wie ein Standardschema und schränkt weitere Änderungen ein. Sie können eine standortdefinierte Spalte löschen oder die Länge einer standortdefinierten Zeichenfolgenspalte ändern, indem Sie das DBMS und das Schema extern zu WSP manuell aktualisieren. Dann führen Sie das Skript "pdm_wspupd" aus, um die Datenbanktabelle "wspcol" zu aktualisieren, um WSP mit den externen Änderungen zu synchronisieren.

Gehen Sie wie folgt vor:

1. Melden Sie sich abhängig von Ihrer CA SDM-Konfiguration bei folgendem Server an:
 - Konventionell: Primärserver
 - Erweiterte Verfügbarkeit: Hintergrundserver
2. Suchen Sie den das Unterverzeichnis "site/mods" in Ihrem CA SDM-Installationsverzeichnis.
3. Bearbeiten Sie die Datei "wsp_schema.sch", um unerwünschte standortdefinierte Spalten zu löschen oder um die Länge der standortdefinierten ZEICHENFOLGE-Spalten zu ändern. Diese Aktualisierungen sind die einzigen Änderungen, die von diesem Verfahren unterstützt werden. Sie können einen standardmäßigen Texteditor verwenden, um die Datei "wsp_schema.sch" zu bearbeiten.

Wichtig! Wenn eine der Indexoptionen (z. B. UNIQUE) angegeben wurden, um eine Spalte zu löschen, dann bearbeiten Sie die Datei "wsp_index.sch", und entfernen Sie Verweise auf die Spalte. Wenn es sich bei der Spalte um die einzige indizierte Spalte in der Tabelle handelt, müssen Sie alle Verweise auf die Tabelle aus der Datei wsp_index.sch entfernen.

4. Bearbeiten Sie Datei "majic/wsp.mods" mit den gleichen Änderungen, die in "wsp_schema.sch" vorgenommen wurden:

- Löschen Sie unerwünschte standortdefinierte Spalten.
- Ändern Sie die Länge der standortdefinierten ZEICHENFOLGE-Spalten.

5. Geben Sie in der Eingabeaufforderung folgenden Befehl ein:

```
pdm_wspupd
```

Das Skript pdm_wspupd liest die Datei wsp_schema.sch, vergleicht sie mit der Tabelle wscol in der Datenbank und schreibt für jeden Unterschied eine Zeile an die Konsole. Als Beispiel dient folgende Ausgabe:

```
PDM_WSPUPD - Update wscol table from wsp_schema.sch
```

```
Reading wsp_schema.sch to for current DBMS information...
```

```
Reading wscol table for WSP schema information...
```

```
String column zSalesOrg.description length changed from 350 to 400
```

```
Column zSalesOrg.sym not found in wsp_schema.sch - deleting wscol row
```

```
pdm_wspupd found 1 WSP-maintained column(s) to update and 1 to delete. Please  
verify that your DBMS has been manually updated to correspond to wsp_schema.sch,  
then reply Y to update wscol or anything else to cancel.
```

6. Überprüfen Sie, ob die von pdm_wspupd gefundenen Änderungen genau den Änderungen entsprechen, die Sie in "wsp_schema.sch" durchgeführt haben. Ist dies der Fall, geben Sie **Y** ein, um die Änderungen zu bestätigen.

Nachdem Sie die Aktualisierung bestätigt haben, verwendet das Skript die Standard-CA SDM-Programme, um die Tabelle „wscol“ zu aktualisieren. Dann zeigt der Schemadesigner Ihre Änderungen an.

7. Halten Sie die CA SDM-Server an.
8. Modifizieren Sie mithilfe des entsprechenden Dienstprogramms für Ihre DBMS die DBMS-Definition der geänderten Spalten:
 - Löschen Sie Spalten aus der Datenbank, die Sie aus "wsp_schema.sch" gelöscht haben.
 - Ändern Sie die Datenbanklänge von beliebigen Zeichenfolgenspalten, die Sie in "wsp_schema.sch" geändert haben.

Achten Sie sorgfältig darauf, dass die in der DBMS vorgenommenen Änderungen exakt den Änderungen in "wsp_schema.sch" entsprechen.

9. Löschen Sie die Datei "wsp_schema.log".
10. [Veröffentlichen von Schemaänderungen](#) (siehe Seite 400).
11. Starten der CA SDM-Server.

So passen Sie eine Web-Schnittstelle von Web Screen Painter an

Web Screen Painter (WSP) ermöglicht es Ihnen, Webformulare an den Anforderungen Ihres Standorts ohne Programmierung anzupassen.

Einige der Knowledge Management-Formulare lassen sich allerdings in der Designansicht von WSP nicht anpassen. Für diese Formulare sind alternative Herangehensweisen zur Anpassung verfügbar:

- Dokumentansicht: Die zum Erstellen des Dokuments verwendete Dokumentvorlage bestimmt die Inhalte dieser Seite. Diese Vorlagen können auf der Registerkarte "Administration" unter "Dokumente" und "Dokumentvorlagen" geändert werden.
- Knowledge-Kategorien – Liste: Diese Seite können Sie mit Web Screen Painter ändern, doch auch die Anwendereinstellungen wirken sich auf die Seite aus. Das Fenster "Voreinstellungen" ermöglicht die Personalisierung pro Anwender. Hier können Sie definieren, welche Dokumenteigenschaften in der Dokumentliste angezeigt werden sollen und wie viele Dokumente pro Seite angezeigt werden sollen.

Gehen Sie wie folgt vor:

1. [Starten Sie Web Screen Painter](#) (siehe Seite 409).
2. [Überprüfen Sie die Voraussetzungen](#) (siehe Seite 409).
3. [Wählen Sie das Formular aus, das angepasst werden soll](#) (siehe Seite 409):
 - [Erstellen Sie ein Formular](#) (siehe Seite 410).
 - [Öffnen Sie ein vorhandenes Formular](#) (siehe Seite 412).
4. [Formulare anpassen](#) (siehe Seite 413)

WSP speichert immer Änderungen auf dem Server, auf dem WSP installiert ist. Wenn Sie eine Datei speichern, können andere WSP-Anwender in einer Vorschauansicht darauf zugreifen. Für normale CA SDM-Anwender ist sie jedoch unsichtbar. Dies liegt daran, dass WSP alle Dateien im Verzeichnis "site/mods/wsp" speichert und dieses Verzeichnis nicht in einer normalen CA SDM-Sitzung verwendet werden kann.
5. Wenn Sie Änderungen am Webformular im Testsystem vornehmen, [führen Sie eine Migration von einem Testsystem auf ein Produktionssystem durch](#) (siehe Seite 430).
6. [Veröffentlichen von Formularänderungen](#) (siehe Seite 431).
7. (Im Bedarfsfall) [Löschen Sie Formulare nach der Veröffentlichung](#) (siehe Seite 433).

Überprüfen der Voraussetzungen

Überprüfen Sie folgende Voraussetzungen, bevor Sie die Anpassung durchführen:

- Das Schema, das Sie in den Webformularen hinzufügen möchten, ist angepasst.
- (Nur bei der Konfiguration für erweiterte Verfügbarkeit) Folgende Voraussetzungen wurden überprüft, um die Webformulare erfolgreich zu veröffentlichen:
 - (Empfohlen) CA SDM-Dienste sind hochgefahren und werden auf allen CA SDM-Servern ausgeführt. Anderenfalls veröffentlicht WSP nur auf den CA SDM-Servern, die hochgefahren sind und ausgeführt werden.
 - (Erforderlich) Mindestens eine Web-Engine-Instanz, die auf jedem CA SDM-Server ausgeführt wird.

Starten von Web Screen Painter

Starten Sie WSP, um Webformulare anzupassen.

Gehen Sie wie folgt vor:

1. Melden Sie sich beim Computer an, auf dem Web Screen Painter installiert ist.
2. Starten Sie WSP.
 - (Windows) Klicken Sie auf "Start", "Programme", "CA", "Service Desk", "Web Screen Painter".
 - (UNIX) Geben Sie den Befehl `pdm_wsp` mit `"$NX_ROOT/bin"` in Ihren Pfad ein.

Wichtig! Unter UNIX muss Firefox installiert sein, um WSP nutzen zu können.

Das Web Screen Painter-Anmeldefenster wird geöffnet.

3. Geben Sie Ihre Anmeldedaten ein.

WSP zeigt das Hauptformular an.

Auswählen des Formulars, das angepasst werden soll

Sie können ein Formular erstellen, oder Sie können ein vorhandenes Formular öffnen, das angepasst werden soll. Wählen Sie eine der folgenden Möglichkeiten aus:

- [Erstellen Sie ein Formular](#) (siehe Seite 410).
- [Öffnen Sie ein vorhandenes Formular](#) (siehe Seite 412).

Erstellen von Formularen

Erstellen von Formularen in WSP.

Gehen Sie wie folgt vor:

1. Klicken Sie auf "Datei" und anschließend auf "Neu".
Das Dialogfeld "Neues Formular" wird geöffnet.
2. Füllen Sie die folgenden Felder nach Wunsch aus:

Schnittstellen- oder Dateityp

Zeigt den Dateityp des Formulars an. Zum Beispiel: Um ein HTML-Formular zu erstellen, wählen eine Schnittstelle aus (Analyst, Kunde, Mitarbeiter, Standard oder PDA). So erstellen Sie ein Formular eines anderen Dateityps, indem Sie einen Typ direkt auswählen (CSS-Stylesheet, HTML oder JavaScript). Wenn Sie eine Schnittstelle oder einen Dateityp auswählen, zeigt WSP eine Liste aller verfügbaren Vorlagen für den ausgewählten Dateityp im Feld "Dateiname" an.

Formulargruppe

Zeigt die Formulargruppe (wie für Ihre CA SDM-Installation angegeben) an, wo Sie Ihr neues Formular oder Ihre neue Datei erstellen möchten. Wenn Sie keine Formulargruppen definiert haben, wird nur die STANDARD-Formulargruppe aufgeführt.

Dateiname

Zeigt die Vorlage für die ausgewählte Schnittstelle oder den ausgewählten Dateityp an. Eine Vorlage enthält die grundlegenden Anforderungen an ein neues Formular bzw. eine neue Datei des gewünschten Typs.

Tabelle für neue Liste oder Detailformular auswählen

Zeigt die CA SDM-Tabellen an, für die Sie eine neue Liste oder ein Detailformular erstellen können. Dieses Feld wird entsprechend Ihrer Auswahl der Schnittstelle (Analyst, Kunde, Mitarbeiter, Standard oder PDA) aufgefüllt.

Hinweis: Pro Tabelle in einer Formulargruppe darf nur ein Detail- oder Listenformular vorhanden sein. Deshalb sollten Sie für Tabellen, die bereits über ein Formular verfügen, das vorhandene Formular bearbeiten (statt ein neues zu erstellen). Wenn Sie mehrere Versionen eines Formulars wünschen, erstellen Sie eine oder mehrere Formulargruppen mit diesen zusätzlichen Versionen.

3. Klicken Sie auf "Neu".
4. Das Formular wird für Ihre Anpassungen angezeigt. Die folgenden zwei Registerkarten werden angezeigt:

Konzeption

Verfügbar für Detailformulare, Listenformulare und Menüleistenformulare, und die Steuerelemente in dem Formular werden ungefähr so angezeigt, wie der Anwender sie sehen würde. Dies entspricht jedoch nicht dem Bild, das ein Endanwender des Formulars sehen würde. Dazu wählen Sie "Tools", "Vorschau" aus.

Source

Ein Programm, ähnlich wie der Editor, in dem Sie den Quellcode von Formularen überprüfen und bearbeiten können. Einige Formulare können nur in der Registerkarte „Quelle“ bearbeitet werden. Diese Formulare werden im Bearbeitungsfenster in der Registerkarte „Quelle“ geöffnet, und die Registerkarte „Design“ ist deaktiviert.

Das Formular ist für die Anpassung vorbereitet.

Wichtig! Beim Erstellen oder Bearbeiten von Detail- bzw. Listenformularen sollten Sie die Präfixe "list_" und "detail_prefixes" im Namen der HTML-Datei verwenden. Verwenden Sie zum Beispiel "list_test.html" und "detail_test.html". Mit diesem Präfix können Sie die Vorschau eines Formulars anzeigen. Wenn Sie eine Detailvorlage unter einem anwenderspezifischen Namen speichern, müssen Sie auch das Tag <PDM_WSP> manuell bearbeiten. Beispiel: <PDM_WSP mode=edit preview="test.html+OP=CREATE_NEW" factory=cr>.

Weitere Informationen:

[Erstellen von Webformulargruppen](#) (siehe Seite 438)

Vorhandene Formular öffnen

Öffnen Sie ein vorhandenes Formular in WSP, um es anzupassen.

Gehen Sie wie folgt vor:

1. Wählen Sie "File", "Open".

Das Dialogfeld "Formular öffnen" wird geöffnet.

2. Wählen Sie den Schnittstellen- (Analytiker, Kunde, Mitarbeiter, Standard) oder Dateityp (CSS-Stylesheet, JavaScript oder HTML) und die Formulargruppe aus, die das Formular enthält, das Sie bearbeiten möchten.
3. Wählen Sie entweder das gewünschte Formular aus der Liste aus, oder geben Sie den Namen in das Textfeld ein.

Wenn Sie einen Namen ins Textfeld eingeben, führt WSP automatisch einen Bildlauf durch, und der erste Name in der Liste wird angezeigt, der mit den eingegebenen Zeichen übereinstimmt. Sie können die Drop-down-Liste "Statusdateien" verwenden, um die angezeigte Dateiliste zu beschränken:

Standort mit unveröffentlichten Änderungen geändert (+)

Schränkt die Liste der Dateien ein, die mit WSP geändert, aber noch nicht veröffentlicht wurden. Diese Dateien sind durch ein Pluszeichen (+) nach dem Dateinamen gekennzeichnet.

Standort geändert (*)

Schränkt die Liste der an Ihrem Standort geänderten Formularen ein, die sowohl veröffentlicht als auch unveröffentlicht sind. Diese nicht veröffentlichten Dateien sind durch ein Pluszeichen (+) nach dem Dateinamen gekennzeichnet. Veröffentlichte Standortänderungen werden mit einem Sternchen (*) nach dem Dateinamen identifiziert.

Alle

Zeigt die Liste ohne Einschränkungen an. Diese nicht veröffentlichten Dateien sind durch ein Pluszeichen (+) nach dem Dateinamen gekennzeichnet. Veröffentlichte Standortänderungen werden mit einem Sternchen (*) nach dem Dateinamen identifiziert.

4. Klicken Sie auf "Öffnen".

Das Formular wird angezeigt und ist für Ihre Anpassung bereit.

Formulare anpassen

Nachdem Sie ein Formular geöffnet haben, das Sie in WSP bearbeiten möchten, können Sie die Symbolleiste, Menübefehle und Verknüpfungen verwenden, um das Formular anzupassen. Sie können folgende Anpassungen durchführen:

- [Einfügen von Steuerelementen](#) (siehe Seite 413)
- [Bearbeiten der Steuerungseigenschaften](#) (siehe Seite 416)
- [Ändern der Menüleisten](#) (siehe Seite 417)
- [Ändern der Stylesheets](#) (siehe Seite 421)
- [Ändern eines QuickInfo-Vorschauformulars](#) (siehe Seite 425)
- [Ändern einer Datenrasterliste auf einem Listenformular](#) (siehe Seite 427)
- [Ändern von Notizbüchern auf einem Detailformular](#) (siehe Seite 429)
- [Ändern von HTML- und JavaScript-Dateien](#) (siehe Seite 430)

Einfügen von Steuerelementen

Hinzufügen einer Steuerung auf dem Formular. Zum Beispiel: Hinzufügen eines Textfelds im Formular.

Folgende Steuerelemente können sowohl in Listen- als auch in Detailformulare eingefügt werden:

Steuerelement	Symbol	Beschreibung
Zeile einfügen		Führt dazu, dass das ausgewählte Steuerelement das letzte in der aktuellen Zeile ist (und die folgenden Steuerelemente in die nächste Zeile verschoben werden).
Zeile löschen	N. rel.	Löscht alle Steuerelemente aus der Zeile, in der sich das derzeit ausgewählte Steuerelement befindet.
Textfeld		Fügt ein Textfeld mit einer oder mehreren Zeilen zur Bearbeitung von Zeichenfolgen oder Text ein.
Dropdownfeld		Fügt eine Dropdownliste zum Bearbeiten eines Feldes ein, das anhand einer Tabelle validiert wird.
Suchfeld		Fügt ein Suchfeld-Steuerelement zur Bearbeitung eines Feldes ein, das mit einer Tabelle validiert wird. Das Steuerelement besteht aus einem Textfeld mit einem Hyperlink in der Beschriftung, über den ein Auswahlformular geöffnet werden kann.

Steuerelement	Symbol	Beschreibung
Schaltfläche		Fügt eine Schaltfläche ein.
Hierarchisches Suchfeld		Entspricht dem Suchfeld-Steuerelement mit der Ausnahme, dass es für ein Feld mit einem hierarchischen Wählschalter (z. B. Request-Kategorie) verwendet wird.
Datum		Fügt ein Datumsfeld ein. Das Steuerelement besteht aus einem Textfeld mit einem Hyperlink in der Beschriftung, über den ein Datumswählschalter geöffnet werden kann.

Die folgenden zusätzlichen Steuerelemente sind nur für Detailformulare verfügbar:

Steuerelement	Symbol	Beschreibung
Kontrollkästchen		Fügt ein Kontrollkästchen ein.
HTML-Editor		Fügt einen HTML-Editor für ein Textfeld ein, das HTML enthält.
Schreibgeschütztes Textfeld		Fügt ein Textfeld ein, das nicht-bearbeitet werden kann.
Schreibgeschütztes Suchfeld		Fügt ein Suchfeld ein, das nicht-bearbeitet werden kann. Das Feld wird als Hyperlink angezeigt, über den das definierende Detailformular aufgerufen werden kann.
Lesezugriff		Fügt ein Datumsfeld ein, das nicht-bearbeitet werden kann.
Notizbuch		Fügt einen Notizblock ein. In einem Detailformular kann nur ein Notizblock verfügbar sein, so dass dieses Steuerelement nur in Formulare eingefügt werden kann, die noch keinen Notizblock enthalten.

Die folgenden zusätzlichen Steuerelemente sind nur für Listenformulare verfügbar:

Steuerelement	Symbol	Beschreibung
Liste		Fügt eine Liste ein. In einem Listenformular kann nur eine Liste enthalten sein, so dass dieses Steuerelement nur in neue Listenformulare eingefügt werden kann.

Gehen Sie wie folgt vor:

1. Klicken Sie mit der rechten Maustaste auf die Position im Formular, an der Sie das Steuerelement einfügen möchten, und wählen Sie "Steuerung einfügen" aus.
Eine Drop-down-Liste wird angezeigt.
2. Aktivieren Sie die [Optionen des Dialogfelds "Steuerung einfügen"](#) (siehe Seite 415).
Das Steuerelement wird auf dem Formular platziert.
3. Wählen Sie "Tools", "Vorschau" aus, um zu überprüfen, wie das Formular dem Endanwender angezeigt wird. Obwohl dieses Fenster einem standardmäßigen CA SDM-Fenster ähnelt und die meisten Schaltflächen und Menüs funktionsfähig sind, handelt es sich hierbei um keine Standardsitzung, so dass Sie auch nicht versuchen sollten, es auf diese Weise zu verwenden.
4. Klicken Sie auf "Datei", "Speichern".
Die Steuerelemente sind auf einem Formular hinzugefügt.

Optionen des Dialogfelds "Steuerung einfügen"

Öffnen Sie im Menü "Datei" das Dialogfeld "Steuerung einfügen". Im Dialogfeld sind alle Benutzeroberflächensteuerungen aufgelistet, die für den Abschnitt des Formulars, den Sie zur Bearbeitung ausgewählt haben, relevant sind.

Das Dialogfeld enthält die folgenden Optionen:

Einfügen vor

Fügt die ausgewählte Steuerung aus der Liste vor der gegenwärtig ausgewählten Steuerung in das Basisformular ein und aktiviert sie als neu ausgewählte Steuerung

Einfügen nach

Fügt die ausgewählte Steuerung aus der Liste nach der gegenwärtig ausgewählten Steuerung in das Basisformular ein und aktiviert sie als neu ausgewählte Steuerung.

Zurück

Verschiebt die gegenwärtig ausgewählte Steuerung zu der Steuerung, die ihr im Formular vorangeht.

Next

Verschiebt die gegenwärtig ausgewählte Steuerung zu der Steuerung, die im Formular auf sie folgt.

Eigenschaften

Zeigt das Dialogfeld "Eigenschaften" für die gegenwärtig ausgewählte Steuerung an.

Schließen

Schließt das Formular "Steuerung einfügen".

Formular nach dem Einfügen schließen

(Aktiviert) Wenn Sie auf "Einfügen vor" oder "Einfügen nach" klicken, wird die ausgewählte Steuerung eingefügt, und das Dialogfeld "Steuerung einfügen" wird geschlossen.

(Deaktiviert) Wenn Sie auf "Einfügen vor" oder "Einfügen nach" klicken, wird die ausgewählte Steuerung eingefügt. Das Dialogfeld "Steuerung einfügen" bleibt geöffnet, damit Sie zusätzliche Steuerungen oder Anfrageeigenschaften für die gegenwärtig ausgewählte Steuerung einfügen können. Wenn Sie das Kontrollkästchen "Formular nach dem Einfügen schließen" deaktivieren, bleibt es deaktiviert, bis Sie es erneut aktivieren oder Ihre WSP-Sitzung beenden.

Standard: Aktiviert

Bearbeiten der Steuerungseigenschaften

Bearbeiten der Eigenschaften eines Steuerelements.

Gehen Sie wie folgt vor:

1. Wählen Sie das Steuerelement aus, und drücken Sie F4.
Das Dialogfeld "Eigenschaften" wird geöffnet.
2. Ändern Sie die Eigenschaften nach Bedarf. Zum Beispiel: Die Eigenschaft "Bezeichnung" gibt die Headerbeschriftung an, die oberhalb eines Steuerelements angezeigt wird. Geben Sie für diese Eigenschaft den gewünschten Wert in der Zelle rechts neben der Eigenschaft "Bezeichnung" ein.
3. Schließen Sie das Dialogfeld "Eigenschaften".
4. Wählen Sie "Tools", "Vorschau" aus, um zu überprüfen, wie das Formular dem Endanwender angezeigt wird. Obwohl dieses Fenster einem standardmäßigen CA SDM-Fenster ähnelt und die meisten Schaltflächen und Menüs funktionsfähig sind, handelt es sich hierbei um keine Standardsitzung, so dass Sie auch nicht versuchen sollten, es auf diese Weise zu verwenden.
5. Klicken Sie auf "Datei", "Speichern".
Die Eigenschaften des Steuerelements sind geändert, und das Formular wird gespeichert.

Ändern der Menüleisten

Formulare, deren Name mit "*menubar_*" beginnt, definieren eine Menüleiste. Die Ansicht "Design" für eine Menüleiste zeigt oben das Menü an. Sie können auf ein Menüelement klicken, um das Menü nach unten zu verschieben. Weitere Möglichkeiten der Bearbeitung von Menüleisten bestehen in der Ansicht "Design" jedoch nicht. Um eine Menüleiste zu bearbeiten, doppelklicken Sie auf den Menüpunkt und zeigen den Menü-Designer an.

Hinweis: Menüs (und Menüleistenformulare) werden nur in der Analystenschnittstelle verwendet. Die Kunden- und Mitarbeiterschnittstellen verwenden eine "Startleiste", die Verknüpfungen und keine Dropdownmenüs enthält. Um die Startleiste in der Kunden- bzw. Mitarbeiterschnittstelle anzupassen, bearbeiten Sie das Formular `std_body_site.html` für die entsprechende Schnittstelle.

Gehen Sie wie folgt vor:

1. Wählen Sie "Tools", "Menü-Designer" aus, oder doppelklicken Sie auf das Menü, das auf der Registerkarte "Design" eines Menüleistenformulars angezeigt wird.
Das Dialogfeld "Menü-Designer" wird angezeigt.
2. Füllen Sie die Felder im Dialogfeld "[Menü-Designer](#) (siehe Seite 418)" aus, um Menüpunkte hinzuzufügen oder zu bearbeiten. Weitere Informationen über das Hinzufügen von Menüpunkten finden Sie im Abschnitt "[In Menüelementen nützliche Funktionen](#) (siehe Seite 420)".
3. Klicken Sie auf "OK", um das Dialogfeld zu schließen.
4. Wählen Sie "Tools", "Vorschau" aus, um zu überprüfen, wie das Formular dem Endanwender angezeigt wird. Obwohl dieses Fenster einem standardmäßigen CA SDM-Fenster ähnelt und die meisten Schaltflächen und Menüs funktionsfähig sind, handelt es sich hierbei um keine Standardsitzung, so dass Sie auch nicht versuchen sollten, es auf diese Weise zu verwenden.
5. Klicken Sie auf "Datei", "Speichern".
Die Menüleiste im Formular ist geändert.

Dialogfeld "Menüdesigner"

Hinweis: Sie können nur auf den Menüdesigner zugreifen, wenn Sie HTML-Formulare bearbeiten, deren Name mit "menubar_" (z. B. menubar_admin.html) beginnt.

Das Dialogfeld "Menüdesigner" wird angezeigt, wenn Sie im Menü „Tools“ die Option "Menüdesigner" auswählen oder auf der Registerkarte "Design" eines Menüleistenformulars auf ein Menü doppelklicken. Über das Dialogfeld "Menüdesigner" können Sie eine Menüleiste, Untermenüs und Menübefehle zum geöffneten Formular hinzufügen. Das Dialogfeld "Menüeditor" enthält die folgenden Steuerelemente:

Menüleiste

Wählen Sie in der Menüleiste das Menüelement aus, das Sie ändern möchten. Um eine Menübezeichnung zu ändern, wählen Sie die Menübezeichnung aus der Liste aus, geben einen neuen Namen ein und klicken auf "Anwenden".

Hinzufügen

Klicken Sie auf diese Schaltfläche, um ein neues Element am Ende der Menüleiste hinzuzufügen.

Einfügen

Klicken Sie auf diese Schaltfläche, um ein neues Element oberhalb des ausgewählten Elements in der Menüleiste einzufügen.

Löschen

Klicken Sie auf diese Schaltfläche, um das ausgewählte Element aus der Menüleiste zu löschen.



Klicken Sie auf diese Schaltfläche, um das ausgewählte Menüelement um eine Ebene nach oben zu verschieben.



Klicken Sie auf diese Schaltfläche, um das ausgewählte Menüelement um eine Ebene nach unten zu verschieben.



Klicken Sie auf diese Schaltfläche, um das ausgewählte Menüelement um eine Ebene nach rechts zu verschieben, um z. B. ein Element als Untermenü oder Befehl anstelle eines Menüs zu definieren.



Klicken Sie auf diese Schaltfläche, um das ausgewählte Menüelement um eine Ebene nach links zu verschieben, um z. B. ein Element als Menüelement anstelle eines Untermenüs oder Befehls zu definieren.

Hinweis: Es ist nur eine Einzugsebene möglich.

Bezeichnung

Geben Sie für das ausgewählte Menüelement einen Namen ein. Weitere Informationen siehe unter Eigenschaft "Bildunterschrift".

Funktion

Geben Sie die JavaScript-Funktion ein, die ausgeführt werden soll, wenn der Anwender auf das Menü klickt. Siehe die Beschreibung der Eigenschaft "Funktion" für mehr Details, einschließlich einiger vordefinierter Funktionen, die in Menüs nützlich sein können.

ID

Geben Sie die HTML/JavaScript-ID ein, die dem Menüelement zugeordnet werden soll.

Hotkey

Geben Sie eine Liste der Zeichen ein, um die Auswahl des Hotkeys von CA SDM für dieses Menüelement festzulegen. Der Hotkey ist in der Menübezeichnung unterstrichen, wenn diese angezeigt wird. CA SDM wählt normalerweise den ersten Buchstaben der Menübezeichnung, der nicht bereits als Hotkey verwendet wird. Sie können ein oder mehrere Zeichen angeben, um die Auswahl auf diese Zeichen zu beschränken. Sie können jedoch auch ein oder mehrere Zeichen angeben, denen ein Punkt vorangestellt ist, um die Auswahl dieser Zeichen zu verhindern.

Bild

Geben Sie die Position des Bildes ein, das neben dem Menüelement angezeigt werden soll.

Intern

Wählen Sie diese Option aus, um anzugeben, dass das Javascript, das von der Funktion aufgerufen wird, im Kontext des aktuellen Fensters ausgeführt werden soll (wobei es sich um ein Popup-Detailfenster handeln kann). Lassen Sie diese Option deaktiviert, wenn die Funktion im Kontext des Hauptformulars ausgeführt werden soll.

Variable

Geben Sie die JavaScript-Variable ein, die dem Menüelement zugeordnet werden soll.

Symbolleiste

Fügt ein Symbol zur Symbolleiste und eine QuickInfo hinzu, die einem Menüelement entspricht, welche sich nicht auf der obersten Ebene befindet.

Symboldatei

Gibt den Speicherort des Symbolleistensymbols an.

QuickInfo

Gibt den Text für die QuickInfo an.

OK

Klicken Sie, um dieses Dialogfeld zu schließen, und Ihre Änderungen zu speichern.

Abbrechen

Klicken Sie, um das Dialogfeld zu schließen, ohne die Änderungen zu speichern.

In Menüelementen nützliche Funktionen

CA SDM bietet eine Menüleiste in fast jedem Formular, über die die Funktionen ausgeführt werden können. Die Menüleiste wird über ein HTML-Formular erzeugt und zeigt den Namen "menubar_xx.html" an. Es wird empfohlen, dass Sie vorhandene Menüleisten mit WSP anpassen und neue definieren.

Die folgenden vordefinierten Funktionen können nützlich für Skripte sein, die von Menüelementen aufgerufen werden:

upd_frame(form)

Lädt ein neues Formular im Inhalts-Frame des Hauptfensters.

create_new(factory, use_template, width, height [,args])

Ruft ein Formular auf, in dem ein neuer Datensatz definiert werden kann.

Popup_window(name, form[, width, height [,features [,args]]])

Ruft ein neues Fenster auf.

showDetailWithPersid(persid)

Ruft einen Detaildatensatz auf.

Die folgenden Begriffe und Definitionen gelten für die vorherigen Funktionen:

Formular

Dies ist entweder ein HTML-Dateiname im Format xxx.html oder ein Vorgangscode (z. B. CREATE_NEW).

factory

Dies ist der Name eines Datenbankobjekts.

use_template

Dies ist entweder wahr oder falsch.

width

Dies gibt die gewünschte Formularbreite oder Null für den Standardwert an.

height

Dies gibt die gewünschte Formularhöhe oder Null für den Standardwert an.

features

Dies ist eine Liste der Fensterfunktionen in dem Format, das auch mit der Standardfunktion window.open verwendet wird.

args

Dies ist ein oder mehrere Argumente im Format „keyword=value“ für den für dieses Formular angegebenen Vorgang.

persid

Dies ist eine permanente ID im Format „factory:ID“.

Ändern der Stylesheets

Mit WSP können Sie CSS-Dateien (Cascading Stylesheets) bearbeiten oder erstellen.

Hinweis: Um bessere Leistungen zu erzielen, werden einige CA SDM-Stylesheets auf zwei Arten bereitgestellt: Einzelne Dateien (z. B. "search_filter.css") und Kombinationsdateien, die mehrere einzelne Dateien als Gruppe zusammenfassen. Kommentare und überzählige Leerzeichen werden vorher entfernt (z. B. "analyst_styles.css"). WSP bearbeitet immer die einzelnen Dateien; Sie können eine Kombinationsdatei nicht direkt bearbeiten. Wenn Sie Änderungen in Stylesheets veröffentlichen, erstellt WSP bei Bedarf automatisch die damit verbundene Kombinationsdatei.

Gehen Sie wie folgt vor:

1. Erstellen oder öffnen Sie die CCE-Stylesheet-Datei.
WSP zeigt die Ansicht "Quelle" des Stylesheets an.
2. Sie können das Stylesheet entweder direkt in der Ansicht "Quelle" bearbeiten oder den Stildesigner durch Auswahl von "Tools", "Stildesigner" anzeigen.
3. Füllen Sie die Felder im [Dialogfeld "Stildesigner"](#) (siehe Seite 422) nach Bedarf aus. Einige Stilattribute wie "margin" und "border" können im Stildesigner weder angezeigt noch bearbeitet werden. Diese Attribute müssen in der Ansicht "Quelle" bearbeitet werden.
4. Klicken Sie im Stildesigner auf "OK".
WSP formatiert das Stylesheet neu und aktualisiert die Ansicht "Quelle".
5. Klicken Sie auf "Datei", "Speichern".
Das Stylesheet ist angepasst.

Dialogfeld "Stildesigner"

Mit dem Stildesigner können Sie Stylesheets bearbeiten oder anpassen. Das Dialogfeld "Stildesigner", das standardmäßig über die Registerkarte "Schriftart und Farbe" aufgerufen werden kann, enthält die folgenden Steuerelemente:

Stilklassen

Wählen Sie aus der Drop-down-Liste ein Stilelement aus, das Sie ändern möchten.

Hinzufügen

Klicken Sie auf diese Schaltfläche, um eine neue Stilklasse hinzuzufügen.

Umbenennen

Klicken Sie auf diese Schaltfläche, um die Stilklasse umzubenennen, die Sie in der Dropdownliste "Stilklassen" ausgewählt haben.

Löschen

Klicken Sie auf diese Schaltfläche, um die Stilklasse zu löschen, die Sie in der Dropdownliste "Stilklassen" ausgewählt haben.

Installierte Schriftarten

Diese Eigenschaft führt die Schriftarten auf, die in dem System installiert sind. Klicken Sie auf die entsprechenden Schaltflächen  und , um die ausgewählten Schriftarten zwischen der Liste "Installierte Schriftarten" und der Liste "Ausgewählte Schriftarten" zu verschieben.

Ausgewählte Schriftarten

Diese Eigenschaft gibt eine hierarchische Liste bevorzugter Schriftarten an, die ein Browser verwendet, um das Stilklasselement zu zeichnen. Ein Browser verwendet die erste Schriftart in der Liste, die im System installiert ist, auf dem der Browser ausgeführt wird.

Klicken Sie auf die entsprechenden Schaltflächen  und , um die ausgewählten Schriftarten in der Hierarchie nach oben bzw. nach unten zu verschieben.

Schriftgröße

Wählen Sie die Schriftgröße aus der Dropdownliste aus.

Fett

Markieren Sie eine Schriftart in der Dropdownliste.

Kursiv

Markieren Sie eine Schriftart in der Dropdownliste.

Keine Wirkung

Wählen Sie diese Option aus, wenn Sie keine Textverzerrungen oder speziellen Effekte wünschen.

Unterstreichen

Wählen Sie diese Option aus, wenn der Text unterstrichen werden soll.

Durchstreichen

Wählen Sie diese Option aus, wenn der Text durchgestrichen werden soll.

Überstreichen

Wählen Sie diese Option aus, wenn der Text überstrichen werden soll.

Vordergrundfarbe

Wählen Sie die Vordergrundfarbe für das Textelement aus, indem Sie auf die Schaltfläche "Durchsuchen" rechts neben der Eigenschaft "Vordergrundfarbe" klicken. Markieren Sie dann in der Farbpalette die gewünschte Farbe und klicken auf "OK"

Hintergrundfarbe

Wählen Sie die Hintergrundfarbe für das Textelement aus, indem Sie auf die Schaltfläche "Durchsuchen" rechts neben der Eigenschaft "Hintergrundfarbe" klicken. Markieren Sie dann in der Farbpalette die gewünschte Farbe und klicken auf "OK"

Transparent

Wählen Sie diese Option aus, wenn der Hintergrund des Stilelements durchsichtig sein soll.

Ein Beispiel des Stilelements wird im Vorschaubereich am unteren Rand des Dialogfeldes angezeigt.

Um die Position des Stilelements festzulegen, klicken Sie auf die Registerkarte "Position". Die Registerkarte "Position" enthält die folgenden Steuerelemente:

Position

Wählen Sie aus der Dropdownliste für das Element eine Position aus. Die Eigenschaft "Position" platziert Elemente in einer statischen, absoluten oder relativen Position. Durch die Auswahl eines statischen Wertes wird das Element gemäß dem normalen Ablauf platziert. Wenn Sie demgegenüber einen absoluten Wert auswählen, wird das Element irgendwo auf der Seite platziert. Bei Auswahl eines relativen Wertes wird das Element relativ zu seiner normalen Position verschoben.

Links

Geben Sie in dem Textfeld für das Element einen Wert für den linken Rand ein. Markieren Sie in der Dropdownliste eine Größe. Diese Eigenschaft ist deaktiviert, wenn die markierte Position den Wert "Statisch" aufweist.

Top

Geben Sie in diesem Textfeld für das Element einen Wert für den oberen Rand ein. Markieren Sie in der Dropdownliste eine Größe. Diese Eigenschaft ist deaktiviert, wenn die markierte Position den Wert "Statisch" aufweist.

Breite

Geben Sie in diesem Textfeld für das Element einen Wert für die Breite ein. Markieren Sie in der Dropdownliste eine Größe.

Höhe

Geben Sie in diesem Textfeld für das Element einen Wert für die Höhe ein. Markieren Sie in der Dropdownliste eine Größe.

Z-Index

Geben Sie in diesem Textfeld für das Element einen Wert für die Stapelreihenfolge ein. Elemente mit einer hohen Stapelreihenfolge befinden sich immer vor Elementen mit einer niedrigen Stapelreihenfolge. Der Z-Index funktioniert nur für Elemente mit einer absoluten Position.

Hinweis: Elemente können eine negative Stapelreihenfolge aufweisen.

Klicken Sie auf die Registerkarte "Andere", um einige Eigenschaften für das Element festzulegen. Die Registerkarte "Andere" enthält die folgenden Steuerelemente:

Sichtbarkeit

Wählen Sie den Sichtbarkeitstyp aus der Dropdownliste aus. Die Eigenschaft "Sichtbarkeit" legt fest, wie der Inhalt eines Elements angezeigt wird, wenn er seinen Bereich übersteigt.

Überlauf

Wählen Sie aus der Dropdownliste den Überlaufstyp für das Element aus. Die Eigenschaft "Überlauf" legt fest, was passiert, wenn der Inhalt eines Elements den festgelegten Bereich übersteigt.

Anzeige

Wählen Sie aus der Dropdownliste den Anzeigetyp für das Element aus. Die Eigenschaft "Anzeige" legt fest, wie ein Element angezeigt wird.

Cursor

Wählen Sie aus der Dropdownliste den Cursortyp für das Element aus. Die Eigenschaft "Cursor" gibt an, welcher Cursortyp erscheint, wenn auf ein Element gezeigt wird.

OK

Klicken Sie, um dieses Dialogfeld zu schließen, und Ihre Änderungen zu speichern.

Abbrechen

Klicken Sie auf diese Schaltfläche, um das Dialogfeld "Stildesigner" zu schließen.

Ändern eines QuickInfo-Vorschauformulars

Durch die QuickInfo-Vorschau können Sie Schlüsseldetails des aktuellen Formulars anzeigen, ohne auf eine Verknüpfung klicken oder eine neue Webseite öffnen zu müssen. Eine QuickInfo-Vorschau wird angezeigt, wenn Sie den Mauszeiger während einer bestimmten Zeitdauer auf eine Objektverknüpfung in einer Liste oder einem Detailformular legen. Wenn Sie den Mauszeiger von der Verknüpfung entfernen, bevor diese Zeit abgelaufen ist, wird die Vorschau nicht angezeigt. QuickInfo-Vorschauen werden standardmäßig in allen schreibgeschützten Listen und Detailformularen angezeigt.

Sie können QuickInfo-Vorschauen für Formulare erstellen, die standardmäßig kein preview_-Formular haben. Sie können QuickInfo-Vorschauen auch für anwenderdefinierte Formulare erstellen, die Sie in Ihrer CA SDM-Umgebung erstellt haben.

Folgende Formulare mit vordefinierter QuickInfo-Vorschau sind verfügbar:

- preview_chg.html (Change)
- preview_cnt.html (Kontakt)
- preview_cr.html (Anfrage)
- preview_in.html (Incident)
- preview_iss.html (Issue)
- preview_KD.html (Knowledge-Dokument)
- preview_nr.html (Configuration Item)
- preview_pr.html (Problem)

Gehen Sie wie folgt vor:

1. Öffnen Sie eins der folgenden Formulare für die Anpassung:
 - Öffnen Sie ein vorhandenes Formular, das kein standardmäßiges "preview_"-Formular hat. Zum Beispiel "detail_loc.html"
 - Öffnen Sie ein vorhandenes Formular mit QuickInfo-Vorschau. Zum Beispiel "preview_chg.html".
2. Passen Sie das Formular an. Fügen Sie zum Beispiel dem Formular anwenderdefinierte Steuerelemente hinzu, oder entfernen Sie sie aus dem Formular.
3. Klicken Sie auf "Datei" und anschließend auf "Speichern unter", geben Sie einen Dateinamen mit dem Präfix "preview_" an, und klicken Sie auf "Speichern". Geben Sie zum Beispiel preview_loc.html ein.

Das Formular mit QuickInfo-Vorschau wird erstellt und angepasst.

Kapitel 8: Ändern einer Datenrasterliste auf einem Listenformular

Durch Datenrasterlisten können Sie die Inhalte einer Produktseite in einem Listenformular anzeigen, ohne eine neue Seite zu öffnen. Diese datengebundene Steuerung listet Elemente der Datenquelle in einer Tabelle auf, sodass Sie Elemente auswählen und sortieren und Daten abrufen können. Zum Beispiel die Optionen zum Erweitern und Reduzieren auf dem Formular "Incident-Liste".

Gehen Sie wie folgt vor:

1. Öffnen Sie ein Listenformular.
2. Gehen Sie in der Design-Ansicht zum blauen Bereich unten im Formular nach den Feldern mit Beschreibungen. In der Quellcode-Ansicht wird der Datenraster im Code zwischen folgenden Zeilen angezeigt:

```
<PDM_MACRO name=lsStart>  
<PDM_MACRO name=lsEnd>
```

Im folgenden Beispiel wird der Datenrasterbereich in der Design-Ansicht angezeigt:

Frühestens erforde... need_by	Spätestens erforde... need_by	Frühestes Öffnungs... open_date
Frühestes Lösungs... resolve_date	Spätestes Lösungs... resolve_date	Frühestes Schließd... close_date
Frühestes geschätz... est_comp_date	Spätestes geschätz... est_comp_date	Frühestes tatsächlic... actual_comp_date
Geringste geschätzte K... QBE.GE.est_cost	Höchste geschätzte Ko... QBE.LE.est_cost	Niedrigste geschätzte D... QBE.GE.est_total_time
Geringste tatsächliche ... QBE.GE.cost	Höchste tatsächliche Ko... QBE.LE.cost	Niedrigste tatsächliche ... QBE.GE.actual_total_time
If End If Change-Nummer Vorlag chg_ref_num templati		

Das Pluszeichen im Datenrasterbereich markiert den Anfang des erweiterbaren Abschnitts der Zeile (d. h. jene Felder, die nur dann angezeigt werden, wenn der Anwender im Listenformularraster auf das Plussymbol klickt). Der folgende Code generiert das Pluszeichen in der Quellcode-Ansicht:

```
<PDM_MACRO name=lsCol attr=open_date label="Open Date" sort="DESC" startrow=yes>
```

Der Parameter *startrow=yes* gibt an, dass eine Zeile gestartet werden soll, und startet den erweiterbaren Abschnitt der Zeile.

3. Verschieben Sie Spalten innerhalb einer Liste per Drag-and-drop. Sie können Spalten zwischen dem Hauptbereich der Zeile und dem erweiterbaren Abschnitt verschieben. Sie können vorhandene Steuerung nicht aus dem Rasterbereich verschieben.
4. Um eine Listenspalte einzufügen, klicken Sie mit der rechten Maustaste auf eine Steuerung oder einen beliebigen Punkt im blauen Hintergrund, und wählen Sie "Spalte einfügen" oder "Steuerung einfügen".
 - Wenn Sie "Spalte einfügen" auswählen, fügt WSP links neben der gegenwärtig ausgewählten Steuerung eine neue Spalte ein.
 - Wenn Sie "Steuerung einfügen" auswählen, öffnet WSP das Dialogfeld "Steuerung einfügen", über das Sie die gewünschte Steuerung zum Formular hinzufügen können.
5. Wählen Sie "Tools", "Vorschau" aus, um zu überprüfen, wie das Formular dem Endanwender angezeigt wird. Obwohl dieses Fenster einem standardmäßigen CA SDM-Fenster ähnelt und die meisten Schaltflächen und Menüs funktionsfähig sind, handelt es sich hierbei um keine Standardsitzung, so dass Sie auch nicht versuchen sollten, es auf diese Weise zu verwenden.
6. Klicken Sie auf "Datei", "Speichern".

Die Datenrasterliste ist auf dem Listenformular geändert.

Ändern von Notizbüchern auf einem Detailformular

Mit der Steuerung für verschachtelte Registerkarten (Notizbuch) können Sie Schlüsseldetails im aktuellen Formular ein- oder ausblenden. Verwenden Sie diese Steuerung beispielsweise, um festzulegen, wie die Registerkarten im Incident-Detailformular angeordnet werden sollen. Über die Ansicht "Design" können Sie auch mithilfe des Notizbuchsteuerelements verschachtelte Registerkarten zu einem Detailformular hinzufügen, das noch kein Notizbuch enthält. Doppelklicken Sie das Notizbuchsteuerelement, um es zu ändern. Verwenden Sie Drag-and-drop, um Notizbuchregisterkarten hinzuzufügen, einzufügen und zu löschen und um ihre Beschriftungen zu ändern. Sie können auch auf die Pfeilschaltflächen nach oben und nach unten klicken, um die Registerkarten neu anzuordnen und die Position der aktuell ausgewählten Registerkarte zu ändern. Das Kontrollkästchen „Neue Zeile“ gibt an, ob die ausgewählte Registerkarte mit einer neuen Zeile in der Notizbuch-Kopfzeile beginnt.

Gehen Sie wie folgt vor:

1. Öffnen Sie ein Detailformular.
2. Gehen Sie in der Design-Ansicht zu dem blauen Bereich des Formulars, der die erste nummerierte Bezeichnung enthält.

In der Quellcode-Ansicht wird das Notizbuch im Code zwischen folgenden Zeilen angezeigt:

```
<PDM_MACRO name=startNotebook hdr=cng_nb>
<PDM_MACRO name=endNotebook>
```

Hinweis: In CA SDM r12.6 können Notizbücher verschachtelte Registerkarten enthalten. In WSP heißen Registerkarte der ersten Ebene (Registerkarten, die weitere Registerkarten enthalten) "Registerkartengruppen". Registerkartengruppen werden in WSP als dunkelblauer Balken angezeigt, der sich über den gesamten blauen Notizbuchbereich erstreckt und eine zentrierte Nummer enthält. Registerkarten niedrigerer Ebenen (Registerkarten, die keine weiteren Registerkarten enthalten) heißen "Registerkarte". In WSP werden Registerkarten niedrigerer Ebenen als Rechtecke mit abgerundeten Ecken angezeigt.

3. Klicken Sie auf eine Registerkarte, um sie auszuwählen. Wenn Sie eine Registerkarte auswählen, wird am unteren Ende des Notizbuchs eine hervorgehobene Verknüpfung zum Inhalt der Registerkarte angezeigt.

Sie können Registerkarten und Registerkartengruppen innerhalb eines Notizbuchs mithilfe von Drag-and-drop verschieben. Wenn Sie eine Registerkartengruppe verschieben, werden alle in ihr enthaltenen Registerkarten mit verschoben.

4. Um eine Registerkarte oder Registerkartengruppe einzufügen, klicken Sie mit der rechten Maustaste auf eine Steuerung oder auf einen beliebigen Punkt im blauen Hintergrund, und wählen Sie "Registerkarte einfügen", "Registerkartengruppe einfügen" oder "Steuerung einfügen" aus.

Wenn Sie "Registerkarte einfügen" oder "Registerkartengruppe einfügen" auswählen, fügt WSP links neben der gegenwärtig ausgewählten Steuerung eine neue Registerkarte oder Registerkartengruppe ein. Wenn Sie "Steuerung einfügen" auswählen, öffnet WSP das Dialogfeld "Steuerung einfügen", über das Sie die gewünschte Steuerung zum Formular hinzufügen können.

5. Wählen Sie "Tools", "Vorschau" aus, um zu überprüfen, wie das Formular dem Endanwender angezeigt wird. Obwohl dieses Fenster einem standardmäßigen CA SDM-Fenster ähnelt und die meisten Schaltflächen und Menüs funktionsfähig sind, handelt es sich hierbei um keine Standardsitzung, so dass Sie auch nicht versuchen sollten, es auf diese Weise zu verwenden.

Klicken Sie auf "Datei", "Speichern".

Ändern von HTML- und JavaScript-Dateien

Sie können die Ansicht der WSP-Quelle verwenden, um HTML- und JavaScript-Formulare zu bearbeiten. Öffnen Sie eine HTML- oder JavaScript-Datei, und führen Sie die notwendigen Änderungen durch.

Hinweis: Um bessere Leistungen zu erzielen, werden einige CA SDM JavaScript-Dateien auf zwei Arten bereitgestellt: Einzelne Dateien (z. B. `window_manager.js`) und Kombinationsdateien, die mehrere einzelne Dateien als Gruppe zusammenfassen. Kommentare und überzählige Leerzeichen werden vorher entfernt (z. B. `std_head.js`). WSP bearbeitet immer die einzelnen Dateien; Sie können eine Kombinationsdatei nicht direkt bearbeiten. Wenn Sie Änderungen im Skript veröffentlichen, erstellt WSP bei Bedarf automatisch die damit verbundene Kombinationsdatei.

Migrieren aus dem Testsystem auf das Produktionssystem

Ein Ziel beim Design von WSP bestand darin, das Entwickeln und Testen von Formularänderungen in einer Produktionsdatenbank sicherer zu gestalten. Funktionen wie die Web Screen Painter-spezifische Verzeichnisstruktur auf dem Server, dedizierte Web Screen Painter-Serverprozesse und schreibgeschützte Vorschau-sitzungen unterstützen dieses Ziel. Viele Anwender ziehen es jedoch vor, ihre Formularänderungen in einem unabhängigen Testsystem zu entwickeln und sie anschließend wie folgt in ein separates Produktionssystem zu migrieren:

1. Kopieren Sie alle zu migrierenden HTML-Formulare aus dem entsprechenden Unterverzeichnis unter "site/mods/www/html" im Testsystem in dasselbe Unterverzeichnis unter "site/mods/wsp/project" auf dem Produktionssystem.

2. Kopieren Sie alle zu migrierenden CSS-, JavaScript- und HTML-Dateien aus dem entsprechenden Unterverzeichnis unter "site/mods/www/wwwroot" im Testsystem in dasselbe Unterverzeichnis unter "site/mods/www/wwwroot/wsp/project" auf dem Produktionssystem.

Hinweis: Stellen Sie sicher, dass Sie die Dateien und Formulare auf den folgenden Servern des Produktionssystems kopieren (abhängig von Ihrer CA SDM-Konfiguration):

- Konventionell: Primärserver
- Erweiterte Verfügbarkeit: Hintergrundserver

Hinweis: Sie können jede beliebige Methode zum Kopieren von Dateien verwenden, die von Ihrem Betriebssystem unterstützt wird, um den in den Schritten 1 und 2 beschriebenen Kopiervorgang auszuführen. Windows-Anwender sollten in den angezeigten Verzeichnispfaden das Backslash-Zeichen (\) durch einen Schrägstrich (/) ersetzen.

Veröffentlichen von Formularänderungen

Wenn Sie mit Änderungen zufrieden sind, können Sie sie für alle CA SDM-Anwender zur Verfügung stellen, indem Sie sie veröffentlichen. Durch das Veröffentlichen werden alle CA SDM-Server mit neuen oder überprüften Formularen aktualisiert.

Gehen Sie wie folgt vor:

1. Wählen Sie "Datei", "Veröffentlichen" aus.

Wenn Sie Änderungen durchgeführt, aber noch nicht gespeichert haben, fordert WSP Sie auf, diese zu speichern. Anschließend wird ein Bestätigungsfenster angezeigt, in dem alle ausstehenden Web Screen Painter-Änderungen (einschließlich derer, die in vorherigen Sitzungen oder von anderen Web Screen Painter-Anwendern gespeichert wurden) angezeigt werden. Standardmäßig werden alle Änderungen für die Veröffentlichung ausgewählt. Sie können die Auswahl der zu veröffentlichenden Änderungen modifizieren, indem Sie darauf klicken.

2. Wenn Sie mit der Auswahl zufrieden sind, klicken Sie auf "OK".
3. (Nur bei der Konfiguration für erweiterte Verfügbarkeit) Wenn die Web-Engine auf keinem der CA SDM-Server ausgeführt wird, dann wird eine Fehlermeldung mit der Liste der CA SDM-Server angezeigt, auf denen WSP keine Veröffentlichungen durchführen konnte. Führen Sie die folgenden Schritte aus:
 - a. Konfigurieren Sie den CA SDM-Server (der Server, der in der Fehlermeldung angegeben ist), um die Korrekturen vorzunehmen.
 - b. Bearbeiten Sie die Datei in WSP, um ein Leerzeichen im <PDM_IF 0>-Makro hinzuzufügen, und speichern Sie die Datei.
 - c. Gehen Sie zurück zu Schritt 1, um das Webformular erneut zu veröffentlichen.

Hinweis: Wenn Sie keine Konfigurationsänderungen durchführen möchten, müssen Sie den Ordner "nx_root/site/mods/www" manuell vom Hintergrundserver auf alle anderen Server kopieren.

4. (Nur bei der Konfiguration für erweiterte Verfügbarkeit) Wenn der Hintergrundserver während der Veröffentlichung abstürzt, [stellen Sie die HTML-Änderungen wieder her](#) (siehe Seite 432).
5. (Für Formulare mit QuickInfo-Vorschau) Führen Sie folgenden Befehl aus, nachdem Sie die Änderungen veröffentlicht haben:

```
pdm_webcache -H
```

Der Web-Cache wird aktualisiert. WSP stellt die ausgewählten Änderungen für alle Anwender bereit, die auf allen Servern aktiv sind.

Wiederherstellen der HTML-Änderungen

Sie können die HTML-Änderungen wiederherstellen, wenn der Hintergrundserver während der Veröffentlichung fehlschlägt.

Wichtig! Wir empfehlen Ihnen, die Wiederherstellungsschritte nicht direkt in der Produktionsumgebung auszuführen. Stellen Sie sicher, dass Sie sie zuerst in einer Test- oder Entwicklungsumgebung validieren.

Gehen Sie wie folgt vor:

1. Navigieren Sie in das folgende Verzeichnis auf dem abgestürzten Hintergrundserver:
`$NX_ROOT$/site/mods/www/wwwroot/wsp/project/web`
2. Kopieren Sie den gesamten Inhalt des Webordners.
3. Melden Sie sich beim neuen Hintergrundserver an, und fügen Sie den gesamten kopierten Inhalt in den Ordner
`"$NX_ROOT$/site/mods/www/wwwroot/wsp/project/web"` ein.
4. Setzen Sie die Veröffentlichung der Änderungen auf dem neuen Hintergrundserver fort. Weitere Informationen finden Sie im Abschnitt "[Veröffentlichen von Formularänderungen](#)" (siehe Seite 431).

Löschen von Formularen nach der Veröffentlichung

Es können nur am jeweiligen Standort geänderte Formulare gelöscht werden. Requests zum Löschen eines vorher veröffentlichten Formulars werden wirksam, wenn Sie Änderungen veröffentlichen.

Wählen Sie "Datei" > "Löschen des Formulars rückgängig machen", um eine ausstehende Löschanfrage abubrechen. Sie können Änderungen an einem Formular nach dessen Veröffentlichung nicht mehr aufheben. Die einzige Möglichkeit zum Ändern eines veröffentlichten Formulars besteht darin, es erneut zu bearbeiten.

HTML-Vorlagen (HTMPL-Formular)

Formulare werden in der Web-Schnittstelle von CA SDM als HTML-Vorlagen in Dateien mit dem Suffix ".html" bereitgestellt. Diese werden in diesem Dokument als HTMPL-Formulare bezeichnet.

Ein HTMPL-Formular enthält standardmäßige HTML-Tags (einschließlich JavaScript) plus Spracherweiterungen, die von einem CA SDM-Server-Daemon (oder Dienst) interpretiert werden, der standardmäßigen HTML-Code an den Browser liefert. Diese Erweiterungen sind:

- Verweise auf Servervariablen. Diese sind durch einen Namen, der mit einem Dollarzeichen beginnt, gekennzeichnet. Es kann sich dabei um die Werte von Spalten in der CA SDM-Datenbank, Referenzen auf Konfigurationseigenschaften des Webmoduls oder andere Serverinformationen handeln.
- Besondere Tags, welche das Webmodul leiten, um Aufgaben auf dem Server (z. B. das Lesen von Informationen aus der CA SDM-Datenbank) auszuführen. Diese Tags weisen Namen im Format <PDM_...> oder <pdm_...> auf.

Hinweis: Für Anpassungen der CA SDM-Formulare mit WSP müssen Sie weder mit den HTMPL-Erweiterungen noch mit HTML selbst vertraut sein.

Weitere Informationen:

[Servervariablen](#) (siehe Seite 462)

[HTMPL-Tags](#) (siehe Seite 438)

Vorlagenbenennungskonventionen

Mit Hilfe der folgenden Benennungskonventionen werden die vier grundlegenden Arten von HTML-Dateien gekennzeichnet, wobei xxx das Objekt ist:

Vorlagentyp	Name
Liste (Suchfilter und Ergebnisse)	list_xxx.html
Kombiniertes Detailformular, das schreibgeschützt ist und bearbeitet werden kann (Analytikerschnittstelle)	detail_xxx.html
Schreibgeschütztes Detailformular	detail_xxx_ro.html
Zu bearbeitendes Detailformular	detail_xxx_edit.html

Definitionen von Objekten und deren Eigenschaften finden Sie in folgenden Verzeichnissen:

- (UNIX) \$NX_ROOT/bopcfg/majic/*.maj
- (Windows) *installationsverzeichnis*\bopcfg\majic*.maj

Informationen zu den Objekten und Attributen, die CA SDM definieren, finden Sie im *technischen CA SDM-Referenzhandbuch*.

HTML-Verzeichnisse

Im *Administrationshandbuch* werden die im Lieferumfang von CA SDM enthaltenen Web-Schnittstellen beschrieben. Es gibt verschiedene Sätze von HTML-Dateien zum Implementieren dieser Schnittstellen, die in der folgenden Tabelle aufgeführt sind:

Betriebssystem	Verzeichnis, das HTML-Dateien enthält
Windows	<i>installationsverzeichnis</i> \bopcfg\www\html\web\interface
UNIX	\$NX_ROOT/bopcfg/www/html/web/interface

In dieser Tabelle entspricht *interface* dem Namen der Schnittstelle (Analytiker, Kunde oder Mitarbeiter).

Hinweis: Für Dateien der Gastschnittstelle gibt es kein separates Verzeichnis. Gastanwender greifen standardmäßig auf die Dateien der Mitarbeiterschnittstelle zu. Sie können die Benutzerschnittstelle für Gäste ändern, indem Sie den Zugriffstyp ändern, der dem Anwender System_Anonymous zugeordnet ist. Sowohl die Kunden- als auch die Mitarbeiterdateien ändern sich selbst dynamisch in Abhängigkeit davon, ob der aktuelle Anwender ein bekannter Anwender oder ein Gast ist, indem der in diesem Dokument beschriebene Vorlagenbefehl <PDM_IF> verwendet wird.

Unter dem `html`-Verzeichnis sind drei zusätzliche `interface`-Unterverzeichnisse verfügbar:

default:

Enthält HTML-Dateien, von allen Schnittstellen verwendet werden. Wenn Sie nach einer Datei suchen, sieht das Webmodul zunächst in dem Verzeichnis nach, das der Schnittstelle des aktuellen Anwenders entspricht, und anschließend im Standardverzeichnis.

pda/analyst: (UNIX)

pda\analyst: (Windows)

Enthält HTML-Dateien, die von der Schnittstelle für mobile Geräte verwendet werden. In Unicenter Service Desk r11.0 wird die Schnittstelle für mobile Geräte nur für Analysten zur Verfügung gestellt.

web/interface/legacy: (UNIX)

web\interface\legacy: (Windows)

Enthält HTML-Dateien aus Ihrem vorherigen Release von CA SDM, die nicht mehr verwendet werden. Dieses Verzeichnis wird automatisch erstellt, wenn Sie bei der Installation von CA SDM von einem vorherigen Release migrieren. Sie können das Verzeichnis "legacy" löschen, wenn keine der von Ihnen angepassten Dateien auf die Dateien in dem Verzeichnis verweist.

Es wird empfohlen, dass Sie die gelieferten HTML-Dateien nicht direkt modifizieren. Verwenden Sie stattdessen entweder WSP, oder kopieren Sie die Dateien, die Sie ändern möchten, in das Verzeichnis "site mods", und bearbeiten Sie sie hier. Der CA SDM-Webserver sucht im entsprechenden Verzeichnis "site mods" nach einem neuen Formular, bevor er das Verteilungsverzeichnis prüft. Das standardmäßige Verzeichnis "site mods" für jede der Schnittstellen lautet wie folgt:

Betriebssystem	Verzeichnis für standortmodifizierte HTML-Dateien
Windows	<i>Installationsverzeichnis\site\mods\www\html\interface\interface</i>
UNIX	<i>\$NX_ROOT/site/mods/www/html/interface/interface</i>

Hinweis: Wenn Sie das Formular ändern und unter "*installationsverzeichnis\site\mods\www\html\interface*" speichern, können alle Anwender dieses Formular sehen, unabhängig von der Formulargruppe, der sie angehören. Wenn Sie es unter "*Installationsverzeichnis\site\mods\www\html\interface\Schnittstelle*" speichern, können nur die Kontakte die Änderungen anzeigen, die als zugehörig zu der Formulargruppe definiert sind.

In der vorherigen Tabelle entspricht *interface* dem Namen der Schnittstelle (Analytiker, Kunde oder Mitarbeiter). Es gibt kein separates Verzeichnis für Schnittstellendateien für Gäste. Diese Schnittstelle verwendet die Dateien der Mitarbeiterschnittstelle. Der Vorteil für das Speichern von geänderten HTML-Dateien im Verzeichnis "site mods" besteht darin, dass dieses Verzeichnis beibehalten wird, wenn Sie die CA SDM-Wartung oder eine neue Version installieren. Darüber hinaus wird durch das Verwahren der geänderten Dateien im Verzeichnis "site mods" unter Beibehaltung der Originale sichergestellt, dass Sie immer über eine korrekte Kopie der ursprünglich verteilten HTML-Datei verfügen.

Jede Web-Schnittstellenseite weist eine Primärfunktion auf, wie in der folgenden Tabelle angegeben, welche die Haupt-HTML-Vorlagen aufführt. Sie können jedoch <PDM_FORM>-Blöcke zu einer Vorlage hinzufügen, um direkt auf einen von der Web-Schnittstelle unterstützten Vorgang zuzugreifen. Sie können z. B. das Hauptmenü ändern, um Felder zum Einreichen eines Issue einzuschließen, ohne die zwischenliegende Seite zu verwenden, oder Sie können Suchkriterienfelder und eine Schaltfläche "Suchen" zu einem Listenformular hinzufügen:

Webseite	HTML-Vorlage
Hauptformular	menu_frames.html
Change anzeigen/erstellen/aktualisieren	detail_chg.html
Liste von Changes anzeigen	list_chg.html
Issue anzeigen/erstellen/aktualisieren	detail_iss.html
Liste von Issues anzeigen	list_iss.html
Request anzeigen/erstellen/aktualisieren	detail_cr.html
Liste von Requests anzeigen	list_cr.html
Detailinformationen einer Ankündigung anzeigen	detail_cnote.html
Liste von Ankündigungen anzeigen	list_cnote.html
Login	login.html

Hinweis: Eine vollständige Liste der Vorlagen finden Sie in den Verzeichnissen, die in der Tabelle am Anfang dieses Abschnitts aufgeführt sind.

Webformulargruppen

Sie können angepasste Webseiten in einer oder mehreren Formulargruppen zusammenfassen. Die Verzeichnisse von Formulargruppen befinden sich in den folgenden Verzeichnissen:

Windows

Installationsverzeichnis\site\mods\www\html\web\interface

Installationsverzeichnis\site\mods\www\wwwroot\subdirectory

UNIX

\$NX_ROOT/site/mods/www/html/web/interface

\$NX_ROOT/site/mods/www/wwwroot/subdirectory

Jede Formulargruppe bildet ein Unterverzeichnis in diesen Verzeichnissen. Sie geben das angepasste Formularverzeichnis im Feld „Anpassung der Formulargruppe“ für den Zugriffstyp an.

Wenn ein Anwender ein Formular anfordert, sucht das Webmodul zunächst im entsprechenden Verzeichnis für das angepasste Formular, dann im Standardverzeichnis für die Web-Schnittstelle des Anwenders und schließlich im Standardverzeichnis. Sie können für dieselbe Web-Schnittstelle mehrere Zugriffstypen mit jeweils einer anderen angepassten Formulargruppe definieren. Auf diese Weise können Sie spezielle Formulare für verschiedene Arten von Anwendern definieren und dennoch die meisten Formulare von der Standardschnittstelle verwenden.

Ein ähnliches Verfahren wird ausgeführt, wenn eine Webseite eine Datei aus einem der Unterverzeichnisse von wwwroot (css, html, img oder scripts) anfordert. Die Web-Engine prüft eine HTML-Referenz des Formulars "CAisd/img/xxx.gif" und konvertiert es in eine der folgenden GIF-Dateien, wobei die erste Datei ausgewählt wird, in der "xxx.gif" gefunden wird:

- /CAisd/sitemods/img/formgroup/xxx.gif
- /CAisd/sitemods/img/xxx.gif
- /CAisd/img/xxx.gif

Erstellen von Webformulargruppen

So erstellen Sie eine Webformulargruppe:

1. Wenn Sie außer den vordefinierten Formulargruppen "Analyst", "Kunde" oder "Mitarbeiter" weitere Formulargruppen benötigen, erstellen Sie eine neue Formulargruppe. Wählen Sie dazu in WSP im Menü "Datei" die Option "Speichern unter", und klicken Sie im Dialogfeld "Formular speichern unter" auf die Schaltfläche "Formulargruppe hinzufügen". Wenn Sie z. B. zwei separate angepasste Versionen der Schnittstelle „Analytiker“ bereitstellen möchten, können Sie hierfür die Formulargruppen „Analytiker1“ und „Analytiker2“ erstellen. Sie können auch eine neue Formulargruppe definieren, wenn die Schnittstelle, die Sie gerade definieren, logisch nicht in eine der vordefinierten Formulargruppen passt.
2. Wählen Sie auf der Web-Schnittstelle (keine Web Screen Painter-Vorschau) im Menü "Administration" die Option "Sicherheit" und "Zugriffstypen" aus. Klicken Sie dann auf einen Zugriffstyp (oder erstellen Sie einen neuen), und verwenden Sie die Dropdown-Liste "Anpassungsformulargruppe" im Fenster "Zugriffstyp - Detail", um einem Zugriffstyp eine Formulargruppe zuzuweisen. <USDK> bestimmt den Zugriffstyp, wenn sich ein Kontakt anmeldet, und verwendet die Anpassungsformulargruppe, um zu bestimmen, wo in der Verzeichnisstruktur "site mods" nach angepassten Formularen zu suchen ist. Wenn das Webmodul keine Formulare im Formulargruppenverzeichnis findet, sucht es erst im Standardverzeichnis für den Zugriffstyp des Anwenders und dann im Standardverzeichnis.
3. Wählen Sie in WSP im Menü "Datei" die Option "Speichern", oder kopieren Sie die angepassten HTML-Dateien manuell in das folgende Verzeichnis:

Unter Windows:

installationsverzeichnis\site\mods\www\html\web\form_group_name

Unter UNIX: *\$NX_ROOT/site/mods/www/html/web/form_group_name*

Nachdem Sie eine neue Webformulargruppe eingerichtet und alle unterstützenden Dateien in die entsprechenden Unterverzeichnisse kopiert haben, müssen Sie den Webservice erneut starten, damit die Änderungen wirksam werden.

HTML-Tags

Dieser Abschnitt beschreibt PDM-Befehle, um HTML-Tags hinzuzufügen.

Weitere Informationen:

[PDM_EVAL: Einfügen des Werts einer Präprozessorvariablen](#) (siehe Seite 439)

[PDM_FORM: Starten eines HTML-Formulars mit einer Sitzungs-ID](#) (siehe Seite 439)

[PDM_FMT: Formatieren von Text einer Servervariablen](#) (siehe Seite 440)

[PDM_IF: Bedingte Verarbeitung](#) (siehe Seite 443)

[PDM_INCLUDE: Einfügen aus einer anderen Datei](#) (siehe Seite 444)

[PDM_JSCRIPT: Bedingtes Einschließen von JavaScript-Dateien](#) (siehe Seite 445)

[PDM_LINK: Erstellen eines Hyperlinks, der einen HTML-Vorgang aufruft](#) (siehe Seite 446)

[PDM_LIST: Formatieren einer Liste mit Datenbankzeilen](#) (siehe Seite 447)

[PDM_MACRO: Einfügen von Text aus einer Makrodatei](#) (siehe Seite 450)

[PDM_NOTEBOOK: Erstellen eines Notizbuchs](#) (siehe Seite 457)

[PDM_PRAGMA: Angeben von Serverinformationen](#) (siehe Seite 457)

[PDM_SCOREBOARD: Erstellen einer Scoreboard-Struktur](#) (siehe Seite 458)

[PDM_SET: Einstellen des Werts einer Servervariablen](#) (siehe Seite 459)

[PDM_TAB: Erstellen einer Registerkarte in einem Notizbuch](#) (siehe Seite 460)

[PDM_WSP: Steuern der WSP-Vorschau](#) (siehe Seite 460)

PDM_EVAL: Einfügen des Werts einer Präprozessorvariablen

Das `pdm_eval`-Tag wird verwendet, um den Wert einer Vorverarbeitungvariablen in die Eingabe des Webmodul-Parsers einzufügen. Wenn das Tag in einem Makro verwendet wird, wird es erst wirksam, wenn das Makro abgeschlossen ist.

Das `pdm_eval`-Tag ähnelt `pdm_include` oder `pdm_macro` in seiner Funktionsweise. Es fügt den Text exakt an dem Punkt des Tags in die Analyse ein, so als ob der Wert der Variablen anstelle des Tags kodiert wurde..

`pdm_eval` weist die folgende Syntax auf:

```
<PDM_EVAL TEXT=PRE.name>
```

name

(Erforderlich) Der Name der Vorverarbeitungsvariablen, dessen Wert in die Eingabe des Webmoduls einzufügen ist.

PDM_FORM: Starten eines HTML-Formulars mit einer Sitzungs-ID

Die Tags `<PDM_FORM>` und `</PDM_FORM>` können zu jeder beliebigen Web-Schnittstellen-HTML-Vorlage hinzugefügt werden, um ein HTML-Formular mit zwei ausgeblendeten Feldern für die Servervariablen `SID` (Sitzungs-ID) und `FID` (Formular-ID) zu erstellen. Der optional `OP`-Operand erstellt wie mit dem `PDM_LINK`-Tag ein zusätzliches ausgeblendetes Feld für eine der unterstützten Operationen. Mit Ausnahme für die automatisch generierten ausgeblendeten Felder werden die Tags `<PDM_FORM>` und `</PDM_FORM>` auf dieselbe Weise wie die Standard-HTML-Tags `<form>` und `</form>` verwendet (und als Teil von ihrer Erweiterung generiert).

PDM_FMT: Formatieren von Text einer Servervariablen

Die Tags `<PDM_FMT>` und `</PDM_FMT>` werden zum Formatieren von Textblöcken verwendet, die von Servervariablen (`$args.xxx`) wie von den Argumenten gesteuert eingefügt werden.

Hinweis: `<PDM_FMT>` wird für Literale einschließlich der Variablen "`$prop.xxx`" ignoriert.

In der nachstehenden Tabelle werden die folgenden Tags erläutert:

Eigenschaft	Beschreibung
ESC_STYLE= NONE C HTML JS JS2 URL	Gibt den Umwandlungstyp des formatierten Texts an. Gültige Werte sind: KEINE Standardeinstellung. Gibt an, dass für kein Zeichen im Textkörper eine besondere Behandlung erforderlich ist. C Behandeln Sie die in C-Programmen bedeutungsvollen Zeichen ' , " , \ , \r , ` und \n auf besondere Weise. Diese Zeichen werden umgewandelt. HTML Folgende Zeichen sind in HTML-Text von besonderer Bedeutung und erfordern daher eine besondere Behandlung: & wird zu &amp; ' wird zu &apos; " wird zu &quot; < wird zu &lt; > wird zu &gt; JS Folgende Zeichen sind in JavaScript-Text von besonderer Bedeutung und erfordern daher eine besondere Behandlung: ' wird zu %27 " wird zu %22 / wird zu %2F \ wird zu %5C \r wird zu %0D \n wird zu %0A JS2 Entspricht JS, keine besondere Behandlung des Zeichens, /, und besondere Behandlung von zwei zusätzlichen Zeichen: - % wird %25 - Zeilenumbrüche erhalten das Suffix %0A URL Übersetzen Sie alle Zeichen, die keine Buchstaben oder Ziffern sind, sowie '@*-_.#' bis '%xx', wobei xx eine hexadezimale Kodierung des übersetzten Zeichens ist.

Eigenschaft	Beschreibung
JUSTIFY=LEFT CENTER RIGHT TRUNCATE WRAP LIN	Gibt die Ausrichtung des formatierten Textes an. Gültige Werte lauten: TRUNCATE Standardeinstellung. Entfernt die HTML-Formatierung, indem "<" und ">" durch "&lt;" und "&gt;" ersetzt werden. Hinweis: Weitere Informationen finden Sie unter KEEPLINKS und KEEPTAGS. LEFT CENTER RIGHT Stellt genau die durch das Argument WIDTH angegebene Breite an Zeichen her, je nach Bedarf gekürzt oder mit Leerzeichen aufgefüllt, wobei eingebettete neue Zeilen durch ein Leerzeichen ersetzt werden und der Ausgabertext durch die Tags <pre> und </pre> begrenzt wird. Das Argument WIDTH muss als positive Ganzzahl angegeben werden. WRAP Gleiche Eigenschaft wie LEFT, mit Ausnahme dass beim Textumbruch Wörter berücksichtigt werden (d. h. kein Zeilenumbruch innerhalb eines Worts). LINE Entspricht TRUNCATE mit der Ausnahme, dass alle eingebetteten Zeilenumbrüche durch das Tag
 ersetzt werden.
KEEPLINKS=YES NO	Wenn KEEPLINKS=YES angegeben ist, wird die Aktion JUSTIFY=LINE oder JUSTIFY=TRUNCATE geändert, um die HTML-Anchor-Tags (Aktion:) zu bewahren, während alle anderen „<“- und „>“-Zeichen konvertiert werden. Gegenseitig austauschbar mit KEEPTAGS.
KEEPNL=YES NO	Die normale Aktion von PDM_FMT soll alle eingebetteten Zeilenvorschübe und alle folgenden Leerzeichen in ein einzelnes Leerzeichen umwandeln. Wenn KEEPNL=YES angegeben ist, werden eingebettete Zeilenvorschübe beibehalten. Dieses Argument wird für JUSTIFY=LINE ignoriert.
KEEPTAGS=YES NO	Wenn KEEPTAGS=YES angegeben ist, wird die Aktion JUSTIFY=LINE oder JUSTIFY=TRUNCATE modifiziert, sodass alle HTML-Tags zu beibehalten werden. Gegenseitig austauschbar mit KEEPLINKS.
PAD= YES NO	Wenn PAD=NO angegeben ist, wandelt PDM_FMT leere Zeichenfolgen nicht zu einem einzelnen Leerzeichen um. Dies ist die normale Aktion, wenn WIDTH nicht null ist, oder JUSTIFY TRUNCATE oder WRAP ist.
WIDTH=nn	Wenn diese Eigenschaft nicht null ist, gibt sie an, dass der Text genau auf die für WIDTH angegebenen Zeichen formatiert werden soll.

<PDM_FMT> ohne WIDTH oder JUSTIFY führt keine Formatierung an dem eingeschlossenen Text durch, umgibt den Text jedoch mit den Variablen <pre>und </pre>.

Um z. B. eine -mehrzeilige Beschreibung zu erstellen, geben Sie Folgendes ein:

```
<PDM_FMT WIDTH=50 JUSTIFY=WRAP>$args.description</PDM_FMT>
```

Um eine- Ausgabe mit mehreren Spalten zu erstellen, geben Sie Folgendes ein:

```
<PDM_FMT><PDM_FMT WIDTH=20 JUSTIFY=LEFT>$cst.last_name</PDM_FMT>
<PDM_FMT WIDTH=20 JUSTIFY=LEFT>$cst.first_name</PDM_FMT>
<PDM_FMT WIDTH=20 JUSTIFY=TRUNCATE>$cst.middle_name</PDM_FMT>
</PDM_FMT>
```

PDM_IF: Bedingte Verarbeitung

Diese Tags werden für das bedingte Einfügen von Text verwendet. <PDM_IF>-Blöcke können an beliebiger Stelle in HTML-Dateien eingefügt werden – in HTML, in JavaScript und sogar innerhalb von HTML-Tags. <PDM_IF> und <PDM_ELIF> (else if) verwenden beide eher eine einfache konditionelle Klausel als ihre Eigenschaft als Name-Wert-Paare. Wenn die Klausel wahr ist, wird der Text nach dem schließenden Tag in die Datei eingeschlossen. Wenn die Klausel falsch ist, verwirft der Server den Text zwischen dem Tag und dem schließenden Tag. Das schließende Tag kann <PDM_ELIF>, <PDM_ELSE> oder </PDM_IF> sein.

Die Tags <PDM_ELSE> und <PDM_ELIF> sind optional. Wenn beide angegeben sind, müssen die <PDM_ELIF>-Tags dem <PDM_ELSE>-Tag voranstehen. Zwischen den Tags <PDM_IF> und <PDM_ELSE> (oder </PDM_IF>, wenn <PDM_ELSE> ausgelassen wird) kann eine beliebige Anzahl an <PDM_ELIF>-Tags stehen.

Die Syntax der Bedingung in <PDM_IF> und <PDM_ELIF> lautet folgendermaßen:

- 0 is false; any other number is true
- "" is false; "any-string" is true
- "Wert Operand Wert" bewertet den linken und rechten Wert im Vergleich zueinander gemäß dem *Operator*. Wenn beide Werte aus Ziffern bestehen (der optional - oder + vorausgeht), wird der Vergleich auf numerische Weise ausgeführt. Andernfalls wird er lexikalisch (ASCII-Sortierreihenfolge) ausgeführt. Gültige *op*-Werte lauten:

op-Wert	Beschreibung
==	Gleich
!=	Ungleich
>=	Gleich oder größer als (muss als \>= oder >= geschrieben werden)
"<"	Weniger als (muss als \< oder < geschrieben werden)
">"	Größer als (muss als \> oder > geschrieben werden)
<=	Gleich oder kleiner als (muss als \<= oder <= geschrieben werden)

op-Wert	Beschreibung
&	Führt die Funktion Bit-And des linken und rechten Wertes aus. Wahr, wenn Bits festgelegt sind, falsch, wenn keine festgelegt sind.
%	Gibt "true" zurück, wenn der linke Wert ein gerades Vielfaches des rechten Wertes ist. Andernfalls wird "false" zurückgegeben (nützlich für das Erstellen von zwei-dimensionalen Tabellen).
:	Führt einen byteorientierten Suchmustervergleich wie den Grep-Befehl unter UNIX durch. Gibt „true“ zurück, wenn der linke Wert den regulären Ausdruck enthält, der vom rechten Wert definiert wird.

Beispiel:

```
<PDM_IF $count \>= 10> . . .  
<PDM_ELIF $count &lt; 5> . . .  
<PDM_ELSE> . . .  
</PDM_IF>
```

In PDM_IF-Anweisungen können mehrere Bedingungen angegeben sein. Bedingungen werden durch Konnektoren (entweder && (und) oder || (oder)) voneinander getrennt. Beiden Verbindungen muss nichts vorausgehen. Die Web-Engine untersucht Bedingungen von links nach rechts, bis eine Verbindung erreicht wird. Wenn die Ausgangsbedingung wahr und der Verbinder || ist, gilt die gesamte Bedingung ohne weitere Auswertung als wahr. Wenn die Ausgangsbedingung falsch und der Verbinder && ist, gilt die gesamte Bedingung ohne weitere Auswertung als falsch. Andernfalls gilt die Bedingung für das Webmodul als unbestimmt. In diesem Fall wertet das Webmodul die Bedingung ab dem Konnektor aus.

PDM_INCLUDE: Einfügen aus einer anderen Datei

Das <PDM_INCLUDE>-Tag wird verwendet, um Text aus einer zweiten Datei in eine HTML-Datei einzufügen. Der Server ersetzt das <PDM_INCLUDE>-Tag durch den Inhalt der zweiten Datei.

Eingeschlossene Dateien können <PDM_INCLUDE>-Tags enthalten. Es gibt keine Einschränkung für die Tiefe der Verschachtelung.

Das <PDM_INCLUDE>-Tag unterstützt die folgenden Eigenschaften:

Eigenschaft	Beschreibung
FILE=filename	(Erforderlich) Gibt die einzuschließende Datei an. Das Webmodul durchsucht die für HTML-Dateien verwendeten Verzeichnisse, die für den Zugriffstyp des aktuellen Anwenders definiert sind.

Eigenschaft	Beschreibung
FIXUP=[YES NO]	(Optional) Gibt an, ob die Datei von der Web-Schnittstelle als normale HTML-Vorlagendatei interpretiert werden soll, so dass Variablen, die mit einem Dollarzeichen (\$) beginnen, erweitert und andere CA SDM-Tags wie PDM_LIST und PDM_FORMAT interpretiert werden. Der Wert YES gibt an, dass die Datei als reguläre HTML-Vorlagendatei behandelt werden soll, und der Wert NO gibt an, dass die eingeschlossene Datei wie Text behandelt werden soll. Der Standardwert lautet YES. Hinweis: Damit diese Version mit vorherigen Versionen kompatibel ist, kann der Wert JA durch WAHR oder 1 und der Wert NEIN durch FALSCH oder 0 ersetzt werden. Diese Werte sind veraltet und sollten nicht in neuen Seiten verwendet werden.
propname=value	Gibt an, dass die Eigenschaft „propname“ den angegebenen Wert aufweisen sollte. Auf den Wert der Eigenschaft kann innerhalb der eingeschlossenen Datei zugegriffen werden, indem propname das Präfix \$prop vorangestellt wird. Mit der folgenden Spezifikation können z. B. die eingeschlossene Datei auf \$prop.menubar verweisen: <pre><PDM_INCLUDE ... menubar=no></pre> Globale Eigenschaften können auch in der web.cfg-Konfigurationsdatei angegeben werden. Informationen zu "web.cfg" finden Sie im <i>Administrationshandbuch</i>. Hinweis: Damit diese Version mit vorherigen Versionen kompatibel ist, können die in <PDM_INCLUDE> angegebenen Eigenschaftswerte ohne das vorangehende "prop" im Format \$propname referenziert werden. Diese Verwendung wird mißbilligt und sollte nicht auf neuen Seiten verwendet werden.

PDM_JSCRIPT: Bedingtes Einschließen von JavaScript-Dateien

Das <PDM_JSCRIPT>-Tag wird verwendet, um eine JavaScript-Datei bedingt in ein Formular einzuschließen. Dieses Tag weist zwei Formate auf:

```
<PDM_JSCRIPT file=xxxx.js [include=yes|no]>
```

Pdm_jscript mit file=xxx.js gibt an, dass die JavaScript-Datei "xxx.js" in diesem Formular erforderlich ist. Das Webmodul fügt diese Datei zu einer Liste von JavaScript-Dateien hinzu, die für das Formular erforderlich sind. Die Verarbeitung des Tags findet statt, während das Formular geprüft wird. Sie wird von pdm_if nicht beeinflusst. Ein pdm_jscript-Tag, das auf eine Datei verweist, fügt diese Datei zu der Liste von JavaScript-Dateien hinzu, wenn sie irgendwo in der Datei oder in einer eingeschlossenen Datei oder in einem Makro auftritt.

Das optionale Argument *include=no* kann angegeben werden, wenn die Web-Engine das Tag ignorieren soll. Dieses Argument führt zu einer bedingten Verarbeitung des Tags und ist in erster Linie hilfreich, wenn das Tag in einem Makro aufgerufen wird. Das Makro "dtlTextbox" gibt z. B. Folgendes an:

```
<PDM_JSCRIPT file=spellcheck.js include=&{spellchk}>
```

Hiermit wird angegeben, dass für jedes beliebige Formular, das ein dtlTextbox-Makro enthält, das spellchk=yes angibt, die JavaScript Datei "spellcheck.js" erforderlich ist.

Das zweite Format des Tags "pdm_jscript" lautet:

```
<PDM_JSCRIPT insert=here>
```

"Pdm_jscript" mit "insert=here" fordert die Web-Engine auf, Standard-HTML-<script>-Tags für alle erforderlichen JavaScript-Dateien einzufügen. Das Webmodul verarbeitet diese Form von Tag während der Phase der HTML-Generierung, so dass es von pdm_if beeinflusst wird. Ein pdm_jscript-Tag mit insert=here ist Teil der Datei "std_head_include.html", so dass es auf praktisch jedem Formular verfügbar ist.

Hinweis: Die Web-Engine fügt Skripttags nur ein, wenn es das erste Mal auf "pdm_jscript insert=here" stößt.

PDM_LINK: Erstellen eines Hyperlinks, der einen HTML-Vorgang aufruft

<PDM_LINK> und </PDM_LINK> kann zu jeder beliebigen HTML-Vorlage für Web-Schnittstellen hinzugefügt werden, um Verknüpfungen zu erstellen, die einen HTML-Vorgang aufrufen. Das <PDM_LINK>-Tag generiert das Standard-HTML-Tag und weist ähnliche Argumente auf mit der Ausnahme, dass die Spezifikation einer CA SDM-Operation anstelle eines URLs möglich ist.

Das Format lautet folgendermaßen, wobei *operation* einer der unterstützten Operationen entspricht:

```
<PDM_LINK OP=operation> ... </PDM_LINK>
```

Beispiel:

```
<PDM_LINK OP=MENU> Menü </PDM_LINK>  
&lt;PDM_LINK OP=CREATE_NEW_FACTORY=iss&gt; Issue einreichen &lt;/PDM_LINK&gt;  
<PDM_LINK OP=LOGOUT> Abmelden </PDM_LINK>
```

PDM_LIST: Formatieren einer Liste mit Datenbankzeilen

Die Tags `<PDM_LIST>` und `</PDM_LIST>` werden verwendet, um sich wiederholende HTML-Abschnitte für die Ausgabe von mehreren Datensätzen voneinander zu trennen. Alles zwischen den Tags `<PDM_LIST>` und `</PDM_LIST>` wird einmal für jeden auszugebenden Datensatz wiederholt. Es gibt zwei Arten des Tags `PDM_LIST`:

- Listen von einem Objektattribut, das eine Liste impliziert. So entspricht z. B. das Eigenschaftsattribut des Request-Objekts der Liste mit Eigenschaften, die dem Request zugeordnet sind. Dieser Typ des Tags `PDM_LIST` verfügt immer über eine `SOURCE`-Eigenschaft.
- Listen mit einer expliziten `WHERE`-Klausel. Dieser Typ des Tags `PDM_LIST` verfügt immer über eine `WHERE`-Eigenschaft.

Objektattribute vom Typ `<PDM_LIST>` weisen folgende Eigenschaften auf:

Eigenschaft	Beschreibung
ESC_STYLE= NONE C HTML JS JS2 URL	Gibt den Umwandlungstyp des formatierten Texts an. Gültige Werte sind: KEINE Standardeinstellung. Gibt an, dass für kein Zeichen im Textkörper eine besondere Behandlung erforderlich ist. C Behandeln Sie die in C-Programmen bedeutungsvollen Zeichen ' , " , \ , \r , ' und \n auf besondere Weise. Diese Zeichen werden umgewandelt. HTML Folgende Zeichen sind in HTML-Text von besonderer Bedeutung und erfordern daher eine besondere Behandlung: & wird zu &amp; ' wird zu &apos; " wird zu &quot; < wird zu &lt; > wird zu &gt; JS Folgende Zeichen sind in JavaScript-Text von besonderer Bedeutung und erfordern daher eine besondere Behandlung: ' wird zu %27 " wird zu %22 / wird zu %2F \ wird zu %5C \r wird zu %0D \n wird zu %0A JS2 Entspricht JS, keine besondere Behandlung des Zeichens, / , und besondere Behandlung von zwei zusätzlichen Zeichen: - % wird %25 - Zeilenumbrüche erhalten das Suffix %0A. URL Übersetzen Sie alle Zeichen, die keine Buchstaben oder Ziffern sind, sowie '@*_._.#' bis '%xx', wobei xx eine hexadezimale Kodierung des übersetzten Zeichens ist.
LENGTH= <i>nn</i>	Gibt die Anzahl der Zeilen der Ausgabe an (wird standardmäßig auf „alle“ gesetzt).

Eigenschaft	Beschreibung
<code>PREFIX=prefix</code>	Gibt das Präfix zu Referenzen auf Attribute aus Datensätzen in der Liste an. Diese werden in der Form <code>\$prefix.attr_name</code> im Text zwischen <code><PDM_LIST></code> und <code></PDM_LIST></code> referenziert. Die Eigenschaft <code>PREFIX</code> ist in Listen mit Objektvariablen optional. Wenn <code>PREFIX</code> ausgelassen ist, wird der Wert von <code>SOURCE</code> auch für das Präfix verwendet.
<code>SEARCH_TYPE=DISPLAY GET_DOB</code>	Gibt die Methode an, die der Server zum Erstellen des Listenformulars verwenden soll: <code>DISPLAY</code> Gibt an, dass der Server nur eine Abfrage für das gesamte Formular ausgeben soll. <code>GET_DOB</code> Gibt an, dass der Server separate Abfragen für jede Zeile des Formulars ausgeben soll. Die Auswahl beeinflusst die Listenleistung, die ebenfalls von der Komplexität (der Anzahl an Verbindungen, die für die Anzeige erforderlich sind) der Liste und den Merkmalen der DBMS abhängt. <code>GET_DOB</code> hat eine voraussagbarere Leistung als <code>DISPLAY</code> und ist der Standardwert.
<code>SORT=index-name</code>	Gibt den Indexnamen an, der zum Sortieren verwendet wird. Der Standardwert für dieses Argument lautet <code>DEFAULT</code> (d. h., der erste Sortierindex für die zu Grunde liegende Factory).
<code>SOURCE=source</code>	Gibt die Objektvariable an, die diese Liste definiert. Dieses Feld erfordert eine Eingabe. Fügen Sie in der <code>PDM_LIST</code> -Anweisung kein Dollarzeichen (\$) vor <code>source</code> ein. Wenn die Eigenschaft <code>PREFIX</code> nicht angegeben ist, wird <code>source</code> auch als Präfix für Verweise auf Attribute von Datensätzen in der Liste verwendet, in Verweisen mit dem Format <code>\$source.attr_name</code> . Wenn <code>source</code> in einem Verweis verwendet wird, ist ein vorangestelltes Dollarzeichen erforderlich.
<code>START=nn</code>	Gibt die erste Ausgabezeile an (wird standardmäßig auf null gesetzt).

Beispiel:

```

<table border>
<tr>
<th>Child Change Order Number</th>
<th>Summary</th>
</tr>
<PDM_LIST SOURCE=args.children>
<tr>
<td>$args.children.chg_ref_num</td>
<td>$args.children.summary</td>
</tr>
</PDM_LIST>
</table>

```

Da kein Präfix angegeben wurde, wird Referenzen auf Attribute der aufgeführten Datensätze das Präfix `$args.children`, der Quellwert, vorangestellt.

In einer WHERE-Klausel weist PDM_LIST die folgenden Eigenschaften auf:

Eigenschaft	Beschreibung
FACTORY= <i>name</i>	Gibt eine zu suchende Objektklasse an. Diese Eigenschaft ist erforderlich.
LENGTH= <i>nn</i>	Gibt die Anzahl der Zeilen der Ausgabe an (wird standardmäßig auf „alle“ gesetzt).
ORDER_BY= <i>attr-name</i>	Geben Sie den Attributnamen an, nach dem sortiert werden soll. Es kann den Modifizierer DESC (absteigend) oder ASC (aufsteigend) enthalten.
PREFIX= <i>prefix</i>	Gibt das Präfix zu Referenzen auf Attribute aus Datensätzen in der Liste an. Diese werden in der Form <i>\$prefix.attr_name</i> im Text zwischen <PDM_LIST> und </PDM_LIST> referenziert. Die Eigenschaft PREFIX ist in einer WHERE-Klausel-Liste erforderlich.
START= <i>nn</i>	Gibt die erste Ausgabezeile an (wird standardmäßig auf null gesetzt).
WHERE= <i>where-clause</i>	Geben Sie die WHERE-Klausel für die Suche an. Sie kann Attribute (mit Punkten) enthalten. Diese Eigenschaft ist erforderlich.

Beispiel:

```
<table>
<tr>
<th>Child Change Order Number</th>
<th>Summary</th>
</tr>
<PDM_LIST PREFIX=list FACTORY=chg WHERE="status = 'OP'">
<tr>
<td>$list.chg_ref_num</td>
<td>$list.summary</td>
</tr>
</PDM_LIST>
</table>
```

PDM_MACRO: Einfügen von Text aus einer Makrodatei

Das <PDM_MACRO>-Tag wird verwendet, um eine Makrodatei in eine HTML-Datei einzufügen. Die Funktionsweise dieses Tags ähnelt der des Tags PDM_INCLUDE mit zwei wichtigen Unterschieden:

- Eine Datei, die von PDM_MACRO eingeschlossen wird, weist eine formelle Argumentliste mit erforderlichen Argumenten und Argumenten mit Standardwerten auf.
- Eine Datei, die von PDM_MACRO eingeschlossen wird, stammt immer aus dem Verzeichnis, das für die Konfigurationseigenschaft MacroPath angegeben ist, unabhängig vom Zugriffstyp des aktuellen Anwenders.

NAME=macroname

(Erforderlich) Gibt das einzuschließende Makro an. Das Webmodul fügt das Suffix „.mac“ an und sucht nach der Datei in dem Pfad, der von der Konfigurationsdateieigenschaft MacroPath angegeben wird.

Andere Eigenschaften können in Abhängigkeit vom eingeschlossenen Makro erforderlich sein. Eine Makrodatei weist das folgende allgemeine Layout auf:

```
Kommentare
#args
name1 [= value1]
name2 [= value2]
...
#data
data to insert
```

Im Folgenden wird das Dateilayout Zeile für Zeile erläutert:

- **comments:** Die einzigen gültigen Anweisungen in einem Makro vor der Anweisung **#args** sind Kommentare. Kommentare sind entweder durch das Zeichen **#** oder **//** am Anfang gekennzeichnet.
- **#args:** Muss genau so kodiert werden, wie angezeigt, mit dem Rautezeichen (**#**) in Spalte Eins und keinen weiteren Informationen in der Zeile. Diese Anweisung steht am Anfang des args-Abschnitts, der Argumentdefinitionen und Kommentare enthalten kann.
- **name [=value]:** Definiert ein Argument für das Makro. Nur Argumente, die explizit im args-Abschnitt genannt werden, sind für das Makro gültig. Ein Wert, der für ein Argument im args-Abschnitt angegeben wird, entspricht dem Standardwert des Arguments. Argumente ohne Standardwert sind erforderlich und müssen vom Anrufer an die **<PDM_MACRO>**-Anweisung geliefert werden.
- **#data:** Muss genau so kodiert werden, wie angezeigt, mit dem Rautezeichen (**#**) in Spalte Eins und keinen weiteren Informationen in der Zeile. Diese Anweisung steht am Anfang des Datenabschnitts, der Teil des Makros ist, das mit **PDM_MACRO** in die Datei eingefügt wird. Alles im Datenabschnitt wird in die aufrufende Datei eingeschlossen, einschließlich der Zeilen, die Kommentare vor dem Datenabschnitt enthalten.
- **data to insert:** Die in die aufrufende Datei einzufügenden Daten. Diese Daten können im folgenden Format Referenzen auf Argumente enthalten:
- **&{arg_name}:** Diese Referenzen werden durch den Wert des Arguments ersetzt, der vom Anrufer geliefert wird, oder durch den Standardwert, wenn der Anrufer keinen Wert geliefert hat.

Das Webmodul liest Makrodateien normalerweise nur einmal, wenn sie jeweils das erste Mal verwendet werden, und speichert anschließend das analysierte Makro im eigenen Speicher. Dies verbessert zwar die Leistung, kann aber ungünstig sein, wenn Sie ein Makro entwickeln. Verwenden Sie die Konfigurationsdateieigenschaft `SuppressMacroCache`, um dieses Verhalten zu verhindern und damit das Webmakro alle Makros im Speicher verwirft, sobald es mit der Verarbeitung eines neuen Formulars beginnt.

So kommentieren Sie PDM_MACRO-Tags aus

Geben Sie zum Auskommentieren von `<PDM_MACRO>`-Tags ein Ausrufezeichen vor dem P ein: `<!PDM_MACRO>` Um zu verhindern, dass der Browser den auskommentierten Teil des Formulars verarbeitet, fügen Sie `<PDM_IF 0>` vor dem `<!PDM_MACRO>`-Tag und `</PDM_IF>` nach der Zeile ein, die Sie auskommentiert haben.

Beispiel:

```
<PDM_IF 0>
```

```
<!PDM_MACRO NAME=dtlDropdown hdr="Status" attr=status lookup=no  
evt="onBlur=\\\\"detailSyncEditForms(this)\\\\"">  
<!PDM_MACRO NAME=dtlDropdown hdr="Priority" attr=priority lookup=no  
evt="onBlur=\\\\"detailSyncEditForms(this)\\\\"">
```

```
</PDM_IF>
```

Vordefinierte Makros für WSP

CA SDM enthält eine Anzahl von vordefinierten Makros. Die meisten dieser Makros fügen JavaScript-Text ein, um ein Element auf einem Webformular zu erstellen. Mit Web Screen Painter können Sie Formulare mit diesen Makros erstellen und ändern.

Makros für Detailformulare

Folgende Liste beschreibt die Makros für Detailformulare:

button

Fügt eine grafische Schaltfläche ein.

dtlCheckbox

Fügt ein Kontrollkästchen in ein Detailformular ein.

dtlDate

Fügt ein Datumsfeld in ein Detailformular ein.

dtlDateReadonly

Fügt ein schreibgeschütztes Datumsfeld in ein Detailformular ein.

dtlDropdown

Fügt eine Dropdownliste in ein Detailformular ein.

dtlEnd

Beendet ein Detailformular.

dtlEndTable

Beendet eine Tabelle in einem Detailformular.

dtlForm

Beginnt ein Detailformular.

dtlHTMLEditBox

Fügt ein Detailformularfeld ein. Dabei handelt es sich um ein Textfeld, das einen HTML-Editor enthält.

dtlHier

Fügt ein Detailformularfeld ein. Dabei handelt es sich um ein Textfeld, das mit Hilfe einer hierarchischen Suche anhand einer externen Tabelle validiert wird.

Wichtig! Wir empfehlen, dass Sie in der HTML-Datei das Makro "dtlHier" nicht in "dtlLookup" ändern. Verwenden Sie stattdessen im Optionsmanager die Option "suppress_web_hier_search", sodass die Funktion für das automatische Vervollständigen korrekt funktioniert.

dtlLookup

Fügt ein Detailformularfeld ein. Dabei handelt es sich um ein Textfeld, das anhand einer externen Tabelle validiert wird.

dtlLookupReadOnly

Fügt ein Detailformularfeld ein. Dabei handelt es sich um einen schreibgeschützten Hyperlink auf eine externe Tabelle.

dtlReadOnly

Fügt ein schreibgeschütztes Textfeld in ein Detailformular ein.

dtlStart

Beginnt die erste Tabelle in einem Detailformular.

dtlStartExpRow

Beginnt eine erweiterbare Zeile in einem Detailformular.

dtlStartRow

Beginnt eine normale Zeile in einem Detailformular.

dtlTextbox

Fügt ein Textfeld in ein Detailformular ein.

contactLookup

Mit dem Makro "contactLookup" wird eine Kontaktsuche erstellt. Dieses Makro enthält die folgenden Argumente:

```
contactLookup("&{header}", "&{frameName}", "&{factory}", "&{lookupName}");
```

Header

Identifiziert die Suchkopfzeile.

frameName

(Erforderlich) Gibt den Formularnamen an.

factory

Gibt die Factory an.

Standard: "agt"

lookupName

(Erforderlich) Gibt den Suchnamen an.

Mit den folgenden Befehlen können Sie dieses Element auch aktivieren oder deaktivieren:

```
contactLookupDisable(-Name, bDisable)
```

bDisable=

- Aktiviert
Deaktiviert das Element.
- Deaktiviert
Aktiviert das Element.

dtlCheckboxReadonly

Das Makro "dtlCheckboxReadonly" gibt ein schreibgeschütztes Kontrollkästchen im HTML-Detailformular an. Das Makro enthält die folgenden Argumente:

```
detailCheckboxReadonly("&{hdr}", "&{attr}", &{colspan}, "$args.&{attr}", "&{on}", "&{off}");
```

hdr

Gibt den Text der Kopfzeile an.

Standard: "\$args.&{attr}.DISPLAY_NAME"

attr

(Erforderlich) Gibt den Namen des Attributs an.

on = "X"

Gibt den Wert an, der im schreibgeschützten Formular angezeigt wird, wenn das Feld aktiviert ist.

off = ""

Gibt den Wert an, der im schreibgeschützten Formular angezeigt wird, wenn das Feld nicht aktiviert ist.

colspan = 1

Gibt die Anzahl der Spalten im Formular an.

Sowohl in schreibgeschützten als auch in bearbeitbaren Formularen wird das Feld so angezeigt, wie in den Argumenten "on" und "off" angegeben.

Hinweis: Dieses Makro gleicht "dtlCheckbox.mac", ist aber immer schreibgeschützt, auch im Bearbeitungsmodus.

Makros für Listenformulare

IsCol

Gibt eine Spalte in einem Listenformular an.

IsEnd

Beendet den Listenabschnitt in einem Listenformular.

IsStart

Beginnt den Listenabschnitt in einem Listenformular.

IsWrite

Fügt Text in den sich wiederholenden Abschnitt eines Listenformulars ein.

sfDate

Fügt ein Datumsfeld in einen Suchfilter ein.

sfDropdown

Fügt eine Dropdownliste in einen Suchfilter ein.

sfEnd

Beendet einen Suchfilter.

sfHier

Fügt ein Suchfilterfeld ein. Dabei handelt es sich um ein Textfeld, das mit Hilfe einer hierarchischen Suche anhand einer externen Tabelle validiert wird.

sfLookup

Fügt ein Suchfilterfeld ein. Dabei handelt es sich um ein Textfeld, das anhand einer externen Tabelle validiert wird.

sfStart

Beginnt einen Suchfilter.

sfStartRow

Beginnt eine Zeile in einem Suchfilter.

sfTextbox

Fügt ein Textfeld in einen Suchfilter ein.

Makros für Menüleisten

In der folgenden Liste werden die Makros für Menüleisten beschrieben:

endMenu

Beendet ein Menü in einer Menüleiste.

menuItem

Definiert ein globales Element in einem Menü.

endMenubar

Beendet eine Menüleiste.

menuItemLocal

Definiert ein Element im Kontextmenü des aktuellen Fensters.

menubarItem

Definiert ein Menü in einer Menüleiste.

startMenu

Beginnt ein Menü in einer Menüleiste.

startMenubar

Beginnt eine Menüleiste.

PDM_NOTEBOOK: Erstellen eines Notizbuchs

In zahlreichen Formularen in der CA SDM-Analytikerschnittstelle werden verschachtelte Registerkarten (Notizbücher) verwendet. Mit verschachtelten Registerkarten können Sie mehrere Gruppen von Feldern in demselben physischen Bereich des Bildschirms anzeigen, wobei immer nur eine Gruppe zu sehen ist. Der Anwender wählt die Feldergruppe aus, die sichtbar ist, indem er oben im Notizbuch auf eine Registerkarte klickt oder indem er die Tastenkombination `Alt+n` drückt, wobei `n` der Nummer der Registerkarte entspricht. Ein Beispiel für ein Formular, in dem ein Notizbuch verwendet wird, ist "Issue-Detail" (`detail_iss.html`). Es wird empfohlen, für Änderungen am Inhalt der Notizbücher den WSP zu verwenden oder ein Notizbuch in ein Formular einzufügen, das noch kein Notizbuch enthält.

Das folgende Tag markiert das Ende eines Notizbuchs:

```
<PDM_MACRO name=endNotebook>
```

PDM_PRAGMA: Angeben von Serverinformationen

Das `<PDM_PRAGMA>`-Tag wird zum Angeben von Informationen verwendet, die vom Webmodul verwendet werden (z. B. die Version). Es generiert keinen HTML-Code, und kann in einem Formular an einer beliebigen Stelle platziert werden. Mögliche Argumente sind:

Argument	Beschreibung
RELEASE=value	Gibt die CA SDM-Versionsnummer an, die diesem Formular entspricht. Dieser Wert ist "110" für alle Formale von Unicenter Service Desk r11.0. Im Formular kann mit der Variablen „\$prop.release“ auf diesen Wert zugegriffen werden.
SITEMOD=value	Gibt eine standortdefinierte Zeichenfolge an, welche die Änderungen identifiziert, die in diesem Formular durchgeführt wurden. Im Formular kann mit der Variablen „\$prop.sitemod“ auf diesen Wert zugegriffen werden.
VERSION=value	Gibt eine CA Technologies-definierte Zeichenfolge an, welche die Versionsnummer des Formulars identifiziert. Im Formular kann mit der Variablen „\$prop.version“ auf diesen Wert zugegriffen werden.

Argument	Beschreibung
OVERIDE=YES NO	Gibt an, ob Werte in dieser PDM_PRAGMA-Anweisung die Werte in vorherigen PDM_PRAGMA-Anweisungen außer Kraft setzen.

CA Technologies verwendet PDM_PRAGMA-Anweisungen, um Formularversionen zu dokumentieren. Alle Formulare von Unicenter Service Desk r11.0 enthalten die folgende PDM_PRAGMA-Anweisung:

```
<PDM_PRAGMA RELEASE=110>
```

Darüber hinaus schließt das Formular std_head.html die folgende JavaScript-Anweisung ein:
cfgFormRelease = "\$prop.release" - 0;

Mit Hilfe der PDM_PRAGMA-Anweisung und der Variablen "cfgFormRelease" kann die CA SDM-Web-Schnittstelle Formulare von Unicenter Service Desk r11.0 von Formularen früherer Versionen unterscheiden. Versionen vor Unicenter Service Desk r6.0 haben die PDM_PRAGMA-Anweisung nicht unterstützt.

Normalerweise werden nur PDM_PRAGMA-Anweisungen auf der höchsten Ebene einer Datei im Formular (d. h. eine, die nicht mit PDM_INCLUDE eingefügt wurde) verwendet, um "\$prop.release", "\$prop.sitemod" und "\$prop.version" festzulegen. Darüber hinaus setzt keine PDM_PRAGMA-Anweisung einen nicht leeren Wertesatz einer vorherigen PDM_PRAGMA-Anweisung außer Kraft. Sie können OVERRIDE=YES angeben, um festzulegen, dass eine PDM_PRAGMA-Anweisung vorherige PDM_PRAGMA-Anweisungen außer Kraft setzen kann oder dass eine PDM_PRAGMA-Anweisung in einer eingeschlossenen Datei verwendet werden kann.

PDM_SCOREBOARD: Erstellen einer Scoreboard-Struktur

Das <PDM_SCOREBOARD>-Tag wird verwendet, um das Scoreboard zu generieren, das auf der linken Seite des Hauptformulars angezeigt wird. Es nimmt folgende Eigenschaften an:

TARGET=value

Gibt den Namen des Ziel-Frames für Listen an, der durch Klicken auf einen Knoten im Scoreboard angefordert wird. Listen werden im angegebenen Ziel geladen, wobei es sich um einen beliebigen Wert handeln kann, der für das Zielattribut einer Verknüpfung unterstützt wird. Der Standardwert ist *_self* (das Fenster, das das PDM_SCOREBOARD-Tag enthält).

Jedes beliebige HTML-Formular, das ein <PDM_SCOREBOARD>-Tag einschließt, muss ebenfalls die JavaScript-Datei "fldtree.js" einschließen. Diese Datei kann mit der folgenden Anweisung im <HEAD>-Abschnitt des Formulars eingeschlossen werden:

```
<SCRIPT LANGUAGE="JavaScript" SRC="$CAisd/CAisd/fldtree.js"></SCRIPT>
```

Darüber hinaus ist es wünschenswert, die Verknüpfung `scoreboard_asof_data` einzuschließen, um die Datierung der Zahlen in der Baumstruktur anzuzeigen. Ein Beispiel für die Verwendung dieses Tags finden Sie in der verteilten Datei `"scoreboard.html"`.

Die Abfragen, die in das Scoreboard eingeschlossen werden, werden durch den Inhalt der Tabelle „User_Query“ (Objektname `usq`) für den aktuellen Anwender definiert. Ein Datensatz in dieser Tabelle definiert jede Zeile im Baum (Ordner oder Knoten).

Ursprünglich weisen Anwender keine Einträge in der Tabelle „User_Query“ auf. Ein Anwender ohne Einträge in der Tabelle „User_Query“ empfängt den Standardsatz der Scoreboard-Abfragen, die seinem Zugriffstyp zugeordnet sind. Ein Anwender mit administrativer Autorität kann auch das Standard-Scoreboard für einen Zugriffstyp anpassen.

PDM_SET: Einstellen des Werts einer Servervariablen

Das `<PDM_SET>`-Tag wird verwendet, um einer Servervariablen einen Wert zuzuordnen. Sie hat die folgende Syntax:

```
<PDM_SET arg.name[+]=value>
```

Argument

(Erforderlich) Gibt den veränderlichen Typ an und muss `arg` zur normalen Verwendung sein.

Hinweis: Es ist kein `$`-Zeichen vorhanden.

Name

(Erforderlich) Gibt den Namen der Variablen an.

+

(Optional) Gibt an, dass der Wert an den vorhandenen Wert der Variablen angehängt werden sollte. Davor und danach dürfen keine Leerzeichen sein.

=

(Erforderlich) Muss genau wie gezeigt angegeben werden, ohne Leerzeichen davor und danach.

value

(Erforderlich) Gibt den Text an, welcher der Variablen zugeordnet oder daran angehängt wird.

Das `PDM_SET`-Tag kann auch in der Vorverarbeitungsphase verwendet werden, um eine Vorverarbeitungsvariable zu erstellen oder zu aktualisieren.

Weitere Informationen:

[Vorverarbeitung mit dem Webmodul](#) (siehe Seite 489)

PDM_TAB: Erstellen einer Registerkarte in einem Notizbuch

Das <PDM_MACRO name=startNotebook hdr=cng_nb>-Tag wird verwendet, um eine Notizbuchregisterkarte zu definieren. Es wird empfohlen, für Änderungen am Inhalt der Notizbücher den WSP zu verwenden oder ein Notizbuch in ein Formular einzufügen, das noch kein Notizbuch enthält.

PDM_WSP: Steuern der WSP-Vorschau

Das <PDM_WSP>-Tag wird verwendet, um die Vorschaufunktion von WSP zu steuern. Es generiert keinen HTML-Code, und kann in einem Formular an einer beliebigen Stelle platziert werden.

Standardmäßig bestimmt WSP, wie eine Vorschau eines Formulars durch Überprüfen des Formularnamens angezeigt werden kann:

- Bei Detailformularen (mit dem Formularnamen `detail_factory.htmlpl`) zeigt WSP das Formular in der Bearbeitungsansicht mit den Daten der Zeile an, die zuletzt in der entsprechenden Tabelle erstellt wurden. Wenn keine Daten in der Tabelle verfügbar sind, zu deren Anzeige Sie berechtigt sind, zeigt WSP die Formularseite zum Erstellen einer neuen Zeile an. In WSP-Vorschausitzungen kann die Datenbank normalerweise nicht aktualisiert werden. WSP zeigt die Formulare in der Bearbeitungsansicht an, damit Sie alle Funktionen im Voraus sehen können. CA SDM ignoriert jedoch eine Speicheranforderung von einer schreibgeschützten Vorschausitzung. Das Webmodul ändert den Text auf der Schaltfläche „Speichern“ in „Schreibgeschützt“, um visuell darauf hinzuweisen.
- Bei Listenformularen (mit dem Formularnamen `list_factory.htmlpl`) zeigt WSP das Formular in der Listenansicht mit den Daten der Zeile an, die zuletzt in der entsprechenden Tabelle erstellt wurde. Wenn keine Daten in der Tabelle verfügbar sind, zu deren Anzeige Sie berechtigt sind, zeigt WSP das Formular in der Suchansicht mit offenem Filter an.
- Bei anderen Formularen zeigt WSP einfach das Formular ohne Datenbankinhalt an.

Sie können dieses Standardverhalten ändern, indem Sie das PDM_WSP-Tag an einer beliebigen Stelle im Formular einfügen. Sie können z. B. ein Formular mit einer Notizbuchregisterkarte im zugehörigen Detailformular anzeigen oder Voraussetzungen für Formulare angeben, die normalerweise in der Umgebung eines anderen Formulars aufgerufen werden. Folgende Argumente sind möglich:

Eigenschaft	Beschreibung
FACTORY= <i>value</i>	Gibt die Objekt-Engine-Factory an, die von diesem Formular verwendet wird.
PREVIEW= <i>name</i> .html <i>value</i> nein	Gibt den URL der Vorschau an. Hierbei kann es sich um den Namen einer HTML-Datei im Format „xxx.html“, einen CA SDM-URL (wird unverändert verwendet, wenn er mit „OP=“ beginnt) oder das Schlüsselwort „nein“ handeln, das angibt, dass von dem Formular keine Vorschau angezeigt werden kann. Ein Wert, der nicht mit "OP=" beginnt, wird durch Ersetzen einer Referenz des Formulars {factory} oder {factory:} durch eine ID bzw. permanente ID der zuletzt erstellten Zeile aus der entsprechenden Factory geändert, zu deren Anzeige der aktuelle Anwender berechtigt ist.
WHERE= <i>value</i>	Gibt eine WHERE-Klausel an, die für die Suche nach einer oder mehreren darstellenden Zeilen verwendet wird, um sie in der Vorschau im Formular anzuzeigen.
MODE= <i>value</i>	Gibt den Modus der erstellten URL an. Folgende Modi sind möglich: ■ GENERAL: Allgemeines Format. Der Modus wird durch das Argument für die Vorschau bestimmt: detail_xxxx.html – READONLY list_xxxx.html – LIST alle anderen – GRONK ■ READONLY: Detaildatei in der schreibgeschützten Ansicht. ■ EDIT: Detaildatei in der Bearbeitungsansicht. ■ LIST: Listendatei. ■ GRONK: Nicht spezifizierte Datei. In diesem Fall vergeben Sie das Argument "Gronk".

Servervariablen

CA SDM-Informationen werden in die HTML-Vorlage mit Variablen eingeschlossen, die mit einem Dollarzeichen (\$) beginnen. Jede Seite wird mit einigen Variablen erstellt, die in der Vorlagendatei dokumentiert sind. Diese Variablen können auf der Seite eingefügt oder in bedingten Anweisungen verwendet werden:

- Einfache Variablen
- Eigenschaftsvariablen
- Umgebungsvariablen
- Geschäftsobjektvariablen
- Listenvariablen

Einfache Variablen

Einfache Variablen geben Kennzeichen an, die an die Webseite weitergegeben werden. Um auf eine einfache Variable zuzugreifen, verwenden Sie den Variablennamen, dem ein Dollarzeichen (\$) voransteht. Auf diese Weise ist der Wert der Variablen verfügbar. Zwei derartige Variablen lauten z. B. \$CAisd und \$cgi. Das Einfügen von \$CAisd in eine Vorlage führt zur Ersetzung des Haupt-CA SDM-Webserver-Installationsverzeichnisses, während \$cgi auf den URL des Programms "pdmweb.exe" verweist. Einfache Variablen sind im oberen Abschnitt der HTML-Datei dokumentiert, die sie verwenden.

Im Folgenden ist eine Liste der Variablen angezeigt, die in allen HTML-Dateien verwendet werden können:

\$ACCESS.group

Das Objekt für Anwenderzugriffsprivilegien enthält die Privilegieneinstellungen der Funktionsgruppe *group* für den aktuell angemeldeten Anwender. Zum Beispiel enthält \$ACCESS.admin den Privilegiwert für die funktionale Gruppe „admin“. Gültige Privilegienwerte sind:

- 0-KEIN ZUGRIFF
- 1-ANZEIGEN
- 2-ÄNDERN

Diese Variable ist im Anmeldeformular nicht verfügbar.

\$cgi

Der URL des Programms "pdmweb.exe".

\$cst

Das Datenobjekt des aktuell angemeldeten Anwenders. Diese Variable ist im Anmeldeformular nicht verfügbar. Sie können auf einzelne Attribute dieses Objekts mit dem Formular `$cst.Attributname` verweisen (z. B. `$cst.first_name`).

\$CAisd

Der URL des Haupt-CA SDM-Webserver-Installationsverzeichnisses.

\$MachineName

Der in der Datei "web.cfg" definierte Rechnername.

Hinweis: Informationen zu "web.cfg" finden Sie im *Administrationshandbuch*.

\$ProductName

Der Produktname, der in der Datei "NX.env" definiert ist.

\$SESSION

Das Sitzungsobjekt speichert alle Sitzungsvariablen einschließlich der Sitzungs-ID (`$SESSION.SID`) sowie alle Variablen, die in der Datei "web.cfg" definiert sind.

Hinweis: Informationen zu "web.cfg" finden Sie im *Administrationshandbuch*.

\$USER_STATE

Anwenderspezifische Statusinformationen.

Eigenschaftsvariablen

Eigenschaftsvariablen stellen eine Eigenschaft der Konfigurationsdatei "web.cfg" dar. In einer HTML-Vorlagendatei können Sie auf alle Einträge in der Datei "web.cfg" zugreifen (einschließlich anwenderspezifische Einträge), indem Sie das Präfix "\$prop" voranstellen.

Eine der Zeilen in der Datei "web.cfg", die z. B. die Anzahl an Einträgen angibt, die auf einer einzelnen Seite in einem Listenformular angezeigt werden, lautet folgendermaßen:

```
ListPageLength 10
```

Sie können in einer HTML-Vorlage auf diese Variable mit der folgenden Spezifikation verweisen:

`$prop.ListPageLength`

Wenn Sie das besondere Tag `<PDM_INCLUDE>` verwenden, um eine andere Datei in eine Vorlagendatei zu integrieren, können Sie zusätzliche Eigenschaften als Attribute des `<PDM_INCLUDE>`-Tags angeben. Sie können auf diese Eigenschaften in der eingeschlossenen Datei auf dieselbe Art verweisen wie auf die Eigenschaften in der Datei "web.cfg". Eine Eigenschaft, die als `<PDM_INCLUDE>`-Attribut angegeben wird, das denselben Namen wie die Eigenschaft web.cfg aufweist, setzt die Eigenschaft web.cfg in der eingeschlossenen Datei außer Kraft.

So erstellt z. B. das folgende `<PDM_INCLUDE>`-Tag die Eigenschaft `$prop.menuubar`, auf die innerhalb der Datei "std_body.html" verwiesen werden kann:

```
<PDM_INCLUDE FILE=std_body.html menuubar=no>
```

Hinweis: Zum Referenzieren auf die Konfigurationsdateieigenschaft xxx gibt es zwei Möglichkeiten: `$prop.xxx` oder `$SESSION.xxx`. Beide geben den gleichen Wert zurück. Die Syntax `$prop.xxx` Syntax wird jedoch bevorzugt, da weniger Serveraufwand anfällt.

Neben den Eigenschaften in der Datei "web.cfg" sind mehrere vordefinierte Eigenschaften verfügbar, auf die mit `$prop` zugegriffen werden kann. Diese sind:

`$prop.browser`

Eine Zeichenfolge, die den verwendeten Server identifiziert. Für den Internet Explorer lautet diese Zeichenfolge „IE“.

`$prop.combo_name`

Eine Zeichenfolge im Format „last_name, first_name middle_name“, die den Namen des aktuellen Anwenders enthält.

`$prop.factory`

Eine Zeichenfolge, welche die Factory enthält, die dem aktuellen Formular zugeordnet ist, wie z. B. "cr" für Requests und "iss" für Issues.

`$prop.FID`

Eine Zeichenfolge, welche die numerische Formular-ID des aktuellen Formulars enthält.

`$prop.form_name`

Eine Zeichenfolge, die den Namen der aktuellen HTML-Vorlage im Format xxx.html enthält.

`$prop.form_name_1`

Eine Zeichenfolge, welche die Teilkette des Formularnamens vor dem ersten Unterstrich enthält. Für das Formular detail_chg_edit.html würde form_name_1 beispielsweise „detail“ lauten.

\$prop.form_name_2

Eine Zeichenfolge, welche die Teilkette des Formularnamens nach dem ersten und vor dem letzten Unterstrich (oder Punkt) enthält. Für das Formular `detail_chg_edit.html` würde `form_name_2` beispielsweise „chg“ lauten.

\$prop.form_name_3

Eine Zeichenfolge, welche die Teilkette des Formularnamens nach dem letzten Unterstrich und vor dem Punkt enthält. Für das Formular `"detail_chg_edit.html"` würde `"form_name_3"` beispielsweise `"edit"` lauten. Für das kombinierte Detailformular, dessen Dateiname das Format `"detail_hatxxx.html"` aufweist, ist `"$prop.form_name_3"` auf die aktuelle Ansicht eingestellt (entweder `"ro"` oder `"edit"`).

\$prop.release

Eine Zeichenfolge, welche die Versionsstufe des Formulars enthält. Die Anweisung `PDM_PRAGMA` enthält weitere Details zu dieser Eigenschaft.

\$prop.SID

Eine Zeichenfolge, welche die numerische Sitzungs-ID der aktuellen Sitzung enthält.

\$prop.sitemod

Eine Zeichenfolge, die den standortdefinierten Änderungsnamen des Formulars enthält. Die Anweisung `PDM_PRAGMA` enthält weitere Details zu dieser Eigenschaft.

\$prop.user_type

Eine Zeichenfolge, die „analyst“, „customer“, „employee“ oder „guest“ enthält.

\$prop.version

Eine Zeichenfolge, welche die Version des Formulars enthält. Die Anweisung `PDM_PRAGMA` enthält weitere Details zu dieser Eigenschaft.

Weitere Informationen:

[PDM PRAGMA: Angeben von Serverinformationen](#) (siehe Seite 457)

Umgebungsvariablen

Umgebungsvariablen stellen einen Eintrag innerhalb der Konfigurationsdatei „NX.env“ dar. Sie können auf jeden Eintrag in der Datei „NX.env“ innerhalb einer HTML-Vorlagendatei verweisen, indem Sie im das Präfix „\$env“ voranstellen.

Eine der Zeilen in der Datei "NX.env", die den Hostnamen des CA SDM-Servers angibt, lautet folgendermaßen:

```
@NX_SERVER=hostname
```

Sie können auf diese Variable innerhalb einer HTML-Vorlagendatei mit der folgenden Spezifikation verweisen:

```
$env.NX_SERVER
```

Geschäftsobjektvariablen

Geschäftsobjektvariablen stellen ein CA SDM-Objekt wie einen Issue oder Request dar. Um auf ein Objekt zuzugreifen, müssen Sie mit dem Variablennamen gefolgt von einem Punkt (.) gefolgt von dem Namen des Attributs, das Sie anzeigen möchten, beginnen. Zum Beispiel bei einem Issue, in der das Objekt gemäß Konvention durch die Variable `args` dargestellt wird, können Sie die Beschreibung, das Öffnungsdatum, die Telefonnummer des Bevollmächtigten, die Anzahl der Aktivitäten für den Issue und die Beschreibung der ersten Aktivität anzeigen, wie im Folgenden dargestellt:

```
$args.description  
$args.open_date  
$args.assignee.phone_number  
$args.act_log.length  
$args.act_log.0.description
```

Sie können geschweifte Klammern verwenden, um den Variablennamen zu begrenzen, wenn er nicht von Leerzeichen umgeben ist. Sie ist z. B. sowohl „\$foo bar“ als auch „\${foo}bar“ gültig. Sie können auch die Variable „args“ verwenden, um auf andere Werte als Attribute (z. B. `$args.KEEP.name`, wie unter Unterstützte Vorgänge beschrieben) zuzugreifen.

Es ist möglich, dass eine Variable, die kein Attribut ist, nicht definiert werden kann. Es kann z. B. möglich sein, auf ein Formular von zwei unterschiedlichen Orten aus zuzugreifen, von denen aber nur einer einen Wert für `$args.KEEP.foo` liefert. Sie können einen Standardwert für einen `$args`-Verweis mit der folgenden Syntax angeben, wobei die Zeichenfolge nach dem Doppelpunkt durch den Verweis ersetzt wird, wenn *variable* nicht definiert ist:

```
${args.variable:default}
```

Zeitzone-Datumsvariablen

Zeitzone-Datumsvariablen sind ein Sonderfall der Geschäftsobjektvariablen. Sie bieten die Möglichkeit, universelle Daten (UTC), die als Ganzzahlen dargestellt werden, in Zeichenfolgedaten zu konvertieren, die an die Zeitzone des Browsers des Anwenders angepasst sind. Die Variable für die Darstellung von Ganzzahldaten lautet:

`$args.attr_name_INT_DATE`

Beispiel: `$args.open_date_INT_DATE`

Factory-Datumsvariablen

Factory-Datumsvariablen sind ein Sonderfall der Geschäftsobjektvariablen. Eine Factory-Datumsvariable wird durch Informationen über ein referenziertes Objekt ersetzt. Sieben solcher Variablen sind verfügbar:

`$args.attr_name.COMMON_NAME`

Der allgemeine Name (extern lesbare Zeichenfolge) der Tabelle, auf die von dem Attribut verwiesen wird. Beispiel: In dem Formular „Request – Detail“ entspricht der Wert für „`$args.assignee.COMMON_NAME`“ dem Kombinationsnamen („last, first, middle“) des Bevollmächtigten.

`$args.attr_name.COMMON_NAME_ATTR`

Der Attributname des allgemeinen Namens in der Tabelle, auf die von dem Attribut verwiesen wird. Beispiel: In dem Formular „Request – Detail“ ist der Wert für „`$args.assignee.COMMON_NAME_ATTR`“ gleich „combo_name“.

`$args.FACTORY_attr_name`

Der Name der Factory, die dem angegebenen Attribut zugeordnet ist. Beispiel: In dem Formular „Request – Detail“ ist der Wert für „`$args.FACTORY_assignee`“ gleich „agt“.

`$args.LENGTH_attr_name`

Die maximale Länge des Attributs. Beispiel: In dem Formular „Request – Detail“ ist der Wert für „`$args.LENGTH_summary`“ gleich „240“.

`$args.attr_name.REL_ATTR`

Das relative Attribut (Fremdschlüssel) des Attributs. Beispiel: in dem Formular „Request – Detail“ entspricht der Wert für „`$args.assignee.REL_ATTR`“ dem Wert des ID-Feldes für den Bevollmächtigten.

`$args.attr_name.REL_ATTR_ATTR`

Der Attributname von rel_attr in der Tabelle, auf die dieses Attribut verweist. Beispiel: In dem Formular „Request – Detail“ ist der Wert für „`$args.assignee.REL_ATTR_ATTR`“ gleich „id“.

\$args.REQUIRED_attr_name

Eine Zeichenfolge, entweder „0“ oder „1“, die angibt, ob das referenzierte Attribut erforderlich ist.

\$args.attr_name.SELECTIONS

Eine Liste der gültigen Auswahlmöglichkeiten für *attr_name*. Dieser Wert ist eine leere Zeichenfolge, wenn *attr_name* kein Verweis auf eine andere Tabelle ist, oder wenn die Größe der Tabelle, auf die *attr_name* verweist, den Wert der Konfigurationsdateieigenschaft *SelListCacheMax* überschreitet. Andernfalls ist die SELECTIONS-Variable eine Zeichenfolge, die den allgemeinen Namen und das relative Attribut von allen Einträgen in der referenzierten Tabelle enthält. Nachfolgende Werte werden von der Zeichenfolge „@,@“ getrennt, so dass der Wert der Variablen das folgende Format aufweist:

„cname1@,@rel_attr1@,@cname2@,@rel_attr2“

\$args.factory_SEL_UNDER_LIMIT

Eine Zeichenfolge, entweder „0“ oder „1“, die angibt, ob die aktuelle Anzahl an Zeilen in der Tabelle, die *factory* entspricht, geringer als der Wert der Konfigurationsdateieigenschaft *SelListCacheMax* ist. Diese Variable wird zu Gunsten der SELECTIONS-Variablen missbilligt, die in allen neuen Formularen verwendet werden sollte.

Factory-Datumsvariablen, die einen Verweis mit Punkten (COMMON_NAME, REL_ATTR und SELECTIONS) enthalten, können mit einem Verweis mit Punkten von beliebiger Länge verwendet werden. Beispiel: In einem Formular „Request – Detail“ kann „\$args.assignee.organization.COMMON_NAME“ durch den externen Namen der Organisation des Bevollmächtigten ersetzt werden.

Listenvariablen

Listenvariablen werden verwendet, um Daten zu wiederholen. Der Zugriff auf Listenvariablen erfolgt über Listen-Tags, wie unter PDM_LIST: Formatieren einer Liste mit Datenbankzeilen beschrieben.

Unterstützte Servervorgänge

Mit den folgenden unterstützten Vorgängen können Sie CA SDM-Webseiten mit Ihren Webseiten integrieren:

CREATE_NEW

Stellt eine Standardschnittstelle bereit, in der Anwender eine neue Zeile in einer angegebenen Tabelle erstellen können. Dabei muss der Objektname angegeben werden. Standardmäßig wird die Vorlage *detail_xxx_edit.html* für das Objekt *xxx* verwendet. Sie können die .html-Datei überschreiben, indem Sie die HTML-Eigenschaft angeben.

Erforderliche Specifier:

FACTORY=object-name

Optionale Specifier:

ALG_PRESET=preset_expression
ALG_PRESET_REL=preset_expression
CREATE_ALG=activity_log_type
HTML=zdetailxxx_factory.html
KEEP.attr_name=value
PRESET=preset_expression
PRESET_REL=preset expression
SET.attr_name=value
use_template=1 | 0 (0 is the default)

Hinweis: Um den HTML-Spezifizierer mit CREATE_NEW zu verwenden, muss das referenzierte Formular einen Namen gemäß der Konvention *zdetailxxx_factory.html* aufweisen. Er muss mit der Zeichenfolge "zdetail" beginnen, gefolgt von beliebigen alphanumerischen Zeichen (einschließlich einer Null-Zeichenfolge), gefolgt von einem Unterstrich und dem Factory-Namen.

ENDSESSION oder LOGOUT

Beendet die Sitzung, bei der der Anwender derzeit angemeldet ist. ENDSESSION ist der bevorzugte Vorgang.

GENERIC_LIST

Bietet eine Standardschnittstelle, über die der Anwender eine Liste von jeder Tabelle in der Datenbank anzeigen kann. Dabei muss der Objektname angegeben werden. Standardmäßig wird die Vorlage *list_xxx.html* für das Objekt *xxx* verwendet. Sie können die .html-Datei überschreiben, indem Sie die HTML-Eigenschaft angeben.

Erforderliche Specifier:

FACTORY=object-name
KEEP.attr_name=value

DISPLAY_FORM

Bietet eine Standardschnittstelle, über die der Anwender jedes beliebige angepasste Formular anzeigen kann.

Erforderliche Specifier:

HTMPL=*html_file*

Hinweis: DISPLAY_FORM ersetzt JUST_GRONK_IT. Bestehende Implementierungen können JUST_GRONK_IT weiterhin verwenden, da die Funktionsweise dieselbe wie bei DISPLAY_FORM ist. DISPLAY_FORM ist der bevorzugte Vorgang.

MENU

Zeigt die Seite mit dem Hauptmenü an, die in der Eigenschaft "Menü" der Datei "web.cfg" definiert ist

Optionale Specifier:

HTMPL=*menufile*

menufile ist der Name einer alternativen Hauptmenüdatei.

PAGE_EXTENSION

Ermöglicht dem Webmaster, zusätzliche Erweiterungen zur Schnittstelle anzugeben.

Erforderliche Specifier:

NAME=*html_file*

html_file ist einer der Dateinamen, die in der Anweisung "UserPageExtensions" der Konfigurationsdatei aufgeführt wird.

Optionale Specifier:

REQUIRES_LOGIN=1

Falls vorhanden, wird eine Anmeldeseite angezeigt, sofern der Anwender derzeit nicht angemeldet ist. Fehlt dieser Spezifizierer oder ist er auf Null gesetzt, so wird die Datei angezeigt ohne zu überprüfen, ob der Anwender aktuell angemeldet ist.

RELOG

Zeigt die Anmeldeseite an.

SEARCH

Bietet eine Standardschnittstelle, über die in der Datenbank nach Tabellen gesucht werden kann. Bei diesem Vorgang wird davon ausgegangen, dass eine entsprechende "search_xxx.html"-Datei erstellt wurde. xxx ist der *Objektname* wie in "bopcfg" in den .maj-Dateien des Verzeichnisses "majic" definiert.

Hinweis: Weitere Informationen finden Sie im *technischen CA SDM-Referenzhandbuch*. Standardmäßig werden die Ergebnisse dieser Suche in list_xxx.html angezeigt. Sie kann jedoch durch Angeben der HTML-Eigenschaft überschrieben werden.

Erforderliche Specifier:

FACTORY=object-name
QBE.op.attr_name=value

Optionale Specifier:

ALG_PRESET=preset_expression
ALG_PRESET_REL=preset_expression
CREATE_ALG=activity_log_type
HTML=list_html_file
KEEP.attr_name=value

SEC_REFRESH

Aktualisiert die Anwenderinformationen für den Zugriff im Sicherheitsundersystem. Für diesen Vorgang wird für Anwender, die über MODIFY-Berechtigungen (für die Funktionsgruppe "admin") verfügen, im Menüfenster ein Hyperlink angegeben. Nachdem die Zugriffsrechte der Anwender mit dem Sicherheitsprogramm aktualisiert wurden, bietet dieser Vorgang die Möglichkeit, die Zugriffsinformationen zu aktualisieren. (Dadurch werden die Sicherheitsinformationen für alle Anwender aktualisiert.)

Hinweis: Sicherheitsaktualisierungen stellen einen asynchronen Prozess dar. Nachdem eine Sicherheitsaktualisierung ausgeführt wurde, wird eine Meldung in der Standardprotokolldatei (stdlog) angezeigt.

SET_MENU

Das Verhalten dieses Vorgangs entspricht dem Verhalten von MENU, wenn MENU mit der HTML-Variablen verwendet wird. Der einzige Unterschied besteht darin, dass dieser Vorgang das Standardmenüformular für das Menüformular festlegt, das in der HTML-Eigenschaft angegeben ist.

Erforderliche Specifier:

HTML=html_file

Hinweis: Dieser Vorgang setzt die Einstellung für MENU in der Datei "web.cfg" außer Kraft, bis der Webservice neu gestartet wird.

SHOW_DETAIL

Bietet eine Standardschnittstelle, über die der Anwender ein -schreibgeschütztes Detail einer Zeile in einer angegebenen Tabelle anzeigen kann. Der permanente ID-Name muss angegeben werden (von dem der Objektname abgeleitet wurde). Standardmäßig wird die Vorlage detail_XXX_ro.html für das Objekt XXX verwendet. Die .html-Datei kann durch Eingabe der HTML-Eigenschaft überschrieben werden.

Erforderliche Specifier:

PERSID=*persistent-id*

Optionale Specifier:

ALG_PRESET=*preset_expression*

ALG_PRESET_REL=*preset_expression*

CREATE_ALG=*activity_log_type*

HTML=*readonly_detail_html_file*

UPDATE

Bietet eine Standardschnittstelle für die Bearbeitung von Tabellen. Die ID und der Objektname müssen übergeben werden, damit dem Anwender ein bearbeitungsfähiges Detailformular angezeigt wird. Standardmäßig hat der Anwender zwei Minuten lang exklusiven Zugriff auf den Datensatz. Dabei wird garantiert, dass er Änderungen in die Datenbank einfügen kann, wenn er sie in diesem Zeitraum übermittelt.

Erforderliche Specifier:

PERSID=*persistent-id* or

SET.id=*id-of-row-to-update* FACTORY=*object-name*

Optionale Specifier:

NEXT_PERSID=*persistent-id* (des Datensatzes, der nach der erfolgreichen Aktualisierung angezeigt wird)

KEEP.attr_name=*value*

KEY.attr_name=*value*

HTML=zdetailxxx_factory.html

Hinweis: Um den HTML-Spezifizierer mit UPDATE zu verwenden, muss das referenzierte Formular einen Namen gemäß der Konvention zdetailxxx_factory.html aufweisen. Er muss mit der Zeichenfolge "zdetail" beginnen, gefolgt von beliebigen alphanumerischen Zeichen (einschließlich einer Null-Zeichenfolge), gefolgt von einem Unterstrich und dem Factory-Namen.

Hinweis: Informationen zu "web.cfg" finden Sie im *Administrationshandbuch*.

Vorgangsvariablen

In der folgenden Tabelle sind die Variablen aufgeführt, die für jeden der Vorgänge in der vorherigen Tabelle festgelegt werden können:

Variablen	Beschreibung	Betrieb
ALG_PRESET ALG_PRESET_REL	Gibt Werte für ein oder mehrere Attribute des Aktivitätsprotokolls an, das als Ergebnis der CREATE_ALG-Variablen geschaffen wurde. Wenn CREATE_ALG nicht angegeben ist, werden ALG_PRESET und ALG_PRESET_REL ignoriert.	CREATE_NEW SEARCH SHOW_DETAIL
CREATE_ALG	Gibt den Aktivitätsprotokolltyp eines Aktivitätsprotokolls an, das als Nebeneffekt des Vorgangs erstellt wird. Verwenden Sie die Variablen ALG_PRESET und ALG_PRESET_REL, um Werte für die Attribute des neuen Aktivitätsprotokolls anzugeben. Wie lange das Erstellen des Aktivitätsprotokolls dauert, hängt vom Vorgang ab, wie im Folgenden aufgeführt: CREATE_NEW Das Aktivitätsprotokoll wird erstellt, wenn der neue Datensatz gespeichert wird. Wenn der neue Datensatz nicht gespeichert wird, wird auch kein Aktivitätsprotokoll erstellt. SEARCH Das Aktivitätsprotokoll wird erstellt, wenn ein Datensatz im Listenformular ausgewählt wird. Wenn der Datensatz nicht ausgewählt, sondern angezeigt wird (d. h., wenn der Anwender explizit den Befehl „Ansicht“ im Mouseover-Menü des Listenformulars auswählt), wird kein Aktivitätsprotokoll erstellt. SHOW_DETAIL Das Aktivitätsprotokoll wird erstellt, bevor der Datensatz angezeigt wird.	CREATE_NEW SEARCH SHOW_DETAIL
FACTORY	Gibt die Objektklasse an, nach der gesucht bzw. die erstellt oder aktualisiert werden soll. Sie können einen beliebigen als OBJECT angegebenen Namen in den *.maj-Dateien in "\$NX_ROOT/bopcfg" verwenden, wie im technischen CA SDM-Referenzhandbuch aufgeführt.	CREATE_NEW GENERIC_LIST SEARCH UPDATE

Variablen	Beschreibung	Betrieb
HTMPL	Ermöglicht dem HTMPL-Autor, die Standardkonventionen für die Benennung von Vorlagen außer Kraft zu setzen, und gibt explizit die HTMPL-Datei an, die angezeigt werden soll und nicht die Standardvorlage. Hinweis: Wenn der HTMPL-Spezifizierer mit CREATE_NEW oder UPDATE verwendet wird, muss der Name des referenzierten Formulars der Namenskonvention "zdetailxxx_factory.html" entsprechen, wobei xxx beliebige Zeichen sind und <i>factory</i> dem Herstellernamen entspricht.	CREATE_NEW DISPLAY_FORM JUST_GRONK_IT MENU SEARCH SET_MENU SHOW_DETAIL UPDATE
KEEP.name	Gibt den Wert an, der gespeichert und zwischen Seiten übergeben werden kann.	CREATE_NEW GENERIC_LIST SEARCH UPDATE
KEY.attr_name	Entspricht SET.attr_name mit der Ausnahme, dass dies eine Suche für attr_name angibt, wobei es sich um einen Verweis auf eine andere Tabelle oder ein anderes Objekt handeln muss.	UPDATE
NEXT_PERSID	Gibt die permanente ID des Datensatzes an, der als nächstes angezeigt werden soll.	UPDATE
PERSID	Gibt die permanente ID des anzuzeigenden Datensatzes an. Sie können dies auf eine der folgenden Arten angeben: Direkt mit einer permanenten ID, die aus einem Herstellernamen, einem Doppelpunkt (:) und einer eindeutigen Datenbank-ID (Ganzzahl) besteht. Beispiel: PERSID=chg:1234 gibt den Change mit der Datenbank-ID 1234 an. Indirekt mit einer permanenten ID, die aus einem Herstellernamen, einem Doppelpunkt (:), einem Attributnamen, einem zweiten Doppelpunkt (:), und einem Wert besteht. Diese Form von PERSID gibt den Datensatz der angegebenen Factory an, die über ein Attribut des angegebenen Wertes verfügt. Beispiel: PERSID=chg:chg_ref_num:demo:3 gibt den Change mit der Referenznummer demo:3 an.	SHOW_DETAIL UPDATE
PRESET PRESET_REL	Gibt Werte für ein oder mehrere Attribute des Datensatzes an, der als Ergebnis der CREATE_NEW-Variablen erstellt wurde. Wenn CREATE_NEW nicht angegeben ist, wird PRESET ignoriert.	CREATE_NEW

Variablen	Beschreibung	Betrieb
QBE.op.attr_name	Gibt die Werte an, die beim Durchführen einer Suche verwendet werden. Diese Werte werden mit einem QBE-Schlüsselwort identifiziert, wobei <i>attr_name</i> einen beliebigen Attributnamen auf einem Ticket identifiziert, der eingerichtet werden kann, und <i>op</i> angibt, wo nach dem Attribut zu suchen ist: EQ ist gleich dem Wert NE ist ungleich dem Wert GT ist größer als der Wert LT ist kleiner als der Wert GE ist größer als oder gleich dem Wert LE ist kleiner als oder gleich dem Wert NU ist NULL NN ist NOT NULL IN entspricht dem Ausdruck SQL LIKE KY enthält den eingegebenen Text Wenn Sie keine QBE-Variablen definieren, wird das Standardsuchfenster angezeigt.	SEARCH
SET.attr_name	Gibt einen Attributnamen an, der beim Erstellen eines Tickets verwendet werden soll, wobei <i>attr_Name</i> ein beliebiges Attribut in einem Ticket kennzeichnet, das festgelegt werden kann. Die Attributnamen variieren in Abhängigkeit vom zu Grunde liegenden Objekt. Alle Objekte und ihre Attribute sind in den *.maj-Dateien im Majic-Verzeichnis in "bopcfg" zu finden, wie im <i>technischen CA SDM-Referenzhandbuch</i> aufgeführt.	CREATE_NEW UPDATE
SET.id	Gibt die Datenbank-ID der zu aktualisierenden Zeile an.	UPDATE
SKIPLIST	Wenn diese Variable auf 1 eingestellt ist, wird bei Suchvorgängen mit 1 Treffer keine Ergebnisliste angezeigt. Stattdessen wird das schreibgeschützte Detail direkt angezeigt.	SEARCH
use_template	Wenn diese Variable auf 1 eingestellt ist, gibt der SEARCH-Vorgang eine Liste mit Vorlagen zurück. Die von Ihnen in der Liste ausgewählte Vorlage wird in dem CREATE_NEW-Vorgang verwendet, um einen neuen Datensatz auszufüllen. Diese Variable ist für Changes, Issues und Requests gültig.	CREATE_NEW SEARCH

Weitere Informationen:

[Syntax von PRESET, PRESET_REL, ALG_PRESET und ALG_PRESET_REL](#) (siehe Seite 476)

Syntax von PRESET, PRESET_REL, ALG_PRESET und ALG_PRESET_REL

Die Schlüsselwörter PRESET, PRESET_REL, ALG_PRESET und ALG_PRESET_REL in dem URL geben Anfangswerte für Attribute des Tickets bzw. Aktivitätsprotokolls an. Es gibt zwei mögliche Formate:

[ALG_]PRESET=attr:value

Zeigt an, dass für das angegebene Attribut des Tickets oder Aktivitätsprotokolls der angegebene Wert definiert werden soll. Beispiel: Mit der folgenden Spezifikation wird die Beschreibung des neuen Tickets auf „Hello.“ festgelegt.

PRESET=description:Hello

[ALG_]PRESET_REL=attr:obj.relattr:testattr:value

Zeigt an, dass für das angegebene Attribut des Tickets oder Aktivitätsprotokolls ein Wert definiert werden soll, der aus einer anderen Datenbanktabelle kopiert wird. Der Wert wird aus dem *relattr*-Attribut des *Objekts* kopiert, dessen *testattr* über den angegebenen *Wert* verfügt. Beispiel: Die folgende Spezifikation legt für das analyst-Attribut des neuen Tickets die ID des Kontakts mit der Anwender-ID xyz123 fest:

PRESET_REL=analyst:cnt.id:user:xyz123

Wenn dieses Format verwendet wird, muss die implizierte Abfrage einen einmaligen Datensatz abrufen. Wenn mehrere Kontakte (oder keiner) die Anwender-ID xyz123 aufweisen, hat die Spezifikation PRESET in dem Beispiel keine Auswirkung.

Die Schlüsselwörter PRESET, PRESET_REL, ALG_PRESET und ALG_PRESET_REL können so oft wie gewünscht im URL verfügbar sein, so dass mehrere Attribute eingestellt werden können. Alternativ kann ein einzelner Schlüsselwort-Operand mehrere Werte durch @@ getrennt angeben. Wenn der Separator „@@“ verwendet wird, können Sie Werteformate für die Schlüsselwörter [ALG_]PRESET und [ALG_]PRESET_REL nicht vermischen. Im folgenden Beispiel werden zwei unterschiedliche Arten für die Angabe von Werten für Ticketbeschreibung, -zusammenfassung und -analytiker gezeigt:

PRESET=description:Hello+PRESET=summary:HelloThere+PRESET_REL=analyst:cnt.id:user id:xyz123

PRESET=description:Hello@@summary:HelloThere+PRESET_REL=analyst:cnt.id:user:xyz123

Für Requests, Issues, Incidents, Probleme und Changes unterstützen PRESET und PRESET_REL das Schlüsselwortattribut ASSET, um ein Objekt mit einem Asset zu verknüpfen. Das ASSET-Attribut aktualisiert das affected_resource-Attribut eines Request, Incident oder Issue oder die Asset LREL eines Incidents oder eines Change.

Verknüpfungen – Beispiele

Die folgenden Verknüpfungsbeispiele schließen den Pfad zu CA SDM nicht ein. Alle CA SDM-URLs beginnen mit Code in folgendem Format:

`http://hostname[:port]/CAisd/pdmweb.exe`

Dabei entspricht *hostname* dem Namen Ihres Servers und *port* (optional) der Portnummer, wenn Sie Tomcat verwenden. Dieser Code wird in den folgenden URL-Beispielen als eine Ellipse (...) angezeigt:

- Um einen Request mit einem betroffenen Endanwender mit der Anwender-ID "tooda01" zu erstellen, geben Sie beispielsweise die URL ein:

`...?OP=CREATE_NEW+FACTORY=cr+PRESET_REL=customer:cnt.id:userid:tooda01`

- Um eine Liste aller Requests von Anwender "tooda01" anzuzeigen, geben Sie beispielsweise folgende URL an:

`...?OP=SEARCH+FACTORY=cr+QBE.EQ.assignee.userid:tooda01`

- Um das Detailformular für den Request "1234" anzuzeigen, geben Sie beispielsweise folgende URL an:

`...?OP=SHOW_DETAIL+FACTORY=cr+PERSID=cr:ref_num:1234 (schreibgeschützt)`

`...?OP=UPDATE+FACTORY=cr+PERSID=cr:ref_num:1234 (zu bearbeiten)`

Hinweis: Wenn Sie Webservices für die Authentifizierung verwenden, können Sie die Anmeldeaufforderung umgehen. Informationen zur Methode "getBopsid()" finden Sie im technischen CA SDM-Referenzhandbuch.

Erweiterte Anpassung

Beim Anpassen von Webseiten sollten Sie sich über verschiedene Aspekte im Klaren sein. Dies gilt insbesondere dann, wenn Sie zum Ändern von HTML andere Tools als Web Screen Painter nutzen wollen, oder wenn Ihre kundenspezifische Anforderungen außergewöhnlich komplexe Anpassungen verlangen. Es wird dringend empfohlen, CA SDM-Webseiten mithilfe von WSP anzupassen, bevor Sie einen anderen Ansatz ausprobieren. Mit WSP können Sie fast jede erforderliche Anpassung ausführen. Die Software verarbeitet auch Anfragen zur Systemverwaltung wie das Einfügen von Aktualisierungen in das Verzeichnis "site mods" und das Verteilen von veröffentlichten Dateien auf alle Server.

Das Webmodul und sein Cache

Bei der Anpassung von Webseiten ist es hilfreich, die Struktur des CA SDM-Webservers zu verstehen. Die Web-Schnittstelle verwendet entweder einen J2EE-Servlet-Container wie Tomcat oder einen HTTP-Standardserver wie Apache oder Microsoft Internet Information Server (IIS). Wenn ein Benutzer eine CA SDM-Webseite anfordert, ruft der HTTP-Server das verfügbare Programm "pdmweb.exe" auf.

Nachdem das Programm gestartet wurde, stellt "pdmweb.exe" eine Verbindung mit einem CA SDM-Daemon (oder Windows-Dienst) her, der die Web-Engine aufruft. Das Webmodul interpretiert die Anfrage des Benutzers. Für die meisten Anfragen ist es erforderlich, dass das Webmodul nach einer Vorlagendatei (HTMPL) sucht und sie in Standard-HTML überträgt. Für die Übertragung ist es normalerweise erforderlich, dass das Webmodul mit einem CA SDM-Server kommuniziert, um die Datenbank zu lesen oder zu aktualisieren und die Datenbankinformationen in den generierten HTML-Code einzuschließen. Sobald der HTML-Code vollständig ist, sendet ihn die Web-Engine an das Programm "pdmweb.exe", das ihn wiederum zurück an den Browser des Benutzers sendet.

Um die Leistung zu maximieren, liest die Web-Engine jede HTMPL-Datei nur einmal. Nachdem die Datei analysiert und bestimmt wurde, wie sie in HTML übertragen wird, speichert das Webmodul die analysierte Datei in seinem Cache, wodurch die Verarbeitungszeit erheblich reduziert wird, wenn die Datei das nächste Mal angefordert wird. Obgleich der Cache in einer Produktionsumgebung durchaus nützlich ist, kann er in einer Entwicklungsumgebung nachteilig sein, denn Änderungen an HTMPL-Dateien werden erst wirksam, nachdem die Web-Engine neu gestartet oder das Dienstprogramm "pdm_webcache" ausgeführt wurde. In einer Entwicklungsumgebung können Sie dieses Verhalten umgehen, indem Sie die Konfigurationsdateieigenschaft "SuppressHtmlCache" angeben. Allerdings wird empfohlen, den HTMPL-Cache in einer Produktionsumgebung nicht zu deaktivieren. Dies würde sich stark auf die Gesamtleistung der Web-Engine auswirken.

Hinweis: Weitere Informationen finden Sie im *Administrationshandbuch*.

Die Webseiten, die von "pdmweb.exe" bedient werden, werden durch Lesen der HTMPL-Dateien generiert und zum Generieren von HTML verwendet. HTML-Vorlagendateien sind durch das Dateisuffix von ".html" gekennzeichnet. Diese Vorlagendateien können Sie ändern und somit die CA SDM-Webseiten anpassen.

Das Programm "pdm_webcache"

Verwenden Sie das Programm "pdm_webcache", um ein oder mehrere HTML-Formulare aus dem Cache des Webmoduls zu entfernen. Dadurch wird das Webmodul gezwungen, diese Formulare von der Diskette abzurufen, wenn sie das nächste Mal verwendet werden, damit die Änderungen an den Formularen wirksam werden.

pdm_webcache [-f *form-name*] [-g *form-group*] [-i *interface*] [-p *process*] [-v]

-f *form-name*

Gibt den Namen des Formulars, das aus dem Cache entfernt werden soll (z. B. detail_cr.html). Sie können "%" (oder "**") als Platzhalterzeichen verwenden, um mehrere Formulare auszuwählen. Zum Beispiel die Spezifikation:

-f detail%

wählt alle Detailformulare aus.

Dieses Argument ist optional. Wenn es weggelassen wird, werden alle Formulare im Cache ausgewählt.

-g *Formulargruppe*

Gibt den Namen der Formulargruppe an, die aus dem Cache entfernt werden soll (z. B. Analytiker). Sie können „%" (oder „*“) als Platzhalterzeichen verwenden, um mehrere Formulargruppen auszuwählen. Zum Beispiel die Spezifikation:

-g Anal%

wählt alle Formulargruppen aus, die mit „Anal“ beginnen.

Dieses Argument ist optional. Wenn es weggelassen wird, werden alle Formulargruppen im Cache ausgewählt.

-i *Schnittstelle*

Gibt den Namen der Web-Schnittstelle an, die aus dem Cache entfernt werden soll (z. B. Analytiker, Kunde oder Mitarbeiter). Sie können „%" (oder „*“) als Platzhalterzeichen verwenden. Zum Beispiel die Spezifikation:

-i a%

wählt die Analytikerschnittstelle aus.

Dieses Argument ist optional. Wenn es weggelassen wird, werden alle Schnittstellen im Cache ausgewählt.

-p *Prozess*

Gibt den Namen des Webmodul-Prozesses an, dessen Cache geändert werden soll (z. B. web:local).

Dieses Argument ist optional. Wenn es weggelassen wird, werden alle Webmodule ausgewählt.

-v

Gibt die Ausgabe in Textform an. Wenn dieses Argument angegeben ist, führt pdm_webcache den vollen Namen von jedem Formular auf, das aus dem Cache entfernt wurde, und zwar in folgendem Format:

Schnittstelle:Formulargruppe:Formularname

Dieses Argument ist optional. Wenn es weggelassen ist, gibt pdm_webcache nur die Anzahl an Formularen aus, die aus dem Cache des Webmoduls entfernt wurden.

So ändern Sie HTML-Vorlagen

In der Regel können Sie zwei Arten von Änderungen an HTML-Vorlagen vornehmen:

- Sie können Änderungen vornehmen, die für den Benutzer sichtbar sind, jedoch von der Web-Schnittstelle nicht vor der Anzeige geändert werden. Sie können z. B. eine GIF-Datei mit Ihrem Unternehmenslogo in den Web-Schnittstellenseiten ("Pass Through") einfügen, indem Sie eine Referenz zur entsprechenden Vorlagendatei hinzufügen, oder Sie könnten JavaScript zur Ihrer Seite hinzufügen, um die Eingabe zu validieren. Alle Änderungen, die Sie an der HTML-Datei vornehmen, die nicht in einem PDM-Tag enthalten sind, wie im Folgenden definiert, werden unverändert an den HTML-Code übergeben, der an den Benutzer zurückgegeben wird.
- Sie können die ersetzbaren Abschnitte der Vorlagen ändern. Beispielsweise können Sie der Seite "Anfrage - Detail" neue Anwendungsdaten hinzufügen.

Anhand verschiedener Einträge in der Vorlage haben Sie folgende Möglichkeiten:

- Informationen aus CA SDM dem Benutzer anzeigen.
- eine Abfragenseite einrichten.
- Verknüpfungen zu anderen CA SDM-Seiten mit Hilfe von Verknüpfungs-Tags erstellen.

Dateien, die nicht geändert werden sollten

Gewisse HTML-Vorlagen und JavaScript-Dateien enthalten Informationen, die für viele CA SDM-Webformulare erforderlich sind. Die Informationen in diesen Vorlagen sind sowohl versionsabhängig als auch kritisch für die erfolgreiche Operation der CA SDM-Web-Schnittstelle. Deshalb werden diese Dateien immer ersetzt, wenn eine neue Version von CA SDM herausgegeben wird. Durchgeführte Änderungen an diesen Dateien werden nicht aktualisiert.

Die Vorlagen, die von diesen Einschränkungen betroffen sind, lauten folgendermaßen:

ahdtop.html

Enthält Stile, Skripte und JavaScript-Variablen, die in der ganzen CA SDM-Web-Schnittstelle verwendet werden. Diese Datei gehört zum Haupt-Frameset der Web-Schnittstelle und ist während einer Sitzung immer verfügbar. Alle CA SDM-Formulare haben Zugriff auf die JavaScript-Variablen „ahdtop“, die auf das Fenster mit „ahdtop.html“ verweist.

menu_frames.html

Definiert das HTML-Frameset, das vom CA SDM-Hauptformular verwendet wird.

msg_cat.js

Enthält den Text aller Meldungen, die in CA SDM-JavaScript-Dateien verwendet werden.

reports.html

Enthält Daten, die für Webberichte erforderlich sind.

std_body.html

Enthält Standardinformationen, die am Anfang des Abschnitts „BODY“ der meisten HTML-Vorlagen verwendet werden.

std_footer.html

Enthält Standardinformationen, die am Ende des Abschnitts „BODY“ der meisten HTML-Vorlagen verwendet werden.

std_head.html

Enthält Standardinformationen, die am Anfang des Abschnitts „HEAD“ der meisten HTML-Vorlagen verwendet werden.

styles.html

Enthält CSS-Stile, die in der ganzen CA SDM-Web-Schnittstelle verwendet werden.

Obwohl Sie diese Dateien nicht direkt ändern können, können Sie zusätzliche Informationen zu ihnen hinzufügen. Jede eingeschränkte Datei „xxx.html“ (mit Ausnahme von „menu_frames.html“ und „reports.html“) weist eine entsprechende Datei „xxx_site.html“ auf, die Sie anpassen können. Zum Beispiel können Sie „ahdtop.html“ weitere Informationen hinzufügen, indem Sie „ahdtop_site.html“ anpassen, oder neue Meldungen hinzufügen, indem Sie „msg_cat_site.js“ anpassen.

Die „xxx_site.html“-Datei zu jeder eingeschränkten Datei wird nach der Hauptdatei geladen. So können Sie JavaScript in der Hauptdatei überschreiben oder ändern. Gehen Sie sorgfältig vor, wenn Sie Informationen ändern, da schlecht entworfene Änderungen an diesen Dateien unerwartete Probleme in der gesamten CA SDM-Web-Schnittstelle verursachen können.

Weitere Informationen:

[Vom HTTP-Server verwendete Verzeichnisse](#) (siehe Seite 486)

Richtlinien für neue HTML-Dateien

Sie können Ihre eigenen HTML-Dateien zur CA SDM-Web-Schnittstelle hinzufügen. Befolgen Sie diese Richtlinien, um sicherzustellen, dass Ihre HTML-Dateien gut mit dem Rest der CA SDM-Schnittstelle interagieren:

1. Schließen Sie die folgende Anweisung irgendwo im <HEAD>-Abschnitt der Datei ein. Diese Anweisung sollte gegebenenfalls der <TITLE>-Anweisung folgen. Sie definiert mehrere globale JavaScripte-Variablen, die für die CA SDM-Web-Schnittstelle erforderlich sind, und registriert auch Ihre Seite mit dem CA SDM-Fenstermanager:

```
<PDM_INCLUDE FILE=std_head.html>
```

2. Schließen Sie das folgende Attribut als Teil des <BODY>-Tags der Datei ein. Dieses Attribut unterstützt den CA SDM-Fenstermanager dabei, Ihre Seite zu verfolgen:

```
onUnload="deregister_window() "
```

3. Schließen Sie die folgende Anweisung am Anfang des <BODY>-Abschnitts Ihrer Datei ein. Das Argument „menubar=no“ ist optional. Wenn es angegeben wird, unterdrückt es die CA SDM-Menüleiste:

```
<PDM_INCLUDE FILE=std_body.html [menubar=no]>
```

4. Schließen Sie die folgende Anweisung am Ende des <BODY>-Abschnitts Ihrer Datei ein.

```
<PDM_INCLUDE FILE=std_footer.html>
```

Hinzufügen von benutzerdefinierten Statusinformationen

Viele Kunden möchten ihre eigenen Statusinformationen in die CA SDM-Webseiten einbetten. In diesem Fall muss CA SDM die Statusinformationen an alle nachfolgenden Seiten, die er bedient, bis zur Sitzung des Benutzers weiterleiten. Diese Informationen können mit bedingten Anweisungen in den HTML-Dateien abgefragt werden.

Statusinformationen für die Sitzung eines Benutzers werden erhalten, indem das Sonderattribut USER_STATE in Ihren Verknüpfungen oder Formularen eingerichtet wird. Nach dem Senden an die Web-Engine von CA SDM verfügt jede Seite, die dem Benutzer angezeigt wird, über die HTML-Variable USER_STATE. Diese ist auf den letzten Wert gesetzt, der für USER_STATE gesendet wurde.

Die folgenden Beispiele zeigen, wie Sie einen Eintrag in CA SDM von einem anderen Bereich Ihres Standorts, wie z. B. von Seiten für den Vertrieb einrichten können:

- Verwenden von Hyperlinks

```
<a href="/CAisd/pdmweb.exe?USER_STATE=Sales">Service Desk</a>
```

- Verwenden von Formularen mit ausgeblendeten Feldern

```
<form action="http://IhrHost.com/CAisd/pdmweb.exe">
<input type=hidden name=USER_STATE value=Sales>
```

Klicken Sie auf die Schaltfläche für den Service Desk.

```
<input type=submit>
</form>
```

Dann können Sie Ihre HTML-Formulare auf der Basis von Statusinformationen anpassen:

```
<PDM_IF "$USER_STATE" == "Vertrieb">
```

Benutzerdefinierte Informationen für Vertriebsmitarbeiter

```
<PDM_ELIF "$USER_STATE" == "Ingenieure">
```

Benutzerdefinierte Informationen für Ingenieure

```
<PDM_ELSE>
```

Informationen für alle anderen

```
</PDM_IF>
```

Direktes Erstellen einer Anfrage von einer Vorlage

Über eine URL können Sie eine Anfrage direkt aus einer Vorlage erstellen.

Beispiel

```
http://Rechnername/CAisd/pdmweb.exe?FACTORY=cr+OP=CREATE
NEW+PERSID=cr:3106+use_template=1
```

wobei cr:3106 der persid der Vorlage entspricht.

Konfigurieren eines Tickets für schnelles Schließen mit vordefinierten Informationen

In der Ad-hoc-Profil-Ansicht können Sie ein Ticket zum schnellen Schließen erstellen, wie z. B. ein Incident zum schnellen Schließen. Fügen Sie beim Erstellen eines Tickets zum schnellen Schließen der URL eine voreingestellte Zeichenfolge hinzu, um automatisch eine Beschreibung, eine Zusammenfassung oder sonstige Feldinformationen hinzuzufügen.

Führen Sie die folgenden Schritte aus, um dem Ticket für schnelles Schließen eine voreingestellte Zeichenfolge hinzuzufügen:

1. Kopieren Sie die Datei `ahdtop_site.html` von `NX_ROOT/bopcfg/www/html/default` nach `NX_ROOT/site/mods/html/www/default`.
2. Bearbeiten Sie die Datei "[ahdtop_site.html](#)" (siehe Seite 484) mit der entsprechenden Variablen (je nach dem Typ des Tickets zum schnellen Schließen).
3. Melden Sie sich bei CA SDM an.
4. Erstellen Sie ein Ticket zum schnellen Schließen.

Die voreingestellten Informationen werden dem Ticket hinzugefügt.

Erstellen eines Tickets für schnelles Schließen mit vordefinierten Optionen

In "Ad-hoc-Profil" können Sie ein Ticket zum schnellen Schließen erstellen, wie z. B. ein Incident zum schnellen Schließen. Über die Option zum schnellen Schließen können Sie ein neues Ticket in einem Schritt öffnen und schließen, wenn Sie z. B. den Incident in der gleichen Sitzung öffnen und lösen. Beim Erstellen eines Tickets zum schnellen Schließen können Sie der URL eine voreingestellte Zeichenfolge hinzufügen, um automatisch eine Beschreibung, eine Zusammenfassung oder sonstige Feldinformationen hinzuzufügen.

So erstellen Sie ein Ticket zum schnellen Schließen mit voreingestellten Optionen

1. Kopieren Sie die Datei `ahdtop_site.html` von `NX_ROOT/bopcfg/www/html/default` nach `NX_ROOT/site/mods/html/www/default`.
2. Bearbeiten Sie die Datei `"ahdtop_site.html"`, um die entsprechende Variable (abhängig vom Typ des Tickets zum schnellen Schließen) mit der voreingestellten Zeichenfolge hinzuzufügen.

- Schnelles Schließen - Incident - `"var-quick_close_preset_in"`
- Schnelles Schließen - Problem - `"var-quick_close_preset_pr"`
- Schnelles Schließen - Anfrage - `"var-quick_close_preset_cr"`
- Schnelles Schließen - Issue - `"var-quick_close_preset_iss"`

Beispiel: In der folgenden Zeichenkette wird für einen Incident zum schnellen Schließen die Beschreibung auf `"HelloIncident"` und die Zusammenfassung auf `"HelloIncidentSummary"` festgelegt.

```
var quick_close_preset_in =  
"PRESET=description:HelloIncident@summary:HelloIncidentSummary";
```

3. Melden Sie sich bei CA SDM an.
4. Wählen Sie auf der Registerkarte "Service Desk" die Option "Ansicht" > "Ad-hoc-Profil" aus.
5. Füllen Sie eines oder mehrere der Suchfelder für den Kontakt aus, und klicken Sie auf "Suchen".

In der "Schnellprofil - Kontaktliste" werden die Kontakte, die Ihren Suchkriterien entsprechen.

6. Wählen Sie einen Kontakt aus.
 7. Klicken Sie auf "Schnelles Schließen".
- Das Ticket wird mit den voreingestellten Informationen erstellt.

Vom HTTP-Server verwendete Verzeichnisse

Bei der Standardinstallation von CA SDM werden zwei virtuelle Verzeichnisse für Ihren HTTP-Server definiert:

- Das virtuelle Verzeichnis "CAisd" zeigt auf das folgende Verzeichnis Ihrer CA SDM-Installation:

Unter Windows: *installationsverzeichnis\bopcfg\www\wwwroot*
Unter UNIX: *\$NX_ROOT/bopcfg/www/wwwroot*
- Das virtuelle Verzeichnis "CAisd/sitemods" zeigt auf das folgende Verzeichnis Ihrer CA SDM-Installation:

Unter Windows: *installationsverzeichnis\site\mods\www\wwwroot*
Unter UNIX: *\$NX_ROOT/site/mods/www/wwwroot*

Die Unterverzeichnisse unter diesen virtuellen Verzeichnissen sind:

Unterverzeichnis	Inhalt
css	Stylesheets
help	Hilfe zur Web-Schnittstelle
html	HTML-Dateien
img	Grafikdateien
scripts	JavaScript
sitemods	Standortdefinierte Anpassungen

Wenn Sie eine angepasste Version einer der Dateien im Verzeichnis "css", "html", "img" oder "scripts" erstellen möchten, wird empfohlen, dass Sie die Datei nicht im Verzeichnis "/CAisd" aktualisieren. Speichern Sie die Datei stattdessen im entsprechenden Unterverzeichnis von "/CAisd/sitemods". Wenn Sie z. B. ein Stylesheet im Verzeichnis "/CAisd/css" ändern möchten, speichern Sie die angepasste Version im Verzeichnis "/CAisd/sitemods/css". Wenn das Webmodul eine HTML-Datei analysiert, modifiziert es automatisch Dateinamen, die mit \$CAisd beginnen, so dass sie auf "sitemods" verweisen, wenn die Datei in einem Unterverzeichnis von "sitemods" existiert.

Die Verwendung des Verzeichnisses `"/CAisd/sitemods"` weist folgende Vorteile auf:

- Sie ermöglicht das Verfolgen der verteilten Dateien, die Sie geändert haben.
- Sie bietet den einfachen Zugriff auf die ursprüngliche Version, wenn eine Frage oder ein Problem auftritt.
- Sie vereinfacht das Verfahren zum Installieren der Wartung oder einer neuen Version, da bei der Installation von CA SDM nichts in das Verzeichnis `"/CAisd/sitemods"` eingefügt wird.

Hinweis: Das Unterverzeichnis `"/CAisd/sitemods/help"` ist nicht vorhanden. Da es sich bei den Hilfedaten um standardmäßige HTML-Dateien (keine HTMPL-Vorlagen) handelt, kann das Webmodul die Dateireferenzen nicht dynamisch ändern. Wenn eine Anpassung der Hilfedaten erforderlich ist, müssen Sie die Änderungen in `"/CAisd/help"` vornehmen.

Das HTML-Unterverzeichnis enthält ein paar häufig verwendete Dateien, die vom Webmodul nicht verarbeitet werden müssen und die Leistung verbessern können, wenn sie im Cache des Browsers gespeichert werden. Wenn Sie eine angepasste Version einer beliebigen dieser Dateien erstellen, prüfen Sie die Datei sorgfältig auf Referenzen zu anderen angepassten Dateien. Da keine Verarbeitung durch das Webmodul stattfindet, müssen Sie gegebenenfalls manuell eine Referenz auf das Verzeichnis `"sitemods"` einfügen.

Download von PDF-Anhängen

Wenn Sie einen PDF-Anhang herunterladen und in CA SDM anzeigen möchten, wird die PDF-Datei möglicherweise nicht richtig dargestellt, oder es wird ein leeres Fenster angezeigt. Dies kann nach der Aktualisierung von Adobe Acrobat auf Version 7.0 oder 8.0 vorkommen. Führen Sie folgende Schritte aus, um die PDF-Datei korrekt in CA SDM anzuzeigen:

1. Legen Sie für den Parameter *forceDecompressOnDownload* in `"$NX_ROOT\bopcfg\www\CATALINA_BASE\webapps\CAisd\WEB-INF\web.xml"` die Einstellung JA fest.

Hinweis: `"$NX_ROOT"` ist unter Linux `"/opt/CAisd"`.

2. Starten Sie die CA SDM-Dienste neu.

Nachschlagen von Informationen in Referenztabellen

Eingabefelder in einem Detailformular zum Bearbeiten eines Datensatzes in einer Datenbank haben den Namen `SET.attr_name`. Beim Speichern des Datensatzes werden Daten aus SET-Feldern direkt in den zugrunde liegenden Datensatz kopiert. Ein Eingabefeld für ein Attribut, das auf eine andere Tabelle verweist, sollte deshalb das `REL_ATTR` (Fremdschlüssel) der Tabelle enthalten. Dies ist normalerweise die ID, die permanente ID oder der Code des Referenzdatensatzes.

Benutzer geben die REL_ATTR-Werte nicht direkt an, und die SET-Felder für Attribute, die auf eine andere Tabelle verweisen, sind ausgeblendet. Das sichtbare Feld auf dem Formular weist die Bezeichnung KEY.attr_name auf. Es enthält den allgemeinen Namen des referenzierten Datensatzes. Ein allgemeiner Name muss in ein REL_ATTR konvertiert werden, um den Datensatz zu aktualisieren. Es gibt mehrere Möglichkeiten, wann dies gemacht werden kann:

- Für Felder mit einer Dropdownliste: Der SET-Wert wird direkt über die Dropdownliste angegeben.
- Für Felder mit Suchfunktion: Wenn der Benutzer auf das Suchsymbol klickt und ein Element auswählt, wird der SET-Wert aus dem ausgewählten Element kopiert.
- Für Felder mit Suchfunktion, in die der Benutzer einen Teilschlüssel eingibt, der den Datensatz eindeutig identifiziert: Nachdem der Benutzer auf die Bezeichnung geklickt hat, fordert der Browser den SET-Wert vom Server an und kopiert beides, den SET-Wert und den vollständigen Schlüssel, zurück in das Formular.
- Wenn die Autofill-Konfigurationsdateieigenschaft angegeben oder standardmäßig übernommen wird, und der Benutzer einen Teilschlüssel angibt, der den Datensatz eindeutig identifiziert, und auf „Notizbuch“ klickt, um das Feld zu verlassen, fordert der Browser den SET-Wert vom Server an und kopiert sowohl den SET-Wert als auch den vollständigen Schlüssel zurück in das Formular.

Wenn andernfalls der Datensatz mit einem KEY-Wert und keinem SET-Wert gespeichert wird, löst das Webmodul den Wert während des Speichervorgangs auf. Wenn ein KEY-Wert nicht zu einem eindeutigen SET-Wert aufgelöst werden kann, wird der Speichervorgang nicht zugelassen und das Bearbeitungsformular erneut angezeigt.

Wenn ein Formular erneut angezeigt wird, weil der Speichervorgang aufgrund eines Auflösungsfehlers bei der Suche fehlgeschlagen ist, sind die folgenden Variablen in der HTML-Datei für jedes Attributfeld verfügbar, für das eine Suche ausgeführt wurde:

LIST_attr

Enthält alle gefundenen Übereinstimmungen. Dies wird in <PDM_SELECT>-Anweisungen typischerweise als die rechte Seite vom Feld „SOURCE=“ angegeben.

FLAGS_attr

Dies wird auf einen der folgenden Werte eingestellt:

0

Zeigt das ursprüngliche Suchfeld an.

1

Mehr als ein und weniger als MaxSelectList wurden gefunden (in diesem Fall wird normalerweise eine <PDM_SELECT>-Liste angezeigt).

2

Es wurden keine Übereinstimmungen gefunden.

3

Es wurden zu viele Übereinstimmungen gefunden (mehr als MaxSelectList).

SEARCH_STATUS_attr string

Enthält die Textzeichenfolge "TooManyMatches" aus der Datei "web.cfg".

Hinweis: Informationen zu "web.cfg" finden Sie im *Administrationshandbuch*.

Angeben von Surchvorgängen nach Kontakten

Wenn Sie einen Kontakt (Nachname, Vorname, zweiter Vorname) in einem bearbeitungsfähigen Formular angeben, können Sie den Kontaktnamen mit Kommas (,) oder Leerzeichen, aber nicht beides, begrenzen. Kommas sind vorzuziehen, weil Namen häufig über eingebettete Leerzeichen verfügen, die Probleme verursachen.

Da eine Kombination aus Kommas und Leerzeichen nicht zulässig ist, besagt die Anwesenheit von Kommas, dass alle Teile des Namens durch Kommas getrennt sind. Wenn keine Kommas vorhanden sind, werden die Namen durch Leerzeichen begrenzt.

Da die Informationen schließlich an eine SQL-Abfrage übergeben werden, dient das Prozentzeichen (%) als Platzhalter. Beispiel: "P%, J%" würde "Public, John", "Penxa, Jane" und anderen Namen entsprechen, deren Nachname mit P und deren Vorname mit J beginnt (ob zwischen der Groß- bzw. Kleinschreibung unterschieden wird, hängt von der zugrunde liegenden Datenbank ab). (Ob zwischen Groß- und Kleinbuchstaben unterschieden wird, hängt von der zugrunde liegenden Datenbank ab.) In ähnlicher Weise würde "P% J%" dieselben Namen finden.

Im Gegensatz dazu würde „P%, Jon D“ alle Kontakte abrufen, deren Vorname Jon lautet und deren zweiter Vorname mit D und deren Nachname mit P beginnt, da das Vorhandensein von einem Komma bedeutet, dass die Namen durch Kommas abgetrennt sind. Deshalb würde nach dem Nachnamen „P%“ und dem Vornamen „Jon D“ gesucht werden. Um diesen Fehler zu vermeiden, geben Sie stattdessen „P%, Jon, D“ an.

Vorverarbeitung mit dem Webmodul

Die Web-Engine durchläuft bei der Verarbeitung einer HTML-Datei zwei Phasen:

- Die Vorverarbeitungsphase, wenn die HTML-Datei und alle referenzierten Dateien (einschließlich Dateien, die von den Tags PDM_INCLUDE und PDM_MACRO referenziert werden) gelesen werden. Die Ausgabe der Vorverarbeitung entspricht einem Eintrag im internen Cache des Webmoduls.
- Die Phase der Generierung, in der das Webmodul das Formular aus dem Cache liest und HTML generiert. Die Ausgabe der Generierung ist HTML-Code, der an den Browser gesendet wird.

Die Vorverarbeitungsphase wird normalerweise vom Webmodul einmal für jedes Formular ausgeführt. Die Generierungsphase wird demgegenüber immer dann ausgeführt, wenn ein Formular angefordert wird.

Sie können während der Vorverarbeitungsphase die Tags PDM_SET und PDM_EVAL verwenden, um Informationen wie HTML-Text zu generieren und zu speichern, die das Webmodul in der Generierungsphase verwenden kann.

Vorverarbeitungsvariablen

Präprozessorvariablen beginnen mit der Zeichenfolge "\$PRE". Sie werden mit dem Tag PDM_SET erstellt und aktualisiert. Dieses Tag weist die folgende Syntax auf, wenn es mit einer Vorverarbeitungsvariablen verwendet wird:

```
<PDM_SET arg.name[+]=value>
```

Dieses Tag weist eine Vorverarbeitungsvariable zu bzw. aktualisiert sie, wobei es die Variable ggf. erstellt. Es wird verarbeitet, wenn das Webmodul darauf stößt, während es ein Formular liest. Nur die unveränderlichen "PDM_IF"-Anweisungen beeinflussen das "PDM_SET"-Tag einer Präprozessorvariablen. Andere Anweisungen werden ignoriert.

Erkennen unveränderlicher PDM_IF-Anweisungen

Das Webmodul erkennt unveränderliche PDM_IF-Anweisungen, wenn es ein Formular analysiert. PDM_IF-Anweisungen gelten als unveränderlich, wenn ihre Argumente ausschließlich aus Literalen, Umgebungsvariablen, konstanten Eigenschaften und Vorverarbeitungsvariablen bestehen. Wenn das Webmodul eine unveränderliche PDM_IF-Anweisung erkennt, bewertet es sofort seine Bedingung. Dies hat die folgenden Auswirkungen:

- Die Tags PDM_SET und PDM_EVAL, die von einer unveränderlichen PDM_IF-Anweisung umgangen werden, werden ignoriert. Alle anderen "pdm_eval"- und "PDM_SET"-Tags, die auf Präprozessorvariablen verweisen, werden auch dann bei der Verarbeitung ausgeführt, wenn sie sich in einer veränderlichen "PDM-IF"-Anweisung befinden.

- Referenzen auf Formularvariablen, die von einer unveränderlichen PDM_IF-Anweisung umgangen werden, werden ignoriert. Und ihr Wert wird nicht abgerufen, wenn das Formular verwendet wird. Mit Hilfe dieses Verfahrens können Sie das Leistungsverhalten eines Formulars verbessern. Die Anweisung im folgenden Beispiel führt dazu, dass die Web-Engine den Wert von "\$args.def" abrufen, bevor das Formular angezeigt wird:

```
<PDM_IF "$env.NX_OTB_MARKET == "itil" && "$args.a" == 1>
<h1>This is form $args.def</h1>
</PDM_IF>
```

Durch das folgende Segment bestimmt die Web-Engine jedoch, dass die erste Anweisung "PDM_IF" unveränderlich ist, und ruft den Wert von "\$args.def" nur ab, wenn \$NX_OTB_MARKET "itil" lautet.

```
<PDM_IF "$env.NX_OTB_MARKET == "itil">
<PDM_IF "$args.a" == 1>
<h1>This is form $args.def</h1>
</PDM_IF>
</PDM_IF>
```

PDM_EVAL: Einfügen von Text aus einer Präprozessorvariablen

Das PDM_EVAL-Tag fügt den Wert einer Vorverarbeitungsvariablen in die Eingabe der Webmodul-Analysefunktion ein. Wenn das Tag in einem Makro verwendet wird, wird es erst wirksam, wenn das Makro abgeschlossen ist.

Das PDM_EVAL-Tag ähnelt PDM_INCLUDE oder PDM_MACRO in seiner Funktionsweise. Es fügt den Text exakt an dem Punkt des Tags in die Analyse ein, so als ob der Wert der Variablen anstelle des Tags kodiert wurde..

PDM_EVAL weist die folgende Syntax auf:

```
<PDM_EVAL text=PRE.name>
```

wobei PRE.name den Namen der Vorverarbeitungsvariablen angibt, deren Wert in die Eingabe des Webmoduls einzufügen ist.

Die Ausführung des PDM_EVAL-Tags kann durch unveränderliche PDM_IF-Anweisungen gesteuert werden.

Wichtig! Unter UNIX muss LIBPATH vor Ausführung des Dienstprogramms gesetzt werden. Für diese Aufgabe verwenden Sie "pdm_task". Bevor Sie das Dienstprogramm ausführen, geben Sie "pdm_task pdm_eval" ein.

Formloses Anpassen von Detailformularen

Die Themen in diesem Abschnitt beschreiben, wie formloses Anpassen von Detailformularen ausgeführt wird.

Verwenden von Javascript in Detailformularen

Verwenden Sie WSP, um Ihre eigenen Felder zu einem Detailformular hinzuzufügen oder um die standardmäßig im Formular verfügbaren Felder neu anzuordnen bzw. deren Bearbeitungsmerkmale zu ändern. Manchmal möchten Sie ein Formular jedoch stärker anpassen, als einfach neue Felder zu einem Raster hinzuzufügen. In CA SDM sind eine Reihe von JavaScript-Funktionen verfügbar, die das Zusammenführen Ihrer eigenen Anpassungen in einem Kombinationsdetailformular vereinfachen und mit denen Sie dem Formular das gewünschte Erscheinungsbild geben können. Diese Funktionen werden folgendermaßen zusammengefasst:

- Sie können HTML immer vor der DetailForm()-Anweisung oder nach der endDetail()-Anweisung platzieren, ohne dass dies Auswirkungen auf die Funktionsweise des Detailformulars haben würde.
- Sie können die detailEndTable()-Funktion verwenden, um die Tabelle zu schließen, die alle Detailformularelemente in einem Raster anordnet. Nachdem Sie diese Aufgabe durchgeführt haben, können Sie eigenes HTML in jedem beliebigen Format anordnen. In diesem Fall befindet sich der HTML-Text innerhalb des Detailformulars. Alle Formularfelder in dem Text werden an das Webmodul übergeben, wenn der Anwender auf „Speichern“ klickt. Sie können die detailNextID()-Funktion verwenden, um ID-Felder für Ihre HTML-Elemente zu generieren, durch die sie an der mausfreien Navigation im Detailformular partizipieren können. Sie können mehrere Beispiele für dieses Verfahren in den Notizbuchregisterkarten (z.B. "xx_alg_tab.html") sehen.
- Sie können Ihren eigenen HTML-Text mit einem dtlStartRow-Makro verfolgen, mit dem Sie die Formatierung von Standarddetailformularen erneut ausführen können. Mit diesem Makro wird ein zweites Raster gestartet, dessen Felder nicht unbedingt mit denen im ersten Raster ausgerichtet sein müssen. Dieses Verfahren wird in jeder Notizbuchregisterkarte verwendet.
- Wenn Sie ein angepasstes Element am Ende einer Zeile einfügen möchten, können Sie die detailWriteRow()-Funktion verwenden, um den Inhalt einer Zeile herauszuschreiben, ohne sie zu schließen. Ein Beispiel für dieses Verfahren stellt der Code dar, der die Schaltfläche "24 Stunden" in detail_cr.html und detail_iss.html generiert.
- Wenn Sie explizit den Inhalt von einem Element in einer Zeile angeben möchten, ohne die Tabelle auszuschließen, die das Raster anordnet, könne Sie die detailRowHdr()-Funktion verwenden, um den Headertext anzugeben, und die detailSetRowData()-Funktion, um den Datentext anzugeben. Ein Beispiel für dieses Verfahren stellt der Code dar, der das Timer-Feld in detail_cr.html und detail_iss.html generiert.

- Wenn Sie eine Funktion angeben, die den Wert eines Feldes (normalerweise in einem Event-Handler) überprüft, und möchten, dass die Ergebnisse während einer browserseitige Überprüfung berichtet werden (so dass ein fehlerhaftes Feld mit einer dicken roten Umrandung und eine Fehlermeldung mit einer gelben Umrandung oben im Formular angezeigt werden), verwenden Sie die Funktion `detailReportValidation()`. Ein Beispiel dafür finden Sie in der Funktion `"validate_duration()"`, mit der die Felder für die Dauer in `"xx_candp_tab.html"` validiert werden. Die Funktion `"validate_duration()"` befindet sich in der Datei `"val_type.js"`.
- Wenn Sie den HTML-Text überprüfen möchten, der für ein Detailformular generiert wird, können Sie die Funktionen `docWrite()` und `docWriteIn()` anstelle der Standardfunktionen `document.write()` und `document.writeIn()` verwenden. Wenn Sie die Funktion `holdHTMLText()` an einer beliebigen Stelle im `<HEAD>`-Abschnitt des Formulars aufrufen, zeigt `<USDK>` ein Debugformular an, das einen `TEXTAREA` mit dem gesamten HTML-Text enthält, der für das Formular generiert wurde. Diesen Text können Sie überprüfen oder kopieren und in ein Prüftool einfügen.

Denken Sie beim Zusammenfügen der Änderungen daran, dass das Kombinationsdetailformular sowohl in einer schreibgeschützten als auch in einer bearbeitbaren Ansicht angezeigt wird. Wenn Ihre Anpassungen ausdrücklich für die eine oder die andere Ansicht gelten, können Sie die aktuelle Ansicht folgendermaßen testen:

- In Javascript ist der Ausdruck `„_dtl.edit“` in der Bearbeitungsansicht wahr und in der schreibgeschützten Ansicht falsch.
- In Javascript oder im offenen HTML können die Anweisungen

```
<PDM_IF "$prop.form_name_3" == "edit">
```

(Wird nur in der Bearbeitungsansicht verwendet)

```
</PDM_IF>
```

oder

```
<PDM_IF "$prop.form_name_3" == "ro">
```

(Wird nur in der schreibgeschützten Ansicht verwendet)

```
</PDM_IF>
```

Wird verwendet, um Code einzuklammern, der nur für die Bearbeitungs- bzw. schreibgeschützte Ansicht gedacht ist.

detailEndTable()

Diese Funktion schließt die HTML-Tabelle ein, welche die Detailformularelemente in einem Raster anordnet. Sie verfügt über keine Argumente.

Sie können ein neues Raster mit dem `dtlStartRow()`-Makro starten. Elemente in einem neuen Raster werden jedoch nicht unbedingt mit Elementen in einem vorherigen Raster ausgerichtet.

detailNextID([colspan,][lastelement])

Diese Funktion gibt eine Zeichenfolge mit folgender Form zurück:

```
" ID=df_nn_nn TABINDEX=n onFocus=func onBlur=func"
```

Das Einfügen dieser Zeichenfolge in ein HTML-Element führt dazu, dass das Element die Konventionen der mausfreien CA SDM-Navigation verfolgt, einschließlich der Erreichbarkeit mit den Pfeiltasten und dem Ändern der Farbe in hellgelb, wenn es fokussiert wird. Die zurückgegebene Zeichenfolge beginnt mit einem Leerzeichen und weist kein Leerzeichen am Ende auf.

colspan

Gibt die Anzahl der Spalten im Raster an, das vom Element eingenommen wird. Dieses Argument ist optional; wenn nichts angegeben wird, weist es den Standardwert „eins“ auf. Wenn es ausgelassen wird, wird davon ausgegangen, dass das Element eine Spalte des Rasters einnimmt. Dies beeinflusst das Verhalten der Pfeiltasten. Das *colspan*-Argument kann ausgelassen werden, auch wenn das *lastelement*-Argument angegeben ist.

lastelement

Dieser boolesche Wert gibt an, ob das Element, für das eine ID generiert wird, das letzte in der Zeile ist. Wenn dieses Argument ausgelassen wird, wird davon ausgegangen, dass auf dieses Element weitere folgen. Dies beeinflusst das Verhalten der Pfeiltasten.

detailNextLinkID()

Diese Funktion gibt eine Zeichenfolge mit folgender Form zurück:

```
" ID=dflnk_nn_nn TABINDEX=0 onFocus=func onBlur=func"
```

Das Einfügen dieser Zeichenfolge in ein HTML-Element, das ein Verbindungselement definiert, führt dazu, dass das Element die Konventionen der mausfreien CA SDM-Navigation befolgt, einschließlich der Erreichbarkeit mit der Pfeiltaste nach oben vom Grundelement und dem Ändern der Farbe in hellgelb, wenn es fokussiert wird. Die zurückgegebene Zeichenfolge beginnt mit einem Leerzeichen und weist kein Leerzeichen am Ende auf.

Diese Funktion verwendet keine Argumente.

detailReportValidation(field, has_error, emsg)

Diese Funktion gibt das Ergebnis der externen Feldüberprüfung in einem Bericht aus. Wenn in dem Bericht angegeben ist, dass die Überprüfung fehlgeschlagen ist, wird das Feld mit einer dicken roten Umrandung und eine Fehlermeldung mit einer gelben Umrandung oben im Formular angezeigt. Der Benutzer darf den Datensatz erst speichern, wenn ein nachfolgender Aufruf für detailReportValidation() das Feld als fehlerfrei berichtet.

Die detailReportValidation()-Funktion ist nur für Felder funktional, die für die browserseitige Überprüfung registriert sind. Alle Felder, die mit Detailformular-Makros erstellt werden, sind automatisch für Überprüfungen registriert. Sie können andere Felder mit detailSetValidateFunction() registrieren.

field

(Erforderlich) Gibt das Formularelementobjekt an, das das Feld enthält. Der einfachste Weg, dieses Element abzurufen, besteht darin, dieses Argument an den Ereignishandler zu übergeben, der die Überprüfung ausführt. Eine andere Möglichkeit besteht darin, die standardmäßige JavaScript-Funktion document.getElementById() zu verwenden.

has_error

(Erforderlich) Ein boolescher Wert oder eine Ganzzahl, der/die angibt, ob das Feld fehlerhaft ist. Das Einstellen eines Feldes als fehlerhaft bewirkt, dass der Benutzer den Datensatz nicht speichern kann und dass das Feld mit einer dicken roten Umrandung hervorgehoben wird. Darüber hinaus wird die entsprechende Fehlermeldung als drittes Argument mit einer gelben Umrandung oben im Formular angezeigt. Das Einstellen eines Feldes als nicht fehlerhaft kehrt diese Änderungen um.

emsg

Eine Textzeichenfolge, welche die anzuzeigende Meldung mit einer gelben Umrandung oben im Detailformular anzeigt, wenn das Kennzeichen *has_Fehler* eingestellt ist. Dieses Argument ist erforderlich, wenn *has_error* eingestellt ist.

detailSetValidate(hdrtext, is_required, maxsize)

Diese Funktion gibt an, dass das Feld, das zuletzt mit einer von detailNextID() bereitgestellten ID erstellt wurde, der browserseitigen Überprüfung unterliegt. Die Überprüfung für erforderliche Felder und für Felder mit einer maximalen Größe erfolgt automatisch. Andere Formen der Überprüfung können durch JavaScript-Funktionen oder Ereignisbehandlungsroutinen bereitgestellt werden, welche detailReportValidation() aufrufen.

Sie sollten detailSetValidate() nur für Formularfelder aufrufen, die Sie selbst definiert haben und deren ID von detailNextID() erstellt wurde. Die detailSetValidate()-Funktion muss aufgerufen werden, direkt nachdem Sie ein Feld erstellt haben, das Sie überprüfen möchten. Es ist unnötig (und führt zu unerwarteten Ergebnissen), die Funktion detailSetValidate() für Felder aufzurufen, die von Detailformular-Makros erstellt wurden.

hdrtext

(Erforderlich) Gibt eine Zeichenfolge an, die für die Identifizierung von Feldern in Fehlermeldungen verwendet wird.

is_required

(Erforderlich) Ein boolescher Wert oder eine Ganzzahl, der/die angibt, ob das Feld erforderlich ist. CA SDM überprüft automatisch, dass alle erforderlichen Felder angegeben sind, wenn der Benutzer versucht, einen Datensatz zu speichern.

maxsize

Eine Ganzzahl, welche die maximale Länge der Daten angibt, die für das Feld zulässig sind. CA SDM überprüft automatisch, dass alle Felder mit einem Wert für *maxsize* eine Länge innerhalb von Grenzen aufweisen, wenn der Benutzer versucht, einen Datensatz zu speichern. Dieses Argument ist erforderlich. Um die *maxsize*-Überprüfung zu unterdrücken, geben Sie den Wert 0 an.

detailRowHdr(hdrtext, colspan, is_required)

Diese Funktion speichert Text für das Headerelement (TH) eines Elements im Raster. Der Text wird erst in das Formular geschrieben, wenn eine detailWriteRow ()-Funktion oder ein dtlStartRow-Makro aufgerufen wird.

hdrtext

Gibt den Text im Headerelement an. Dieses Argument ist erforderlich.

colspan

Gibt die Anzahl der Spalten im Raster an, das vom Element eingenommen wird. Dieses Argument ist optional; wenn nichts angegeben wird, weist es den Standardwert „eins“ auf. Wenn es ausgelassen wird, wird davon ausgegangen, dass das Element eine Spalte des Rasters einnimmt. Dies beeinflusst das Verhalten der Pfeiltasten. Das *colspan*-Argument muss angegeben werden, wenn das *is_required*-Argument angegeben ist.

is_required

Gibt an, ob *hdrtext* in dem Stil angezeigt werden soll, der einem erforderlichen Feld entspricht. Bei dem Argument kann es sich um einen booleschen Wert, eine Zahl oder eine Zeichenfolge handeln. Eine Zahl oder Zeichenfolge gilt als falsch, wenn sie Null lautet und andernfalls als wahr. Dieses Argument ist optional. Wenn es ausgelassen wird, ist *hdrtext* als nicht erforderliches Feld eingestellt.

detailSetRowData(text)

Diese Funktion speichert HTML-Text für das Datenelement (TD) eines Elements im Raster. Der Text wird erst in das Formular geschrieben, wenn eine *detailWriteRow()*-Funktion oder ein *dtlStartRow*-Makro aufgerufen wird. Das einzige Argument ist der HTML-Text des zu speichernden Elements.

detailWriteRow()

Diese Funktion schreibt den HTML-Text, der für die aktuelle Zeile gespeichert wird. Dadurch werden zwei HTML-Tabellenzeilen erstellt, eine für die Headerelemente (TH) und eine für die Datenelemente (TD). Die Funktion schreibt auch das *<td>*-Tag, das ein neues Datenelement beginnt. Das TD-Tag wird automatisch vom *dtlStartRow*-Makro geschlossen. Deshalb ist es unnötig (und falsch), die *<td>*-Tags in dem HTML-Text anzugeben, der auf *detailWriteRow()* folgt. Diese Funktion verwendet keine Argumente.

Verstehen von Listenformularen

Im Folgenden sind Hintergrundinformationen zu den internen Daten von CA SDM-Listenformularen angegeben. Es wird empfohlen, zum Ändern dieser Formulare die Web Screen Painter-Designansicht zu verwenden.

CA SDM-Listenformulare sind mit den folgenden Makros definiert (das mit dem *PDM_MACRO*-Tag aufgerufen wird):

IsStart

Beginnt eine Liste

IsCol

Definiert eine Spalte in einer Liste

lsWrite

Fügt Text in den "pdm_list"-Teil einer Liste ein

lsEnd

Beendet eine Liste

Die allgemeine Form einer Liste, die diese Makros verwendet, lautet:

```
<pdm_macro name=lsStart>
<pdm_macro name=lsCol hdr=hdr1 attr=attr1>
<pdm_macro name=lsCol hdr=hdr1 attr=attr1>
<pdm_macro name=lsEnd>
```

Der erhaltene Text gleicht dem folgenden Beispiel in der HTML-Ausgabe:

```
var rs = new Resultset();           From lsStart
rs.startList(); From lsStart
rs.header("hdr1"); From lsCol
rs.setData("attr1","options"); From lsCol
rs.header("hdr2"); From lsCol
rs.setData("attr2","options"); From lsCol
<PDM_LIST SOURCE=list> From lsEnd
rs.data(attr1) From lsCol/lsEnd
rs.data(attr2) From lsCol/lsEnd
</PDM_LIST> From lsEnd
```

Hinweis: Die Ausgabeliste ist in zwei getrennte Abschnitte unterteilt: den Setup-Abschnitt vor dem <PDM_LIST>-Tag, und die Liste selbst zwischen den Tags <PDM_LIST> und </PDM_LIST>. Das lsCol-Makro verwendet Vorverarbeitungsvariablen und das <PDM_SET>-Tag, um Daten in beide Listenabschnitte auszugeben. Der gesamte Listenabschnitt der Liste wird von einem <PDM_EVAL>-Tag erstellt, das vom lsEnd-Makro generiert wird.

Um Ihr eigenes JavaScript in den Setup-Abschnitt der Liste einzufügen, fügen Sie es einfach an der Stelle hinzu, an der es gebraucht wird. Verwenden Sie das "lsWrite"-Makro, um Ihren eigenen Code in den Listenabschnitt der Liste einzufügen.

lsWrite-Makro

Das lsWrite-Makro gibt Text für den Listenabschnitt einer Liste an (der Teil zwischen den Tags <pdm_list> und </pdm_list>). Text, der für das Textargument dieses Makros angegeben ist, wird verzögert und erst mit dem lsEnd-Makro in den ausgegebenen HTML-Text geschrieben.

lsWrite [both=no|yes]

text="xxx"

beide

Gibt an, dass der Textoperand sofort in den ausgegebenen HTML-Text und in den verzögerten Textpuffer geschrieben werden soll. Für die Ausgabe von JavaScript kann es nützlich sein, die Ausgabe von Setup- und von Listeninformationen durch ein nachfolgendes IsCol-Makro zu umgehen. Optional; Standardwerte ist „Nein“.

text

Gibt den Text an, der von diesem Makro generiert wird. Der angegebene Text wird bis zum IsEnd-Makro verzögert.

Es ist häufig wünschenswert, pdm-Tags und Referenzen auf Formularvariablen mit Hilfe eines IsWrite-Makros in die Textausgabe einzuschließen. Damit sie nicht vom Webmodul während des Analysierens des IsWrite-Makros interpretiert werden, befolgen Sie die folgenden Syntaxregeln:

- Wenn das IsWrite-Makro ein pdm-Tag generiert, lassen Sie der umgebenden Trennzeichen „<“ und „>“ des Tags aus. Um zum Beispiel eine <pdm_else>-Anweisung in den Listenabschnitt der Liste einzufügen, verwenden Sie folgenden Code:

```
<PDM_MACRO NAME=IsWrite text="pdm_else">
```

Das Webmodul fügt automatisch das „<“ und „>“ ein, bevor der Text erstellt wird, wenn es feststellt, dass die ersten vier Zeichen „pdm_“ (oder „PDM_“) lauten.

- Wenn das IsWrite-Makro einen Verweis auf eine Formularvariable generiert, codieren Sie ein @-Zeichen anstelle eines \$-Zeichens, das die Variable bestimmt. Um z. B. einen Verweis auf die Listenvariable \$list.persistent_id zu generieren, verwenden Sie folgenden Code:

```
<PDM_MACRO NAME=IsWrite text="@list.persistent_id">
```

Das Webmodul konvertiert automatisch „@“ zu „\$“, bevor der Text erstellt wird. Damit tatsächlich ein @-Zeichen erstellt wird, stellen Sie ein Backslash-Zeichen voran.

Anpassen der Funktion "In Liste bearbeiten"

Zahlreiche Listenformulare wie die Fenster "Anfrageliste" und "Issue-Liste" verfügen über die Schaltfläche "In Liste bearbeiten". Wenn diese Schaltfläche zur Verfügung steht und ein Ergebnissatz angezeigt wird, kann der Benutzer auf die Schaltfläche „In Liste bearbeiten“ klicken, um den Suchfilter durch ein kleines Bearbeitungsformular zu ersetzen. Mit Hilfe des Bearbeitungsformulars können Benutzer Datensätze direkt im Listenformular aktualisieren. Der Benutzer kann sogar alles aktualisieren, was in der Liste ausgewählt ist, indem er die gewünschten neuen Daten in das Bearbeitungsformular einfügt und auf die Schaltfläche „Alle ändern“ klickt.

Beim Bearbeiten von Listendaten wird erst dann mit dem Server kommuniziert, wenn der Benutzer auf „Speichern“ klickt. Wenn der Benutzer auf "Speichern" klickt, werden alle Aktualisierungen (im Formular gelb markiert) an den Server gesendet, der alle Änderungen in einem Vorgang anwendet, eine Statusmeldung ausgibt und die Liste erneut anzeigt.

Sie können diese Funktion anpassen, indem Sie angeben, ob die Schaltfläche „In Liste bearbeiten“ in einem bestimmten Formular verfügbar ist, und indem Sie angeben, welche Felder im Bearbeitungsformular angezeigt werden sollen, wenn der Benutzer auf die Schaltfläche „In Liste bearbeiten“ klickt.

Um die Schaltfläche „In Liste bearbeiten“ in einem Listenformular einzufügen, geben Sie die folgende Anweisung irgendwo im <HEAD>-Abschnitt des Formulars ein:

```
<SCRIPT LANGUAGE="JavaScript" SRC=$CAisd/CAisd/list_edit.js></SCRIPT>
```

Durch das einfache Hinzufügen dieser Anweisung wird die Schaltfläche im Formular eingefügt. Diese Schaltfläche ist jedoch solange deaktiviert, bis JavaScript-Anweisungen, die den Inhalt des Bearbeitungsformulars angeben, ebenfalls in das Formular eingeschlossen werden. Diese Anweisungen müssen direkt vor den Spezifikationen für den Ergebnissatz platziert werden und weisen folgendes Format auf:

Anweisungen	Kommentare
<code>startListEdit(_search_filter);</code>	Geben Sie die Anweisung genau so an, wie gezeigt
<code>listEditStartRow();</code>	Geben Sie die Anweisung genau so an, wie gezeigt
<code>listEditField("attr[, "hdr"]);</code>	Geben Sie keinen oder mehrere an
<code>listEditReadonly("attr[, "hdr"]);</code>	Geben Sie keinen oder mehrere an
<code>endListEdit();</code>	Geben Sie die Anweisung genau so an, wie gezeigt

Auf die `endListEdit()`-Anweisung muss die `ResultSet()`-Anweisung folgen, die den Ergebnissatz beginnt. Sie geben die Felder und deren Reihenfolge im Bearbeitungsformular an, indem Sie eine oder mehrere `listEditReadonly()`- oder `listEditField()`-Anweisungen codieren.

`startListEdit( _search_filter );`

Diese Anweisung beginnt das Listenbearbeitungsformular. Es muss genau so kodiert werden: `startListEdit( _search_filter );`.

listEditStartRow();

Diese Anweisung beginnt eine neue Zeile mit Feldern im Listenbearbeitungsformular. Es muss genau so kodiert werden: *listEditStartRow();*. Sie müssen die *listEditStartRow()*-Anweisung direkt nach der *startListEdit()*-Anweisung platzieren. Sie können optional zusätzliche *listEditStartRow()*-Anweisungen zwischen den *listEditField()*- und *listEditReadonly()*-Anweisungen einschließen, welche die Felder in dem Formular angeben.

listEditField(attr_name[,hdr]);

Diese Anweisung gibt ein Attribut an, das im Listenbearbeitungsformular einzuschließen ist.

attr_name

Gibt den Namen des Attributs an, das im Bearbeitungsformular einzuschließen ist (einschließlich Punkte, wenn erforderlich). Alle Attribute, die für ein Listenbearbeitungsformular angegeben sind, müssen im Ergebnissatz verfügbar sein. Der angegebene "*attr_name*" muss mit dem in "*rs.showData()*" oder "*rs.showDataWithLink()*" angegebenen Namen identisch sein, womit das Attribut zum Ergebnissatz hinzugefügt wird.

Das Attribut wird auf dem Bearbeitungsformular im gleichen Format angezeigt wie im Suchfilter. Wenn sich das Attribut nicht im Suchfilter befindet, wird es in einem Textfeld mit 20 Zeichen bearbeitet.

attr_name ist ein erforderliches Argument.

hdr

Gibt den Text des Headers für das Feld im Bearbeitungsformular an. Dieses Argument ist optional. Wenn es ausgelassen wird, wird der Headertext aus dem Suchfilter verwendet. Wenn "*hdr*" ausgelassen wird und das Attribut nicht im Suchfiltereintrag für "*attr_name*" enthalten ist, wird im Kopfzeilentext standardmäßig der Attributnamen, eingeschlossen in Fragezeichen, übernommen.

listEditReadonly(attr_name[,hdr]);

Diese Anweisung gibt ein nicht bearbeitbares Attribut an, das im Listenbearbeitungsformular einzuschließen ist. Seine Argumente haben dieselbe Bedeutung wie die für *listEditField()*.

endListEdit();

Diese Anweisung beendet das Listenbearbeitungsformular. Es muss genau so kodiert werden: *endListEdit();*.

Integrieren mit Ihren eigenen Webseiten

Sie können die Funktionalität der CA SDM-Web-Schnittstelle in Ihre eigenen Webseiten integrieren, um eine nahtlose Schnittstelle für Ihre Anwender bereitzustellen.

Hinweis: Die Web-Engine ist die ausführbare Datei, die als Gateway zwischen dem Webserver und dem CA SDM-Server fungiert. Sie ermöglicht mehrere gleichzeitige Verbindungen von einem bestimmten Anwender. Dabei können mehrere Frames gleichzeitig über eine offene Verbindung zum CA SDM-Webmodul-Prozess verfügen.

Sie können die Web-Schnittstellen folgendermaßen integrieren:

- Indem Sie Verknüpfungen von einer beliebigen Webseite zur entsprechenden CA SDM-Webseite erstellen, ohne die Menüseite der Web-Schnittstelle zu durchlaufen.
- Indem Sie HTML-Formulare zu Ihren Webseiten hinzufügen, die Eingaben sammeln und unterstützte Vorgänge direkt ausführen, ohne eine CA SDM-Webseite zur Eingabe von Daten anzuzeigen.
- Indem Sie Webformulargruppen erstellen, die verwendet werden können, um Anwendern HTML-webbasierte Formulare über ihren Zugriffstyp zuzuordnen. Webformulargruppen können ähnlich den Formulargruppen der Verwaltungsschnittstelle zum Anpassen Ihrer HTML-Seiten verwendet werden.

Weitere Informationen:

[Unterstützte Servervorgänge](#) (siehe Seite 469)

Verknüpfen mit CA SDM-Funktionen

Sie können direkte Verknüpfungen zu wichtigen CA SDM-Funktionen erstellen, ohne die Hauptseite anzuzeigen. Normalerweise greifen Sie hierfür auf das Popupfenster für das neue Fenster zu, welches die CA SDM-Informationen enthält. Sie können aber auch Ihre Webseite durch die CA SDM-Seite ersetzen.

In beiden Fällen zeigt das Produkt die angeforderte Seite auf dieselbe Weise an, wie sie auch der Benutzer in einer normalen Sitzung sieht, jedoch ohne Hauptseite und Scoreboard. Analysten zeigen die Hauptseite und das Scoreboard durch Auswahl der Option "Scoreboard wiederherstellen" im Menü "Datei" an. Diese ist nur auf Seiten verfügbar, die durch Umgehen der Hauptseite angezeigt werden.

Um eine Verbindung zu erstellen, welche die Hauptseite umgeht, geben Sie eine URL im folgenden Format an:

```
http://hostname[:port]/CAisd/pdmweb.exe?OP=operation+var=value+...
```

In dieser Beispiel-URL steht *hostname* für den Hostrechner des Webserver, *port* für die Portnummer (normalerweise 8080), die nur bei Verwendung von Tomcat als HTTP-Server erforderlich ist, *operation* für eine der unterstützten Operationen und *var=value* für eine oder mehrere Variablen, die für den Vorgang zulässig sind.

So kann z. B. eine Verknüpfung, die das Formular zum Erstellen einer neuen Anforderung lädt, folgendermaßen angegeben werden:

```
<A  
HREF=http://hostname/CAisd/pdmweb.exe?OP=CREATE_NEW+FACTORY=cr>Anfragedefinitio  
n</A>
```

Weitere Informationen:

[Verknüpfungen – Beispiele](#) (siehe Seite 477)

Senden von Formularen an CA SDM

Sie können auch auf CA SDM-Funktionen zugreifen, indem Sie Ihren Webseiten HTML-Formulare hinzufügen, die auf unterstützte Vorgänge verweisen. Wenn das Formular mit genug Informationen eingereicht werden, um einen Vorgang wie das Erstellen einer Anfrage auszuführen, wird der Vorgang ohne Anzeige eines Formulars zum Eingeben von zusätzlichen Informationen ausgeführt.

Wenn Sie zu Ihrer Webseite ein HTML-Formular hinzufügen:

- Die AKTION des Formulars entspricht dem URL für "pdmweb.exe".
- Die METHODE lautet SENDEN.
- Entweder sollte der Name der Schaltfläche „Absenden“ einem der unterstützten Vorgänge entsprechen, oder es sollte ein ausgeblendetes Feld mit der Bezeichnung „OP“ verfügbar sein, dessen Wert einem der unterstützten Vorgänge entspricht.

Um z. B. ein HTML-Formular zu erstellen, das die Seite zum Erstellen einer neuen Anfrage lädt, geben Sie folgenden Code an:

```
<FORM ACTION=/CAisdCAisd/pdmweb.exe METHOD=POST>  
<INPUT type=HIDDEN NAME=FACTORY VALUE=iss>  
.  
.  
.  
<INPUT type=SUBMIT NAME=CREATE_NEW VALUE=" OK ">  
</FORM>
```

Anpassen von JavaScript

Die CA SDM-Web-Schnittstelle verwendet sehr viel JavaScript und fügt eine Reihe von JavaScript-Dateien in das Verzeichnis `"/CAisd/scripts"` ein. Wenn Sie eine dieser Skriptdateien anpassen möchten, speichern Sie die geänderte Version im Verzeichnis `"/CAisd/sitemods/scripts"`, wie bereits unter [Vom HTTP-Server verwendete Verzeichnisse](#) (siehe Seite 486) beschrieben.

Aus Gründen einer besseren Leistungsstärke werden die JavaScript-Dateien im Verzeichnis `"/CAisd/scripts"` komprimiert, wobei Kommentare und unnötige Leerzeichen entfernt werden. Komprimierte Dateien sind schwieriger zu lesen. Die nicht komprimierten Versionen von allen JavaScript-Dateien können Sie in einem der folgenden Verzeichnisse finden:

- (UNIX) `$NX_ROOT/sdk/scripts`
- (Windows) `$NX_ROOT/sdk/scripts`

Vermeiden Sie, sofern dies möglich ist, angepasste Versionen von ganzen JavaScript-Dateien zu erstellen. Jede Datei enthält eine Reihe von Funktionen, von denen Sie möglicherweise nur eine ändern möchten. In den meisten Fällen können Sie einzelne Funktionen überschreiben, indem Sie eine geänderte Funktion in die JavaScript-Datei `"sitemods.js"` einfügen. Dieser Ansatz wird zum Ändern von JavaScript dringend empfohlen.

sitemods.js

Eine Skeleton-Datei *sitemods.js* gehört zum Lieferumfang von CA SDM. Alle verteilten HTML-Dateien schließen diese Datei am Ende ihres `<head>`-Abschnitts ein, so dass sie zur letzten geladenen Datei wird. Da es sich um die letzte Datei handelt, überschreiben alle darin definierten Funktionen vorher unter dem gleichen Namen eingeschlossene Funktionen. Damit können Sie Ihre Version einer verteilten JavaScript-Funktion bereitstellen, ohne den verteilten Code direkt zu ändern.

Dieser Ansatz ist für Funktionen, die während des Ladens in den `<head>`-Abschnitt aufgerufen werden, nicht effektiv (z. B. für Funktionen in `"menubar.js"` und `"ahdmenus.js"`).

Die meisten JavaScript-Funktionen können Sie jedoch mit folgenden Schritte anpassen:

1. Fügen Sie eine geänderte Version der Funktion in `"sitemods.js"` ein.
2. Speichern Sie die aktualisierte Kopie von `"sitemods.js"` im Verzeichnis `"/CAisd/site/mods/www/wwwroot/scripts"`.

Weitere Informationen:

[Ändern der Menüleisten](#) (siehe Seite 417)

Ändern von Kontextmenüs

Zahlreiche Formulare in CA SDM verwenden Kontextmenüs, die durch Klick mit der rechten Maustaste auf ein Objekt aufgerufen werden. Mit Hilfe von Web Screen Painter können Sie Kontextmenüs ändern, indem Sie enthaltene Optionen entfernen oder modifizieren bzw. neue hinzufügen.

Hinweis: Weitere Informationen über das Hinzufügen von Menüoptionen finden Sie in der *Hilfe zu Web Screen Painter*.

Aktualisieren und Erstellen von Changes als Mitarbeiterbenutzer

Standardmäßig kann ein Benutzer die Changes nur über die Web-Schnittstelle für Mitarbeiter anzeigen. Führen Sie die folgenden Schritte aus, um das Erstellen und Aktualisieren von Changes durch Mitarbeiter zu aktivieren:

1. Melden Sie sich bei der Web-Schnittstelle als Administrator an, und wählen Sie die Registerkarte "Administration".
2. Wählen Sie aus dem Menü „Sicherheit“ die Option „Zugriffstyp“ aus.
Die Liste der Zugriffstypen wird angezeigt.
3. Klicken Sie auf die Verknüpfung für den Mitarbeiter, um das Fenster "Zugriffstyp – Detail" für den Mitarbeiter anzuzeigen.
4. Legen Sie in der Registerkarte "Funktionszugriff" für Changes "modify" fest, und speichern Sie.
5. Klicken Sie auf die Schaltfläche „Zurück“, um zur Registerkarte „Administration“ zurückzukehren, und wählen Sie dann „Datenaufteilungen“, „Datenaufteilung – Liste“ aus.
6. Klicken Sie auf "Mitarbeiter", um das Fenster "Datenaufteilung – Detail" anzuzeigen. Suchen Sie im Fensterbereich "Einschränkungen - Liste" in der Spalte "Typ" nach den folgenden Change_Request-Tabellen:
 - Vor-Aktualisierung
 - Erstellen
7. Klicken Sie für jede Tabelle, die Sie bearbeiten möchten, auf den Tabellennamen, um das Fenster "Datenpartitionseinschränkung - Detail" der Tabelle anzuzeigen.
8. Klicken Sie auf die Schaltfläche "Bearbeiten".
9. Bearbeiten Sie die Bedingungen folgendermaßen:
Ändern Sie "id = 1" in "affected_contact = @root.id".
10. Klicken Sie auf "Speichern".

Wenn Sie sich jetzt als Mitarbeiter an der Web-Schnittstelle anmelden, wird die Verknüpfung "Change erstellen" angezeigt.

Hinzufügen einer Verknüpfung "Geschlossene Changes" im Mitarbeiter-Scoreboard

Sie können das Produkt verwenden, um dem Mitarbeiter-Scoreboard der Web-Schnittstelle eine Option für den Knoten "Geschlossene Changes" hinzuzufügen.

So fügen Sie einen Knoten "Geschlossene Changes" hinzu

1. Melden Sie sich bei dem Produkt als Administrator an.
2. Klicken Sie auf die Registerkarte "Service Desk".
3. Wählen Sie "Datei", "Scoreboard anpassen".
Das Dialogfeld "Scoreboard anpassen" wird angezeigt.
4. Klicken Sie auf die Option "Rolle", und wählen Sie "Mitarbeiter" in der Dropdown-Liste aus.
5. Klicken Sie unter "Neuen Knoten hinzufügen" auf die Verknüpfung "Gespeicherte Abfrage" des Knotens.
Das Dialogfeld "Gespeicherte Abfragen - Liste" wird angezeigt.
6. Suchen Sie in der Liste der gespeicherten Abfragen nach geschlossenen Changes, und wählen Sie sie aus. Dies wird in der Regel als Code "CHGUBIN7" angezeigt.
7. Um einen Speicherort für den neuen Knoten anzugeben, wählen Sie ein Element in der Scoreboard-Baumstruktur auf der linken Seite aus.
8. Klicken Sie auf "Neuen Knoten hinzufügen".
Der neue Knoten mit dem Namen "Geschlossene Changes" wird in die Scoreboard-Baumstruktur eingefügt.
9. Klicken Sie auf "Fertig".

Herunterladen von Anhängen

Wenn Sie einen Anhang in CA SDM herunterladen, wird der Anhang automatisch im Browserfenster angezeigt, ohne eine Aufforderung von Ihnen abzuwarten. Diese Aktion kann gefährlich sein, wenn der Anhang einen Virus enthält.

Sie haben in CA SDM die Möglichkeit, das Anzeigen des Dialogfelds "Speichern unter" zu erzwingen, mit dem Sie zu einer Eingabe aufgefordert werden, ob Sie den Anhang auf der Festplatte speichern oder öffnen möchten. Das Speichern eines Anhangs kann eine sichere Methode sein, da Sie den Anhang auf der Festplatte speichern und scannen können, bevor Sie ihn tatsächlich öffnen. Sie haben auch die Möglichkeit, die Anzeige des Dialogfelds „Speichern unter“ nur für bestimmte Typen von Anhängen zu erzwingen.

Sie können die Anzeige des Dialogfelds "Speichern unter" über die Servlet-Konfigurationsdatei "web.xml" erzwingen. Die Datei "web.xml" kann unter den folgenden Pfaden gefunden werden:

Windows: \$NX_Root\bopcfg\www\CATALINA_BASE\webapps\CAisd\WEB-INF\web.xml

Linux: \$NX_ROOT ist "/opt/CAisd"

Kapitel 9: Anpassung der Event-Protokoll-Datenspeicherung

Die Systemumgebungsvariable "`@NX_EVENT_LOG_EXCLUDE`", die in der Datei "`NX.env`" festgelegt wird und einen Neustart der CA SDM-Services erfordert, ermöglicht die Steuerung der im Event-Protokoll gespeicherten Datenmengen ("event_log"-Tabelle). Diese Variable lässt Sie nur die Events speichern, die Sie verfolgen und über die Sie berichten möchten, bzw. die Sie als Teil von "Letzte Aktivität" verwenden möchten. Diese kann über eine Schaltfläche von der Seite "Ad-hoc-Profil" aus gestartet werden.

In dieser Variablen sind Listenelemente durch Kommata getrennt (z. B. `@NX_EVENT_LOG_EXCLUDE = FAQ,KD_OPEN`). Wenn Sie z. B. die "LOGIN,LOGOUT"-Events aus der folgenden Tabelle verwenden möchten (Wert "`@NX_EVENT_LOG_EXCLUDE`" für "LOGIN,LOGOUT"), zeichnet das Produkt keine An- und Abmeldungs-Events auf.

Richten Sie sich nach den folgenden Informationen, wenn Sie Daten für die Speicherung im Event-Protokoll mithilfe dieser Variablen anpassen:

Event	Aufzählung	Von	Sätze	Kommentare
LOGIN	1	CA SDM		Gibt an, dass der Anwender sich beim System anmeldet.
LOGOUT	2	CA SDM	numdata1	Gibt an, dass sich der Anwender abmeldet, wobei numdata1=Abmeldegrund: 0 -normal 1 -Zeitlimit 2 -nicht normal
CR_CREATE	3	CA SDM	sd_obj_type, sd_obj_id, kd, numdata1	Gibt an, dass der Anwender einen Request erstellt, wobei numdata1=ID des betroffenen Endanwenders.
ISS_CREATE	4	CA SDM	sd_obj_type, sd_obj_id, kd, numdata1	Gibt an, dass der Anwender einen Change erstellt, wobei numdata1=ID des betroffenen Endanwenders.
CHG_CREATE	5	CA SDM	sd_obj_type, sd_obj_id, kd, numdata1	Gibt an, dass der Anwender einen Issue erstellt, wobei numdata1=ID des betroffenen Endanwenders.

Event	Aufzählung	Von	Sätze	Kommentare
EMAIL	6	Knowledge Management	kd	Gibt an, dass der Analytiker ein Dokument per E-Mail versendet.
LINK	7	Knowledge Management	kd, sd_obj_type, sd_obj_id	Gibt an, dass der Anwender eine Lösung übernimmt und sie mit einem Ticket verknüpft.
UNLINK	8	CA SDM	sd_id, sd_obj_type, sd_obj_id	Gibt an, dass der Anwender die Verknüpfung zwischen einer Lösung und einem Ticket aufhebt.
SEARCH	9	Knowledge Management	numdata1,	Gibt an, dass der Anwender Knowledge-Dokumente durchsucht, wobei numdata1= CI_ASKED_QUES ID.
FAQ	10	Knowledge Management	numdata1	Gibt an, dass die FAQs durchsucht werden, wobei numdata1= O_INDEXES ID (Kategorie).
DT_NAVIGATE	11	Knowledge Management	kd, numdata1, textdata1	Gibt an, dass der Anwender durch eine Entscheidungsbaumstruktur navigiert, wobei numdata1= ES_NODES ID textdata1=Pfad.
KD_BOOKMARK	12	Knowledge Management	kd	Gibt an, dass der Anwender ein Lesezeichen für ein KD anlegt.
KD_COMMENT	13	Knowledge Management	kd, numdata1	Gibt an, dass der Anwender einem KD einen Kommentar hinzufügt, wobei numdata1= O_COMMENTS ID.
KD_CREATE	14	Knowledge Management	sd_obj_type, sd_obj_id, kd	Gibt an, dass ein Anwender ein Dokument erstellt. CA SDM-IDs werden verwendet, wenn ein KD mit der Knowledge-Sendefunktion von einem Request oder Issue aus erstellt wird.
KD_OPEN	15	Knowledge Management	kd, numdata1	Gibt an, dass ein Anwender ein KD öffnet, wobei numdata1=BU_TRANS ID.
KD_RATE	16	Knowledge Management		Gibt an, dass ein Anwender ein KD bewertet, wobei numdata1=BU_TRANS ID.

Event	Aufzählung	Von	Sätze	Kommentare
KD_NEW	17	Knowledge Management	numdata1	Gibt an, dass ein Anwender auf der Registerkarte "Knowledge" auf den Ordner "Neue Dokumente" klickt.
NX_ATTACH_AUDIT_TO_NEW_TICKET	18	CA SDM		Wenn ein Anwender ein neues Ticket öffnet, werden alle Events für die gegenwärtige Sitzung standardmäßig auf der Registerkarte "Event-Protokoll" des Tickets angezeigt. 0 - Nur für das Ticket relevante Events werden auf der Registerkarte "Event-Protokoll" angezeigt. 1-Alle Events für die gegenwärtige Sitzung werden auf der Registerkarte "Event-Protokoll" des Tickets angezeigt
TICK_OPEN	19	CA SDM		Gibt an, dass das Ticket angezeigt wurde.
TICK_SEARCH	20	CA SDM		Gibt an, dass der Anwender nach Tickets gesucht hat, und verknüpft die Anzahl der Suchen.
KD_PRNT	21	Knowledge Management	kd	Gibt an, dass das Knowledge-Dokument gedruckt wurde.

Anpassen von CA Business Intelligence-Berichten

Sie können CA Business Intelligence-Berichte anpassen, nachdem Felder und Tabellen im CA SDM-Schema definiert wurden.

Hinweis: Information zum Durchführen von Schemaänderungen finden Sie in der Schemadesigner-Änderungsübersicht.

Bevor Sie anfangen, überprüfen Sie, dass Sie folgende Schritte ausgeführt haben:

- CA Business Intelligence wurde installiert und für einen korrekten Betrieb zusammen mit CA SDM konfiguriert.
- Anwenderberechtigungen, Rollen, Authentifizierungsoptionen und Datenpartitionssicherheit wurden für die Berichterstellungsumgebung eingerichtet.

Hinweis: Informationen zur Einrichtung der Sicherheitsoptionen für CA Business Intelligence finden Sie im *Administrationshandbuch*.

Infrastruktur von CA Business Intelligence

CA Business Intelligence (CA BI) ist eine Infrastruktur für Unternehmensberichte, die es Ihnen ermöglicht, Berichte für CA SDM-Benutzer und -Rollen zu erstellen, zu verwalten, zu speichern, zu planen und zu verteilen. BusinessObjects Enterprise XI Release 2 und die dazugehörigen Tools bilden zusammen mit BusinessObjects Crystal Reports XI das Rückgrat der Architektur. BusinessObjects Enterprise-Tools sind in einem in CA SDM erstellten Paket enthalten, in dem die grundlegenden Berichterstellungs-Tools von CA SDM in einem branchenführenden Business Intelligence-Rahmen zusammengeführt werden.

Hinweis: Crystal Reports ist als primäre Komponente von CA BI im Lieferumfang enthalten. Das Berichterstellungs- und -verwaltungstool Crystal Reports XI ist jedoch nicht enthalten. Crystal Reports XI ist ein getrennt lizenziertes Produkt, das von BusinessObjects erworben und zusammen mit CA BI verwendet werden kann.

Berichtskomponenten

Nachfolgend sind die wichtigsten, in der CA Business Intelligence-Infrastruktur enthaltenen Komponenten aufgeführt:

- **CA SDM Datenbank/Domsrvr/ODBC-Treiber** - Die Berichtsdaten werden in einer SQL Server- oder Oracle-CA SDM-Datenbank gespeichert. BusinessObjects-Berichtsanwendungen (Crystal Reports und Web Intelligence) greifen auf die Datenbank über einen ODBC-Treiber zu, der direkt mit der Objekt-Engine (domsrvr) von CA SDM verbunden ist. Alle CA SDM-Sicherheitseinstellungen, einschließlich derjenigen zu Datenpartition und Einschränkungen der Mandantenfähigkeit, werden automatisch auf Berichte angewendet.
- **Central Management Server** - Der zentrale Verwaltungsserver (Central Management Server, CMS) ist das zentrale Repository zur Speicherung aller Objekte, die in den einzelnen Berichterstellungsprozessen verwendet werden.

- **Central Management Console** - Die zentrale Verwaltungskonsole (Central Management Console, CMC) ist die Hauptverwaltungseinrichtung für BusinessObjects. Sie sorgt für den Zugriff auf alle BusinessObjects-Verwaltungsfunktionen. Mithilfe der CMC können Sie Berichte bereitstellen und Benutzerzugriff sowie Ordnerberechtigungen für InfoView zuweisen.
- **BusinessObjects-Universum** - Das Universum ist eine geschäftliche Darstellung eines Data Warehouse oder einer transaktionalen Datenbank. Es beschreibt die Klassen (Tabellen) und Objekte (Spalten), die in Berichten verwendet werden. CA SDM Universum wird während der Installation ebenfalls installiert und konfiguriert. Sobald die Installation abgeschlossen ist, wird die Universums-Verbindung verschiedenen Gruppen und Benutzern in CA SDM zugewiesen.
 - **Designer** - Der Designer ist ein Tool in BusinessObjects Enterprise, mit dem Sie das CA SDM-Universum ändern können, das eine Metaebene zwischen dem CA SDM-Schema und den BusinessObjects-Berichterstellungs-Tools bildet. Mit dem Import-/Exportassistenten können Sie Objekte in CMS einfügen oder daraus extrahieren.
- **Vordefinierte Standardberichte** - Vordefinierte Berichte sind webbasierte CA SDM- und Knowledge Management-Berichte, die entweder mit BusinessObjects Web Intelligence (WebI) oder mit Crystal Reports entwickelt wurden. Die Berichte können als Modelle zum Definieren standortspezifischer Berichte verwendet werden.
- **InfoView** - BusinessObjects InfoView ist eine Web-Schnittstelle, die es autorisierten CA SDM-Benutzern ermöglicht, durch Anzeige, Ausführung und Planung von Berichtstypen wie WebI und Crystal Reports mit webbasierten vordefinierten Berichten zu interagieren. Berichte werden im öffentlichen Abschnitt von InfoView in Ordnern gespeichert.
- **Ad-hoc-Berichte** - Ad-hoc-Berichte werden mit Hilfe einer plugin-basierten WebI-Schnittstelle in InfoView erstellt und verwaltet. Dieses Tool dient Benutzern, die problemlos einfache Berichte erstellen möchten, ohne Abfragen zu schreiben.

Entwicklungsumgebung

Das Aktualisieren der CA BI-Infrastruktur durch Schemaänderungen in CA SDM gehört zu den administrativen Funktionen. Ein Administrator, der ein geändertes Schema für Berichte höherstuft, muss die Umgebung getrennt von der Produktionsumgebung einrichten.

Einige von CA BI verwendete Tools benötigen eine Windows-basierte Architektur. Das bedeutet, dass für Linux/UNIX-Installationen CA BI auf einem Windows-Computer konfiguriert werden muss, um mit der CA BI-Installation in der Linux/UNIX-Produktionsumgebung zu interagieren. Wenn Sie Windows-Server in der Produktion verwenden, sollten Sie einen zusätzlichen Windows-Computer für Ihre Entwicklungsumgebung konfigurieren.

Tools

Das Aktualisieren der CA BI-Infrastruktur durch Schemaänderungen in CA SDM gehört zu den administrativen Funktionen. Um geänderte Schemaänderungen in die Berichte höherstufen zu können, benötigen Sie die folgenden Tools in Ihrer Entwicklungsumgebung:

BusinessObjects Designer

Dieses vollständige Client-Tool für Windows wird auf dem CA BI-Produktionsserver als Teil der grundlegenden CA BI-Installation für Windows installiert. Wenn es sich bei dem CA BI-Server um eine Nicht-Windows-Architektur handelt oder wenn kein Anmeldezugriff auf den CA BI-Produktions-Anwendungsserver gewünscht wird, müssen Sie eine getrennte CA BI-Installation auf einem Windows (Entwicklungs-)Server erstellen. Eine CA BI-Entwicklungsserverinstallation ermöglicht den Remotezugriff auf CA BI-Produktionsobjekte, unabhängig von der Architektur der CA BI-Produktionsserverinstallation.

BusinessObjects Web Intelligence

Dieses webbasierte Berichterstellungstool wird für die Änderung und Erstellung von Web Intelligence-Berichten (WebI) verwendet. Sie können auf das WebI-Tool über die BusinessObjects InfoView-Schnittstelle zugreifen. Administrative Berechtigungen für die WebI- und InfoView-Tools sind ebenfalls in CA BI verfügbar, vor allem, wenn das Tool BusinessObjects Central Management Console (CMC) verwendet wird.

ODBC-Treiber für CA SDM

Bei der CA BI-Installation wird der ODBC-Treiber für CA SDM bereitgestellt. Dank dieser Komponente können WebI und Crystal Reports bei gleichzeitiger Durchsetzung der Datenpartitionssicherheit auf CA SDM-Daten zugreifen. Der ODBC-Treiber wird als Teil der grundlegenden CA BI-Installation auf dem CA BI-Anwendungsserver installiert. Er ist auch als Client-Installation verfügbar und kann somit auf einem Computer, auf dem CA BI nicht ausgeführt wird, zusammen mit dem Crystal Reports XI-Client verwendet werden.

Hinweis: Informationen zum Definieren der Datenpartitionssicherheit für die Berichterstellungsumgebung finden Sie im *Administrationshandbuch*.

Erstellen einer Entwicklungsumgebung

Um eine Entwicklungsumgebung zu erstellen, gehen Sie folgendermaßen vor:

1. Stellen Sie einen Server mit einem unterstützten Windows-Betriebssystem bereit.
2. Installieren und konfigurieren Sie CA SDM.
3. Installieren und konfigurieren Sie CA Business Intelligence.
4. Ändern Sie den Standard-ODBC-Datenquellennamen von "casd_xxxxx" zu "casd_yyyyy", wobei "yyyyy" genau mit dem Datenquellennamen für die Produktionsimplementierung identisch ist.

Wichtig! Ungeachtet der eigentlichen Verbindungseigenschaften muss der Datenquellename in den Entwicklungs- und Produktionsimplementierungen identisch sein.

5. (Optional) Installieren und konfigurieren Sie Crystal Reports XI.

Hinweis: Crystal Reports muss nicht auf dem gleichen Computer wie CA BI installiert sein. Crystal Reports kann auf einem anderen Rechner installiert sein, vorausgesetzt, der ODBC-Treiber für CA SDM ist ebenfalls auf dem Crystal Reports-Rechner installiert, und der Datenquellename wird dahingehend geändert, dass er unabhängig von den eigentlichen Verbindungseigenschaften mit dem der Produktionsimplementierung identisch ist. Weitere Informationen über das Installieren einer einzelnen Kopie des ODBC-Treibers für CA SDM unabhängig von der CA BI-Installation finden Sie in der ODBC-Treiber-Dokumentation.

6. [Erstellen Sie den Rahmen](#) (siehe Seite 516).

Rahmen

Nachdem die Tools in der Entwicklungsumgebung verfügbar gemacht wurden, besteht der nächste Schritt im Erstellen eines Rahmens, mit dessen Hilfe Schemaänderungen bei Produktaktualisierungen beibehalten werden können.

Wichtig: Ändern Sie das mit CA BI installierte Standard-Entwicklungsuniversum für CA SDM nicht. Andernfalls können Ihre Schemaänderungen bei Patch- und Aktualisierungsprozessen überschrieben werden. Eine Änderung des CA SDM-Universums führt letztlich zum Verlust von Schemaänderungen in der CA BI-Infrastruktur.

Das BusinessObjects-Universum ist die Metaebene, die das Schema innerhalb der CA BI-Infrastruktur beschreibt. Statt das von CA bereitgestellte Universum zu ändern, können Sie ein kundenspezifisches Universum erstellen, das mit dem CA SDM-Universum verknüpft ist. Dieser Ansatz ermöglicht das Beibehalten lokaler Schemaänderungen mit nur minimalem Aufwand während des Aktualisierungsprozesses, und CA SDM kann das grundlegende Universum aktualisieren.

Mit der Universums-Dokumentation für BusinessObjects vertraute CA SDM-Kunden kennen weitere dokumentierte Verfahren von BusinessObjects, die es ermöglichen, Universen miteinander zu verbinden. Der hier beschriebene Prozess ist allerdings der einzige, der von CA zum Beibehalten von Kundenänderungen unterstützt wird.

Das Standard-Universum wird "CA SDM" genannt und ist im CA-Universenordner innerhalb der Central Management Console (CMC) gespeichert. Dieses Standard-Universum ist das "Kernel"-Universum in einer Struktur, in der Universen verknüpft sind.

Das CA SDM-Universum kann jeden beliebigen Namen erhalten. Der Name wird bei der Berichterstellung angezeigt. Stellen Sie also sicher, dass ein sinnvoller Name gewählt wird. Das benutzerdefinierte Universum ist das "abgeleitete" Universum in einer Struktur, in der Universen verknüpft sind.

Innerhalb dieses Systems können beliebig viele abgeleitete Universen verwaltet werden. Für die Beibehaltung von Schemaänderungen wird jedoch nur eines benötigt. Um die Wartung zu vereinfachen oder aus Gründen der Sicherheit können mehrere abgeleitete Universen verwendet werden. Solche Entscheidungen werden jedoch allein von Ihren Anfragen in Bezug auf den Produktionssupport bestimmt.

Stellen Sie in einer Umgebung mit mehreren abgeleiteten Universen sicher, dass folgende Punkte beachtet werden:

- Behalten Sie die "z_"-Namenskonvention für den Universumsdateinamen für alle Universen bei.
- Verwenden Sie die CA SDM-Verbindung, und speichern Sie dann das Universum im Ordner "CA Customer Universe" (Benutzerdefiniertes CA-Universum).
- Löschen Sie die Verknüpfung zum Kernel-Universum nicht.

Erstellen eines Frameworks zum Höherstufen von Schemaänderungen in CA BI

Verwenden Sie den BusinessObjects-Designer, um einen Framework zum Höherstufen von Schemaänderungen in CA Business Intelligence zu erstellen.

So erstellen Sie ein Framework zum Höherstufen von Schemaänderungen

1. Öffnen Sie den BusinessObjects Designer.
Wählen Sie im Menü "Designer" die Optionen "File" > "New" aus.
Das Fenster "Universe Parameters" wird angezeigt.
2. Klicken Sie auf die Registerkarte "Definition", und geben Sie im Feld "Name" einen aussagekräftigen Namen für dieses Universe ein.
3. (Optional) Geben Sie eine Beschreibung im Feld "Description" ein.

4. Wählen Sie in der Dropdown-Liste "Connection" die Option "CA SDM" aus.
5. Klicken Sie auf der Registerkarte "Verknüpfungen" auf die Schaltfläche "Verknüpfung hinzufügen".

Das Dialogfeld "Universe to Link" (Zu verknüpfendes Universum) wird angezeigt.

6. Erweitern Sie den Ordner "CA Universes", und führen Sie die folgenden Aufgaben aus:
 - a. Öffnen Sie die Datei "CA Service Desk.unv". Das Dialogfeld "Universe to Link" (Zu verknüpfendes Universum) wird geschlossen, und auf der Registerkarte "Links" (Verknüpfungen) wird das CA SDM-Universum angezeigt.
 - b. Klicken Sie auf "OK", um das Dialogfeld "Universe Parameters" (Universumsparameter) zu schließen.

Es dauert möglicherweise einige Minuten, bis Designer die Verknüpfung verarbeitet und das abgeleitete Universe erstellt.

7. Führen Sie nach dem Erstellen des abgeleiteten Universe die folgenden Aufgaben aus:
 - a. Ändern Sie die folgenden Parameter nach Bedarf.
 - Wählen Sie im Menü "File" die Option "Parameter" aus.
 - Klicken Sie auf die Registerkarte "Parameter".
 - Geben Sie für ANSI92 = JA an.
 - b. Klicken Sie auf die Registerkarte "Controls", und legen Sie in den folgenden Feldern einen für Ihre Implementierung geeigneten Wert fest. Klicken Sie dann auf "OK", um die Werte zu speichern und das Parameterdialogfeld zu schließen:
 - Limit size of result set
 - Limit execution time
 - Limit size of long text objects (minimum of 4000).
 - c. Definieren Sie Hierarchien. Beachten Sie, dass Kundenhierarchien nicht importiert werden.
 - Wählen Sie "Tools" > "Hierarchies" aus.
 - Wählen Sie in einer Mehrfachauswahl alle anwenderspezifischen Hierarchien aus, und klicken Sie dann auf die Pfeilschaltfläche zum Hinzufügen. Alle Hierarchien werden auf die rechte Seite verschoben.
8. Klicken Sie im Menü "Designer" auf "File" > "Save".

Das Dialogfeld "Speichern unter" wird angezeigt.
9. Wählen Sie im Feld "File Name" einen beliebigen beschreibenden Dateinamen aus, und stellen Sie dem Dateinamen "z_" voran. Beispiel: Ein Universe namens "ACME Anvil Co" kann den Standardnamen "ACME_Anvil_Co.unv" annehmen. Ändern Sie diesen Dateinamen vor dem Speichern in "z_ACME_Anvil_Co.unv".

10. Exportieren Sie das abgeleitete Universe wie folgt in CMS:

- a. Wählen Sie im Menü "Designer" die Optionen "File" > "Export" aus.
- b. Wählen Sie in der Dropdown-Liste des Felds "Domain" <Durchsuchen> aus. Suchen Sie und markieren Sie "CA Customer Universes".
- c. Klicken Sie auf OK, um das Universe in das lokale CMS zu exportieren.

Das Dialogfeld "Universe wurde erfolgreich exportiert" wird angezeigt.

Das Framework, das die Höherstufung anwenderspezifischer Schemaänderungen in ganz CA BI ermöglicht, ist jetzt vorhanden.

11. Melden Sie sich als administrativer Anwender bei BusinessObjects InfoView an, und führen Sie die folgenden Schritte aus:

- a. Wählen Sie "Public Folders" aus.
- b. Klicken Sie in der InfoView-Symbolleiste auf "New" > "Folder".
- c. Geben Sie im Feld "Folder Name" eine Beschreibung ein, die für Berichtsanwender aussagekräftig ist, z. B. "Organisationsname - Berichte".
- d. Klicken Sie auf "OK", damit der Ordner unter "Public Folders" erstellt wird.

Damit wird das Mindestframework zur Verwendung und Speicherung von Berichten durch Ihre Organisation erstellt. Dieser Ordnerstruktur können beliebig viele Unterordner und Objekte hinzugefügt werden.

Schemaänderungen an der Infrastruktur

Nach dem Einrichten der CA BI-Entwicklungsumgebung und dem Veröffentlichen von Schemaänderungen auf CA SDM anhand des dokumentierten Prozesses zum Anpassen von Schemadaten können die Schemaänderungen in der CA BI-Infrastruktur höhergestuft werden. Sie können das neue Schema für die Berichterstellung und -änderung verfügbar machen.

Hinzufügen von Schemaänderungen zum abgeleiteten Universum

Das Höherstufen von Schemaänderungen in der CA BI-Infrastruktur ist ebenso einfach wie das Hinzufügen des neuen Schemaobjekts zum abgeleiteten Universum.

Hinweis: Bevor Sie anfangen, überprüfen Sie, dass die erforderlichen Schritte bereits ausgeführt und die neuen Schemaobjekte dem flexiblen CA SDM-Schema hinzugefügt wurden.

So fügen Sie dem abgeleiteten Universum Schemaänderungen hinzu

1. Öffnen Sie den BusinessObjects Designer, und importieren Sie das abgeleitete Universum wie folgt in ein lokales Dateisystem:
 - a. Wählen Sie im Designer-Menü die Option "File" > "New" (Datei > Neu).

Das Dialogfeld "Universe Successfully Imported" (Universum wurde erfolgreich importiert) wird angezeigt.
 - b. Klicken Sie auf "OK".

2. Aktualisieren Sie die Struktur des abgeleiteten Universums folgendermaßen:

- Wählen Sie im Designer-Menü "View" > "Refresh Structure" (Ansicht > Struktur aktualisieren) aus.

Die folgenden Fragen werden angezeigt:

- "Do you want to refresh the out of date columns in selected tables?"
(/Möchten Sie die veralteten Spalten in den ausgewählten Tabellen aktualisieren?) Klicken Sie auf "OK".

Hinweis: Wenn die Meldung "No update needed" angezeigt wird, bedeutet dies, dass die CA SDM-Objektebene nicht ordnungsgemäß mit dem neuen Schema aktualisiert wurde. Lesen Sie die Anweisungen zur Veröffentlichung von Schemaänderungen in CA SDM.

- "Refresh structure: The structure has been successfully modified." (Struktur aktualisieren: Die Struktur wurde erfolgreich geändert.). Klicken Sie auf "OK".

Es werden neue Spalten in der Universumsstruktur auf der rechten Fensterseite angezeigt, in denen neue Objekte für die Verwendung im abgeleiteten Universum bereitgestellt werden.

Die Objekte sind für die CA BI-Tools verfügbar, nachdem sie aus dem rechten Fenster in das linke Fenster verschoben wurden. Wenn Sie dem linken Fenster Objekte hinzufügen, vergewissern sich, dass die [allgemeinen Standards für Schemaänderungen](#) (siehe Seite 520) eingehalten werden.

3. Ziehen Sie die neuen Objekte an die gewünschte Stelle im linken Fenster, und legen Sie sie dort ab.
4. Klicken Sie auf "Speichern".
5. Wählen Sie im Designer-Menü die Option "Datei" > "Exportieren".

Das Dialogfeld "Universe wurde erfolgreich exportiert" wird angezeigt.
6. Klicken Sie auf "OK".

Änderungen, die dem Schema des abgeleiteten Universums hinzugefügt wurden, werden in das lokale CMS exportiert.

7. Wählen Sie im Designer-Menü /"Tools" > "Check Integrity" (Tools > Integrität prüfen) aus.
 - a. Aktivieren Sie im angezeigten Dialogfeld das Kontrollkästchen "Parse Objects" (Objekte analysieren). (Verändern Sie keine anderen Einstellungen.)
 - b. Klicken Sie auf "OK". Die Integritätsprüfung wird gestartet.
Hinweis: Es sollten keine Analysefehler gemeldet werden. Wenn Fehler gefunden werden, ändern Sie Ihre Objekte im linken Bereich so, dass sie keine Analysefehler verursachen.
8. Klicken Sie auf "OK", um das Dialogfeld zu schließen.
9. Exportieren Sie das abgeleitete Universum nach CMS wie folgt:
 - a. Wählen Sie im Designer-Menü die Option "Datei" > "Exportieren".
 - b. Wählen Sie in der Dropdown-Liste "Domain" (Domäne) die Option <Browse> (Durchsuchen), suchen Sie "CA Customer Universes" (Benutzerdefinierte CA-Universen) und wählen Sie die Option aus.
 - c. Klicken Sie auf "OK", um das Universum in das lokale CMS zu exportieren.
Das Dialogfeld "Universe wurde erfolgreich exportiert" wird angezeigt.
10. Speichern Sie Ihre Änderungen, und exportieren Sie das CA SDM-Universum.
Die Änderungen sind jetzt in der CA BI-Berichtsumgebung verfügbar, einschließlich Web Intelligence und Crystal Reports.

Allgemeine Schemaänderungen

Sie können Schemaänderungen im Universum implementieren. Um Sie mit dem Prozess vertraut zu machen, werden in der folgenden Tabelle die üblichen Schemaänderungen aufgelistet, die Sie vorfinden können.

Wenn ein Feldtyp in Web Screen Painter wie folgt definiert ist ...	Befolgen Sie diese Regeln bei der Verwendung des Felds im Universum: Klicken Sie mit der rechten Maustaste auf das Attribut und wählen Sie ...
INTEGER	"Objekteigenschaften", Registerkarte "Definition", Typ = "Zahl"
STRING	"Objekteigenschaften", Registerkarte "Definition", Typ = "Zeichen"
DATUM	"Objekteigenschaften", Registerkarte "Definition", Typ = "Datum" "Objektformat", Registerkarte "Zahl": Wählen Sie die Kategorie "Datum/Uhrzeit"; wählen Sie das Format "mm/dd/yyyy hh:mm:ss AM/PM"

Wenn ein Feldtyp in Web Screen Painter wie folgt definiert ist ...	Befolgen Sie diese Regeln bei der Verwendung des Felds im Universum: Klicken Sie mit der rechten Maustaste auf das Attribut und wählen Sie ...
DAUER	"Objekteigenschaften", Registerkarte "Definition", Typ = "Zahl", "Objekteigenschaften", Registerkarte "Definition", Auswahl = "PdmSeconds(object.attr)"
SREL	Erstellen Sie einen CA SDM-Attribut-Aliasnamen.
BREL	Nicht zutreffend
QREL	Nicht zutreffend
DERIVED	Verwenden Sie ggf. einen geeigneten Datentyp und ein geeignetes Objektformat für den Wert, der im Feld "DERIVED" gespeichert wird. Das Feld "DERIVED" kann ein beliebiges Ergebnis haben, es muss also kein bestimmter Standard befolgt werden.
Sonderfall: "Local" Dies ist kein innerhalb von Web Screen Painter definierter Datentyp, sondern ein Datentyp, der gelegentlich vom Universum verwendet wird, um einen nicht unterstützten Datentyp anzugeben.	Das Feld "Local" wird im rechten Fenster des Universums mit Typ "L" angezeigt. Diese Felder können gezogen, aber nicht in einer Klasse im rechten Fenster des Universums abgelegt werden. In den meisten Fällen werden Felddatentypen wie "binär" nicht vom Universum unterstützt. Sie können jedoch dem linken Fenster des Universums hinzugefügt werden, indem Sie ein Objekt erstellen und d"PDmString (object.attribute)" im Auswahlfenster des Dialogfelds "Eigenschaften bearbeiten" platzieren.

Berichts- und Ordnerstrukturen

In der CA BI-Installation sind mehrere Berichtsobjekte für Crystal Report XI und WebI enthalten. Die Berichte sind im folgenden-CA SDM-Ordner enthalten: "CA Reports\CA SDM".

Wichtig! Ändern Sie das CA SDM-Universum und die Berichtsobjekte in der CA SDM-Ordnerstruktur nicht.

Berücksichtigen Sie die folgenden Informationen über Berichte und die Ordnerstrukturen:

- In den Schritten zum Erstellen eines Rahmens wird erläutert, wie dem öffentlichen Bereich von InfoView Ordner hinzugefügt werden, die für den Endbenutzer spezifisch sind. Innerhalb dieser Ordner kann ein Benutzer zusätzliche Unterordner und Berichtsobjekte erstellen.

- In einer Implementierung, in der jeder Benutzer mit einer eindeutigen CA SDM-Anmelde-ID Zugriff auf CA BI hat, können die Benutzer Berichte für ihre eigenen Zwecke im Bereich "My Folders" (Eigene Ordner) speichern. BusinessObjects erzwingt die Sicherheit der Ordner, indem diese Objekte nur dem angemeldeten Benutzer angezeigt werden.
- In einer Implementierung, in der alle Benutzer eine einzige Berichtsbenutzer-ID für den Zugriff auf CA BI haben, ist der Bereich "My Folders" (Eigene Ordner) für alle Benutzer zugänglich.

Erstellen von Web Intelligence-Berichten

Verwenden Sie CA Business Intelligence, um einen Web Intelligence-Bericht zu erstellen.

So erstellen Sie einen Web Intelligence-Bericht

1. Klicken Sie auf der Registerkarte "Berichte" in CA SDM auf die Schaltfläche "InfoView".

Die Startseite von InfoView wird angezeigt.

2. Klicken Sie in der Menüleiste auf "Neu", "Web Intelligence-Dokument".
3. Wählen Sie das abgeleitete Universum aus, das Sie beim Erstellen des Entwicklungsrahmens definierten.

Das Web Intelligence-Berichterstellungstool wird angezeigt.

Hinweis: Speichern Sie das Dokument in regelmäßigen Abständen. Wenn das Zeitlimit für die Verbindungssitzung überschritten wird, gehen Ihre Berichtsänderungen verloren. Informationen zur Erhöhung des Zeitlimitwerts für die Web Intelligence-Verbindungssitzung finden Sie im *Administrationshandbuch*.

4. Wählen Sie in der Web Intelligence-Symboleiste "Save" > "Save As" (Speichern > Speichern unter) aus.

Das Dialogfeld "Save Document" (Dokument speichern) wird angezeigt.

5. Geben Sie im Abschnitt "General" (Allgemein) einen sinnvollen Namen für diesen Bericht im Feld "Title" (Titel) an.
6. Wählen Sie im Speicherortbereich den entsprechenden Ordner aus.
7. (Optional) Ändern Sie ggf. die Eigenschaften.
8. Klicken Sie auf "OK", um den Bericht zu speichern.

Der Bericht wird im angegebenen Ordner angezeigt und ist für alle Berichtsanwender verfügbar.

Erstellen von Web Intelligence-Berichten

Verwenden Sie CA Business Intelligence, um einen Bericht zu ändern, der in der Ordnerstruktur "CA Reports\CA Service Desk" bereitgestellt wurde.

So ändern Sie einen CA Business Intelligence-Bericht

1. Klicken Sie auf der Registerkarte "Berichte" in CA SDM auf die Schaltfläche "InfoView".
Die Startseite von InfoView wird angezeigt.
2. Navigieren Sie im linken Fenster durch die CA-Berichtsordnerstruktur, und öffnen Sie den gewünschten Web Intelligence-Bericht.
3. Klicken Sie auf den Namen des Berichts, damit der Bericht ausgeführt wird und ein Ergebnis angezeigt.
4. Wählen Sie in der Web Intelligence-Symbolleiste "Save" > "Save As" (Speichern > Speichern unter) aus.
Das Dialogfeld "Save Document" (Dokument speichern) wird angezeigt.
5. Wählen Sie im Speicherortbereich den entsprechenden Ordner aus.
6. Klicken Sie auf "OK", um den Bericht an dem neuen Speicherort zu speichern.
7. Wählen Sie "Document" > "Edit" (Dokument > Bearbeiten).
8. Klicken Sie auf "Edit Query" (Query bearbeiten) (der Name des Universums CA SDM wird auf der Registerkarte "Data" (Daten) angezeigt).
9. Klicken Sie auf die Registerkarte "Properties" (Eigenschaften)". Klicken Sie ggf. auf die Pfeile nach unten neben dem Universum, damit der CA SDM-Text mit einem Auslassungszeichen ("...") angezeigt wird.
10. Klicken Sie auf das Auslassungszeichen ("..."), um das Dialogfeld "Universe" (Universum) anzuzeigen.
Das Fenster "Other Available Universes (Andere verfügbare Universen) wird angezeigt.
11. Wählen Sie den Namen Ihres Universums aus und klicken Sie auf "OK".
Web Intelligence ordnet automatisch alle bekannten Felder des CA SDM-Universums Ihrem Universum zu, und das Dialogfeld "Change Source" (Quelle ändern) wird angezeigt. Grüne Kontrollkästchen werden neben jedem zugeordneten Feld angezeigt. Wenn alle Felder richtig zugeordnet sind, klicken Sie auf "OK", um die Änderung zu bestätigen. Wenn Felder mit einem roten "X" angezeigt werden, klicken Sie auf das Auslassungszeichen ("...") neben dem Feldnamen, und wählen Sie das entsprechende Feld aus.
12. Klicken Sie auf der Web Intelligence-Symbolleiste auf "Edit Report" (Bericht bearbeiten), und wählen Sie die Registerkarte "Properties" (Eigenschaften).

13. Erweitern Sie den Knoten "General" (Allgemein).
14. Klicken Sie auf das Auslassungszeichen ("...") neben dem Dokumenteigenschaftswert.
Das Dialogfeld "Save Document" (Dokument speichern) wird angezeigt.
15. Aktivieren Sie im Abschnitt "Document Options" (Dokumentoptionen) das Kontrollkästchen "Refresh On Open" (Beim Öffnen aktualisieren).
16. Klicken Sie auf "Save" (Speichern), und schließen Sie Web Intelligence.
Der Bericht wird dem entsprechenden Universum zugeordnet und kann nach Bedarf geändert werden.

Erstellen von Crystal Reports

Verwenden Sie Crystal Reports, um einen Bericht im CA Business Intelligence-Universum zu speichern.

So erstellen Sie einen Crystal-Bericht

1. Öffnen Sie Crystal Reports XI.
2. Wählen Sie "Datei" > "Neu" > "Leerer Bericht".
Das Dialogfeld "Database Expert" wird angezeigt.
3. Erweitern Sie den Knoten "Create new Connection" (Neue Verbindung erstellen), und klicken Sie auf "Universes" (Universen).
Das Dialogfeld "BusinessObjects Enterprise" wird angezeigt.
4. Melden Sie sich mit den Administrator-Anmeldeinformationen bei BusinessObjects Enterprise an.
5. Navigieren Sie zu dem Ordner, der das abgeleitete Universum enthält.
6. Wählen Sie das abgeleitete Universum aus und klicken Sie auf "Open" (Öffnen).
Das Dialogfeld "BusinessObjects Query Panel" (BusinessObjects-Abfragefenster) wird angezeigt.
7. Ziehen Sie in der Universums-Baumstruktur die entsprechenden Attribute in die Bereiche "Select" (Auswahl) und "Filter" des Abfragefensters.
8. Wenn der Abfrageerstellungsprozess abgeschlossen ist, wird das Standard-Designertool von Crystal Reports angezeigt.
9. Erstellen Sie den Bericht und führen Sie ihn aus.
Hinweis: Detaillierte Informationen zum Erstellen und Ausführen von Berichten finden Sie in der Crystal Reports-Dokumentation.

10. Speichern Sie den Bericht wie folgt im Business Objects Enterprise-Repository:

- a. Wählen Sie "File" > "Save As" (Datei > Speichern unter).
- b. Wählen Sie im Dialogfeld "Save As" (Speichern unter) die Option "Enterprise" aus.
- c. Navigieren Sie zu dem Ordner, den Sie während der Definition des Entwicklungsrahmens erstellt haben, und speichern Sie den neuen Bericht in BusinessObjects Enterprise.

Der neue Bericht steht nun im Unternehmen zur Verfügung und kann nach Bedarf geändert werden.

Ändern von Crystal Reports

Verwenden Sie Crystal Reports, um einen Bericht im CA Business Intelligence-Universum zu ändern.

So ändern Sie Crystal Reports XI-Berichte

1. Öffnen Sie Crystal Reports XI.
2. Wählen Sie "Datei" > "Neu" > "Leerer Bericht".
Das Dialogfeld "Database Expert" wird angezeigt.
3. Klicken Sie, um "Create new Connection" (Neue Verbindung erstellen) zu erweitern.
Klicken Sie auf "Universes" (Universen).
Das Dialogfeld "BusinessObjects Enterprise" wird angezeigt.
4. Melden Sie sich bei Business Objects Enterprise als Administrator an.
5. Klicken Sie, um zu dem Ordner zu navigieren, der das abgeleitete Universum enthält, und klicken Sie, um das abgeleitete Universum auszuwählen.
Klicken Sie auf "Öffnen".
Das Dialogfeld "BusinessObjects Query Panel" (BusinessObjects-Abfragefenster) wird angezeigt.
6. Navigieren Sie in der Universumsbaumstruktur, um Attribute zu suchen, sie zu den Bereichen "Select" (Auswahl) und "Filter" des Abfragefensters zu ziehen und sie dort abzulegen.

Wenn der Abfragegeerstellungsprozess abgeschlossen ist, wird dem Berichtersteller das Standard-Designertool von Crystal Reports angezeigt.

7. Erstellen Sie den Bericht und führen Sie ihn entsprechend den Crystal Reports-Anweisungen aus.
8. Speichern Sie den Bericht anschließend im Business Objects Enterprise-Repository.
 - a. Wählen Sie "File" > "Save As" (Datei > Speichern unter).
Das Dialogfeld "Save As" (Speichern unter) wird angezeigt.
 - b. Klicken Sie links neben dem Dialogfeld "Save As" (Speichern unter) auf das "Enterprise"-Symbol.
 - c. Navigieren Sie durch die Ordnerstruktur, ausgehend von dem kundenspezifischen Ordner, der an früherer Stelle in diesem Dokument erstellt wurde, und klicken Sie auf "Save" (Speichern), um diesen Bericht in BusinessObjects Enterprise zu speichern.
9. Der neue Bericht steht nun im Unternehmen zur Verfügung und kann nach Bedarf geändert werden.

Übernehmen von neuen Crystal Reports in CA Business Intelligence

Sie können Crystal Reports in ein CA Business Intelligence-Universum verschieben.

So übernehmen Sie neue Crystal Reports in CA Business Intelligence

1. Öffnen Sie Crystal Reports XI.
2. Wählen Sie "File", "Open".
Das Dialogfeld "Öffnen" wird angezeigt.
3. Klicken Sie auf der linken Seite auf "Enterprise".
Das Anmeldedialogfeld für BusinessObjects Enterprise wird angezeigt.
4. Melden Sie sich mit den Administrator-Anmeldeinformationen bei BusinessObjects Enterprise an.
Navigieren Sie ausgehend von "CA Reports\CA Service Desk" durch die Ordnerstruktur, bis der Zielbericht angezeigt wird.
5. Wählen Sie den Zielbericht aus, und klicken Sie auf "Open" (Öffnen).
Der Bericht wird in Crystal Reports angezeigt.
6. Klicken Sie auf "File" > "Save As" (Datei > Speichern unter).
Das Dialogfeld "Speichern unter" wird angezeigt.
7. Geben Sie den Ordner an, den Sie bei der Definition des Entwicklungsrahmens erstellt haben.
8. Klicken Sie auf "Speichern".

9. Wählen Sie im Crystal Reports-Menü "Database" > "Database Expert" (Datenbank > Database Expert) aus.

Das Dialogfeld "Database Expert" wird angezeigt.

10. Wählen Sie im linken Fenster "Create New Connection" > "Universe (Neue Verbindung erstellen > Universum) aus.
11. Wählen Sie das abgeleitete Universum aus.
12. Ziehen Sie alle von diesem Bericht verwendeten Attribute in die neue Abfrage, legen Sie sie dort ab und klicken Sie auf "OK".
13. Ersetzen Sie in jeder Formel und Zelle die ursprünglichen Attribute durch Attribute der neuen Abfrage.
14. Nachdem alle Attribute ersetzt worden sind, gehen Sie wie folgt vor:
 - a. Wählen Sie im Crystal Reports-Menü die Optionen "Database" > "Database Expert" (Datenbank > Database Expert) aus.
 - b. Wählen Sie im Dialogfeld "Database Expert" die ursprüngliche Abfrage aus, und klicken Sie auf die Pfeile nach links in der Mitte zwischen den beiden Fenstern, um die alte Abfrage zu entfernen.
 - Wenn alle Attribute ordnungsgemäß ersetzt wurden, wird die ursprüngliche Abfrage ohne Dokumente zur Lösung von Issues entfernt, und Sie können mit der Änderung des Berichts fortfahren.
 - Wenn ursprüngliche Attribute im Bericht verbleiben, wird die folgende Meldung angezeigt: "The report is using fields from one or more tables. Continue?" (Der Bericht verwendet Felder aus einer oder mehreren Tabellen. Fortfahren?)
 - Klicken Sie auf "Cancel" (Abbrechen), und kehren Sie zum Bericht zurück.
 - Ersetzen Sie weiter alle ursprünglichen Attribute mit Attributen aus der neuen Abfrage, bis die ursprüngliche Abfrage ohne Warnmeldungen entfernt werden kann.

Der Bericht ist für die Anpassung vorbereitet.

Übernehmen vorhandener Access-Berichte in CA Business Intelligence

Vordefinierte Microsoft Access-Berichte werden nicht mehr entwickelt oder mit CA SDM bereitgestellt. Mit den folgenden Schritten können Sie jedoch vorhandene Access-Berichte in die CA Business Intelligence-Berichtsumgebung übernehmen:

1. Fügen Sie die angemessenen CA SDM-Schemaänderungen zu CA Business Intelligence hinzu.
2. Verwenden Sie Web Intelligence oder Crystal Reports, um den Bericht umzuschreiben.

Verschieben aus der Entwicklung in die Produktion

Bis zu diesem Zeitpunkt wurden ein abgeleitetes Universum hinzugefügt, Ordnerstrukturen erstellt und Berichte erstellt und geändert. Daher kann die Entwicklungsstruktur jetzt in die Produktion verschoben werden. In diesem Schritt verwenden Sie den BusinessObjects-Importassistenten.

So verschieben Sie Elemente aus der Entwicklung in die Produktion

1. Wählen Sie im Startmenü "Alle Programme" > "BusinessObjects XI Release 2" > "BusinessObjects Enterprise" > "Import Wizard" (Import-Assistent).

Der Importassistent wird angezeigt.

2. Wählen Sie im Bildschirm "Source Environment" (Quellumgebung) den Eintrag "BusinessObjects XI R2", und geben Sie die notwendigen Anmeldeinformationen für das Entwicklungssystem ein.
3. Wählen Sie im Bildschirm "Destination Environment" (Zielumgebung) *eine* der folgenden Optionen aus:
 - **Das Produktionssystem.** Mit dieser Option werden alle ausgewählten Objekte sofort ins Produktionssystem verschoben.
 - **Eine externe Datei, die zu einem späteren Zeitpunkt ins Produktionssystem importiert werden kann.** Mit dieser Option werden alle Objekte in einer BIAR-Datei (Business Intelligence Archive Resource) gespeichert.
4. Löschen Sie im Bildschirm "Select Objects to Import" alle Einstellungen, und aktivieren Sie dann die folgenden Kontrollkästchen: "Import folders and objects" und "Universe importieren".

Hinweis: Angezeigte Warnungen brauchen Sie nicht zu beachten.

5. Wählen Sie die Ordnerstruktur aus, die Ihren bestimmten Ordner enthält, und deaktivieren Sie die Kontrollkästchen für alle Objekte, die nicht verschoben werden sollen.
6. Klicken Sie im Bildschirm "Import Options for Universes and Connections" (Importoptionen für Universen und Verbindungen) auf die folgende Option: "Import the universes and connections that the selected Web Intelligence and Desktop Intelligence documents use directly" (Von den ausgewählten Web Intelligence- und Desktop Intelligence-Dokumenten verwendete Universen und Verbindungen direkt importieren).
7. Erweitern Sie auf dem Bildschirm "Universe Folder and Universes" (Universumsordner und Universen) den entsprechenden Ordner, in dem das Universum gespeichert ist.

Hinweis: Angezeigte Warnungen brauchen Sie nicht zu beachten.

8. Klicken Sie auf "Fertig stellen".

Wenn die Ordner und Berichte direkt zum Produktionscomputer verschoben wurden, können Sie die Änderungen in InfoView anzeigen. Wenn die Objekte in einer BIAR-Datei platziert wurden, können Sie den Importassistenten zu einem späteren Zeitpunkt ausführen. Wählen Sie die BIAR-Datei als Quellumgebung und den Produktionsserver als Zielumgebung.

Anpassen von Legacy-Berichten

In CA SDM können Sie Legacy-Berichte anpassen oder eigene Berichte entwerfen. Sie können:

- Übersichts-, Detail- oder Analyseberichte aus Legacy-Systemen anpassen, indem Sie z. B. zusätzliche Felder für ganz bestimmte Informationen hinzufügen.
- Neue Berichte erstellen, die ein für Sie nützliches Format aufweisen und in dem alle in der Datenbank verfügbaren Informationen enthalten sind.
- Argumente von Variableninformationen an Berichte übergeben, indem Sie Befehlszeilenargumente in die Berichte einschließen. Die Argumente können Werte oder Ausdrücke wie der aktuelle Wert eines Feldes oder ein SQL WHERE-Klauselausdruck sein.
- Berichte in der Befehlszeile generieren, indem Sie eine Skriptdatei oder eine Menüoption verwenden.

So erstellen Sie einen anwenderspezifischen Bericht:

1. Entwerfen Sie den Bericht:
 - Entscheiden Sie, welche Daten Sie in den Bericht einschließen möchten.
 - Erstellen Sie eine Berichtsvorlage, die SQL-ähnliche Abfragen, Ausdrücke und Funktionen zum Bearbeiten der Daten enthält sowie Anweisungen, um die Daten für den Ausdruck zu formatieren.
2. Generieren Sie den Bericht über:
 - Die Befehlszeile
 - Eine CA SDM-Menüoption
 - Eine Skriptdatei

Hinweis: Wenn Sie über ein -Datenbanksystem eines anderen Anbieters verfügen, können Sie die Tools zum Generieren von Berichten dieses Systems verwenden, um Berichte mit Daten aus der CA SDM-Datenbank zu erstellen. CA SDM bietet mehrere Datenbankansichten, die das Erstellen von anwenderspezifischen Berichten unter Verwendung eines Datenbanksystems -von einem Drittanbieter vereinfachen. Weitere Informationen zum Erstellen von Berichten mit Datenbanken finden Sie in der Dokumentation für Ihr Datenbanksystem. Weitere Informationen über Datenbankansichten finden Sie im *Administrationshandbuch*.

Weitere Informationen:

[Anpassen von Crystal Reports](#) (siehe Seite 555)

Benutzerdefinierte Berichtslayouts

Zum Entwerfen von Berichten müssen Sie über grundlegende Kenntnisse in den folgenden Bereichen verfügen:

- SQL-Abfragen schreiben
- Programmierung, insbesondere in C
- Besondere Programme oder Skriptdateien erstellen, die Sie möglicherweise ausführen müssen, bevor Sie das Berichtsvorlagenprogramm ausführen. So können Sie ein Programm erstellen, das den Benutzer auffordert, ein Argument einzugeben (wie z. B. die Bedingungen für eine WHERE-Klausel).

Hinweis: Bevor Sie einen benutzerdefinierten Bericht erstellen, sollten Sie prüfen, ob der gewünschte Bericht nicht bereits verfügbar ist. CA SDM stellt eine große Auswahl an Crystal Reports und Microsoft Access-Berichten sowie Laufzeitversionen dieser Produkte bereit, mit denen Sie die Berichte ausführen können. Weitere Informationen zu Berichten finden Sie im "*Administrationshandbuch*".

Auswählen von Informationen für Berichte

Hinweise zum Auswählen von Daten aus der CA SDM-Datenbank für benutzerdefinierte Berichte finden Sie im *Technischen Referenzhandbuch* von CA SDM. In diesem Anhang werden Datenbanktabellen, -felder, -beschreibungen und andere Datenbankinformationen aufgeführt.

So erstellen Sie eine Berichtsvorlage

Eine Berichtsvorlage ist eine Datei, die einen Bericht mit einem bestimmten Layout generiert, wenn sie von einem CA SDM-Berichtsprogramm ausgeführt wird. Eine Berichtsvorlage enthält veränderliche Ausdrücke, Funktionen und Anweisungen, die definieren, wie die Daten abgerufen, berechnet und gedruckt werden.

Um eine Berichtsvorlage zu erstellen, generieren Sie eine Datei, die folgende Arten von Berichtsanweisungen enthält:

Blockanweisungen

Mit diesen Anweisungen werden die CA SDM-Datenbanktabellen, aus denen Daten abgerufen werden, und Aktionen, die mit den abgerufenen Daten ausgeführt werden, definiert.

Layoutanweisungen

Mit diesen Anweisungen wird definiert, wie die Datenvariablen und der Text im Bericht ausgegeben werden.

Hinweis: Speichern Sie alle .rpt-Dateien in einem neuen Verzeichnis "\$NX_ROOT/site/mods/rpt" (UNIX) oder "*installationsverzeichnis*\site\mods\rpt" (Windows). In diesem Verzeichnis bleiben die Dateien beim Aktualisieren auf eine neue Version von CA SDM erhalten.

Weitere Informationen:

[Berichtsvorlagenreferenz](#) (siehe Seite 539)

[Beispiel: Berichtsvorlage](#) (siehe Seite 535)

Blockanweisungen

Blockanweisungen liefern die Berichtsvorlage mit ihrem Framework. Sie definieren die zu bearbeitenden Daten und steuern die Ausführung des Berichts. Blockanweisungen beginnen mit einem Namen, der in der ganzen Berichtsvorlage verwendet werden muss. Danach sind sie in zwei Abschnitte unterteilt:

Abschnitt zur Datenabfrage

Dieser Abschnitt enthält SQL SELECT-, WHERE- und SORT-Klauseln, mit denen definiert wird, welche Daten aus der Datenbank abgerufen werden.

Abschnitt zum Ausgabeprogramm

In diesem Abschnitt werden die Aktionen definiert, die mit den abgerufenen Daten ausgeführt werden. Er enthält veränderliche Erklärungen, Funktionen und andere Blockanweisungen, einschließlich verschachtelter Anweisungen, die für konditionelle Berichte verwendet werden können. Dieser Abschnitt kann ebenfalls Layoutanweisungen enthalten, die Daten als ASCII-Text formatieren und drucken.

Im Folgenden ist eine vereinfachte Version der Syntax einer Blockanweisung dargestellt, welche die Beziehung zwischen den beiden Abschnitten zeigt:

```
BLOCK blockname ("SELECT clause", "WHERE clause")
```

```
    SORT clause {output program statements}
```

Der BLOCK im Abschnitt „Referenz“ erläutert die detaillierte Version der Syntax zusammen mit einer Beschreibung der einzelnen Klauseln und Parameter.

Layoutanweisungen in Berichtsvorlagen

Layoutanweisungen definieren, wie Variablen und Text auf der Berichtsausgabe angezeigt werden:

- Sie können die Anweisungen PAGE HEADER und PAGE FOOTER verwenden, um Informationen am oberen und unteren Rand von jeder Berichtssseite einzufügen.
- Sie können HEADER-, HEADER2-, FOOTER- und PRINT-Anweisungen in dem Abschnitt in geschweiften Klammern der übergeordneten BLOCK-Anweisung verschachteln, um Titel und Zusammenfassungen für die verschiedenen *Berichtsabschnitte* (Teile der Berichtsausgabe) zu erstellen.

Hinweis: Gehen Sie beim Verschachteln sorgfältig vor, damit Sie die geschweiften Klammern in Layoutanweisungen nicht mit den geschweiften Klammern verwechseln, die verschachtelte Anweisungen innerhalb einer übergeordneten BLOCK-Anweisung umgeben.

- Sie können Text einschließen, um Labels und Zeichnungsbeschriftungen zu erstellen, um die Darstellung des Berichts zu verbessern.

Die Layoutanweisungen lauten folgendermaßen:

PAGE HEADER

Fügt Informationen oben auf jeder Berichtssseite ein. Sie befindet sich außerhalb der BLOCK-Anweisung.

PAGE FOOTER

Fügt Informationen unten auf jeder Berichtssseite ein. Sie befindet sich außerhalb der BLOCK-Anweisung.

HEADER

Fügt Informationen oben in jedem Berichtsabschnitt ein. Sie befindet sich innerhalb der BLOCK-Anweisung.

HEADER2

Fügt die Kopfzeileninformationen des jeweiligen Berichtsabschnitts oben auf jeder folgenden Seite ein, wenn sich der Berichtsabschnitt über mehrere Seiten erstreckt. Sie befindet sich innerhalb der BLOCK-Anweisung.

FOOTER

Fügt Informationen unten in jedem Berichtsabschnitt ein. Sie befindet sich innerhalb der BLOCK-Anweisung.

PRINT

Fügt Daten in einen Berichtsabschnitt ein. Sie befindet sich innerhalb der BLOCK-Anweisung.

In Layoutanweisungen können Sie auch die folgenden vordefinierten Variablen verwenden:

- CT druckt die aktuelle Uhrzeit
- CD druckt das aktuelle Datum
- PG druckt die Seitenzahl

Datenfelder

Gibt eine beliebige Variable in einer Layout-Anweisung an, die Daten ergibt, wenn Sie den Bericht generieren. Berücksichtigen Sie die folgenden Richtlinien, wenn Sie Felder in Ihre Berichtsvorlage einfügen:

- Schließen Sie Datenfelder in eckigen Klammern ([]) ein.
- Die eckigen Klammern des Feldes definieren den Druckbereich in jeder Ausgabezeile. Dieser Bereich entspricht der Anzahl an Zeichen, die durch die eckigen Klammern begrenzt ist, einschließlich der Klammern. Wenn die Ausgabe einer Variablen länger als der Druckbereich ist, wird die Ausgabe gekürzt. Um sicherzustellen, dass ein Feld über einen ausreichenden Druckbereich verfügt, können Sie zusätzliche Leerzeichen zwischen dem Variablennamen und der schließenden Klammer einfügen. Diese zusätzlichen Leerzeichen ermöglichen die Anzeige von Kontakten mit langen Namen:

```
[contact      ]
```

- Für den Fall, dass eine Ausgabe weniger als eine Zeile in Anspruch nimmt, kann das Feld mit einer spitzen Klammer rechts (>) geschlossen werden. Dadurch wird der Druckbereich bis zum rechten Rand erweitert. Die spitze Klammer rechts, die beispielsweise in einer HEADER-Anweisung verwendet wird, führt dazu, dass das aktuelle Datum gedruckt wird, ohne gekürzt zu werden:

```
[CD          >
```

Hinweis: Wenn sich ein Feld über mehrere Zeilen erstreckt und die Variable als MULTILINE gekennzeichnet ist, hat die spitze Klammer rechts (>) dieselbe Funktion wie die eckige Klammer rechts (]). Wenn die Druckanweisung für eine MULTILINE-Variable mit einer spitzen Klammer rechts (>) geschlossen wird, werden die Zeichen an einem Leerzeichen umgebrochen, um innerhalb des Feldes zu bleiben, das durch die linke eckige Klammer ([) und die rechte spitze Klammer (>) definiert wurde. Auch wenn die Variable nicht MULTILINE ist, werden durch die spitze Klammer rechts (>) alle Daten, unabhängig von ihrer Länge, in der aktuellen Zeile angezeigt.

- Ein Feld in einer Layoutanweisung kann sich auf eine vorher definierte Variable oder einen Spaltennamen beziehen.
- Damit es auf eine Variable oder einen Spaltennamen in einer anderen BLOCK-Anweisung verweist, verwenden Sie folgende Syntax:

```
blockname::column | variable-name
```

Text

Mit Text können Sie zusätzliche Informationen in Ihren Bericht einschließen. Er wird auf der Berichtsausgabe angezeigt genau wie in der Vorlage angegeben. Um Text in eine Layoutanweisung einzuschließen, fügen Sie ihn in einer beliebigen Zeile nach der öffnenden geschweiften Klammer ({} und vor der schließenden Klammer (}) ein. Schließen Sie ihn nicht in Anführungszeichen oder eckigen Klammern ein.

Im folgenden Beispiel werden "ACME Company" und "Page:" vom CA SDM-Berichtsprogramm als Literaltext interpretiert:

```
PAGE HEADER {  
  
                ACME Company                Page: [PG]  
  
}
```

Weitere Informationen:

[FOOTER-Anweisungen für Berichtsvorlagen](#) (siehe Seite 549)
[PAGE FOOTER-Anweisungen für Berichtsvorlagen](#) (siehe Seite 552)
[HEADER-Anweisungen für Berichtsvorlagen](#) (siehe Seite 550)
[HEADER2-Anweisungen für Berichtsvorlagen](#) (siehe Seite 551)
[PAGE HEADER-Anweisungen für Berichtsvorlagen](#) (siehe Seite 553)
[PRINT-Anweisungen für Berichtsvorlagen](#) (siehe Seite 553)

Veränderliche Ausdrücke in Berichtsvorlagen

Alle Werte, die in der Berichtsausgabe angezeigt werden sollen, können einer Variablen zugeordnet werden. Mit veränderlichen Ausdrücken können Sie:

- CA SDM-Daten bearbeiten.
- Funktionen verwenden, um Berechnungen mit abgerufenen Werten auszuführen.

Das folgende Beispiel erstellt die Variable "*Beschreibung*", die auf den Inhalt des Feldes "chg_desc" im Fenster "Change" verweist. Durch das MULTILINE-Kennzeichen kann die Variable vollständig über mehrere Zeilen gedruckt werden:

```
desc = description MULTILINE;
```

Das folgende Beispiel druckt die Beschreibung. Die Ausgabe wird genauso lang sein wie die Länge, die in Klammern definiert ist. Wenn eine längere Beschreibung angezeigt werden soll, erhöhen Sie die Anzahl an Leerzeichen zwischen den Klammern.

```
PRINT { [desc  ] }
```

Beispiel: Berichtsvorlage

Mit der folgenden Vorlage „Bericht für betroffenen Kontakt“ wird gezeigt, wie eine Berichtsvorlage erstellt wird. Mit dieser Vorlage wird ein Bericht erstellt, der offene Änderungsaufträge mit demselben betroffenen Kontakt aufführt:

```

PAGE HEADER {
                                                    Ab: [CD>
                                                    [CT>
}
PAGE FOOTER {
                                                    Seite: [PG>
}
BLOCK chg ("SELECT \
            chg_ref_num, description, priority, \
            status, category, assignee \
        FROM Change_Request",
        "WHERE #Change_Request.status = 'OP' \
AND #Change_Request.requestor = #ca_contact.id \
AND #ca_contact.last_name = ? \
AND #ca_contact.first_name = ? \
AND #ca_contact.middle_name = ? " , $1, $2, $3)
{
        BLOCK st ("SELECT sym FROM Change_Status",
            "WHERE code = ? ", chg::status) {}
        BLOCK (strlen(category)) cat ("SELECT sym FROM Change_Category",
            "WHERE code = ? ", chg::category) {}

HEADER {
            OPEN CHANGE ORDERS WITH SAME REQUESTOR/FROM CONTACT
CHANGE ORDER Summary          Pri   Status   Category          Assignee
}
HEADER2 {
CHANGE ORDER Summary          Pri   Status   Category          Assignee
-----
}

        num = chg_ref_num;
        desc = description MULTILINE;
        pr = deref (priority);
        stat = st::sym;
        catgry = cat::sym;
        asgn = deref (assignee);
PRINT {
[num          ] [desc          ] [pr ] [stat   ] [catgry          ] [asgn ]
}
}

```

PAGE HEADER

Gibt an, was oben auf jeder Seite des Berichts zu drucken ist. CD und CT sind vordefinierte Variablen, die das aktuelle Datum und die aktuelle Zeit angeben. Sie werden oben auf jeder Seite in der Kopfzeile angezeigt. Alle Felder enden mit einer spitzen Klammer, wodurch sich die Felder bis an den rechten Seitenrand ausdehnen können. Da sich "Ab" außerhalb eines Feldes und in einer Zeile nach der öffnenden Klammer befindet, wird es in der Berichtsausgabe als Text angezeigt.

```
PAGE HEADER {                               Ab:  [CD>
                                           [CT>
}
```

PAGE FOOTER

Schließt die Seitenzahl mit dem Text "Seite: " ein.

```
PAGE FOOTER {                               Seite: [PG>
}
```

Hinweis: Da die Anweisungen PAGE HEADER und PAGE FOOTER globale Kopf- und Fußzeilen erstellen, werden sie nicht in die BLOCK-Anweisung eingeschlossen.

Berichtsabschnitt

Erstellt einen Berichtsabschnitt für die Hauptanweisung BLOCK zusammen mit den verschachtelten Anweisungen. Der Berichtsabschnitt ist gewöhnlich nur Teil der Daten im Bericht, wobei dieser Bericht über nur einen Berichtsabschnitt verfügt. Der eindeutige Name dieses Blocks lautet chg.

Die SELECT-Anweisung wählt aus (FROM) drei Tabellen die Spalten aus, die in die Daten für den Bericht eingeschlossen werden sollen, wobei die von der WHERE-Klausel angegebenen Bedingungen erfüllt sein müssen.

Die letzten drei AND-Ausdrücke in der WHERE-Klausel enthalten Fragezeichen, die als Platzhalter für die Argumente fungieren, welche die Werte der Argumente \$1, \$2 und \$3 in dieser Reihenfolge annehmen. Somit steht "\$1" für "ca_contact.last_name", "\$2" für "ca_contact.first_name" und "\$3" für "ca_contact.middle_name". Die Argumente \$1, \$2 und \$3 erhalten die Werte von Befehlszeilenargumenten.

```
BLOCK chg ("SELECT \
...",
"WHERE \
...\
AND #ca_contact.last_name = ? \
AND #ca_contact.first_name = ? \
AND #ca_contact.middle_name = ? ", $1, $2, $3)
```


Kopfzeilen von Berichtsabschnitten

Gibt an, dass die öffnende geschweifte Klammer den Beginn des Teils des Ausgabeprogramms der BLOCK-Anweisung kennzeichnet: die enthaltenen Anweisungen bestimmen, was mit den Daten, die durch die Klauseln SELECT und WHERE abgerufen werden, geschehen soll. Das folgende Beispiel verfügt über verschachtelte HEADER- und HEADER2-Anweisungen, die sich nur auf diesen Berichtsabschnitt auswirken. HEADER2 wird nur gedruckt, wenn sich die Berichtsausgabe über mehrere Seiten erstreckt.

```
{
  ...
  HEADER {
    OPEN CHANGE ORDERS WITH SAME REQUESTOR/FROM CONTACT
CHANGE ORDER Summary          Pri    Status  Category Assignee
  }
  HEADER2 {
CHANGE ORDER Summary          Pri    Status  Category Assignee
-----
  }
}
```

Veränderliche Anweisungen

Dies sind die veränderlichen Ausdrücke, die auf die von den SELECT-Klauseln angegebenen Daten angewendet werden. Sie ordnen Spaltenwerten und den Ergebnissen von Ausdrücken Variablen zu. Diese Variablen entsprechen den Feldern in der folgenden PRINT-Anweisung.

Das MULTILINE-Kennzeichen der Variablen „desc“ führt dazu, dass sie nicht abgeschnitten, sondern über mehrere Zeilen gedruckt bzw. angezeigt werden. Die deref-Funktion wird verwendet, um den Zeichenfolgeausdruck in den referenzierten Spalten zurückzugeben.

```
num = chg_ref_num;
desc = description MULTILINE;
pr = deref (priority);
stat = st::sym;
catgry = cat::sym;
asgn = deref (assignee);
```

Drucken

Enthält die zu druckenden Felder. In diese Anweisung kann auch Text eingeschlossen werden, um die Darstellung des Berichts zu verbessern. Die schließende geschweifte Klammer fällt mit der öffnenden geschweiften Klammer des Ausgabeprogrammabschnitts der BLOCK-Anweisung zusammen.

```
PRINT {
[num ] [desc          ] [pr] [stat] [catgry] [asgn          ]
}
}
```

Weitere Informationen:

[Der Berichtsbefehl](#) (siehe Seite 538)

Erstellen von Berichten

Nachdem Sie die Berichtsvorlage erstellt haben, können Sie den Bericht generieren, indem Sie das CA SDM-Berichtsprogramm ausführen. Zum Ausführen des Programms können Sie Folgendes verwenden:

- Die Befehlszeile
- Eine CA SDM-Menüoption
- Eine Skriptdatei

Hinweis: Wenn Sie einen UNIX-Server verwenden, können Sie den Parameter zum Umleiten der Berichtsausgabe ("rptuiDsp") in den Berichtsbefehl einschließen, um ein Dialogfeld mit Optionen zum Senden des Berichts an den Bildschirm, in eine Datei oder an den Drucker anzuzeigen.

Weitere Informationen:

[So zeigen Sie ein Dialogfeld an \(nur UNIX\)](#) (siehe Seite 539)

Der Berichtsbefehl

Um einen Bericht von der Befehlszeile in UNIX zu generieren, müssen Sie den CA SDM-Berichtsbefehl verwenden:

```
pdm_task report [-h][-e][-f][-F ffstring][-p pagelength] filename [command-line arguments]
```

Hinweis: Dem Berichtsbefehl geht der Befehl "pdm_task" voraus, der erforderliche Umgebungsvariablen festlegt. Wenn der Bericht so ausgerichtet ist, dass er Befehlszeilenargumente akzeptiert, müssen Sie ein Befehlszeilenargument für jedes Argument in der Berichtsvorlage eingeben.

Verwenden Sie unter Windows den Befehl „rpt_srv“:

```
rpt_srv Berichtstitel
```

Das folgende Beispiel enthält die drei Befehlszeilenargumente ("Smith", "Jane" und "L"), die für den Bericht über betroffene Kontakte benötigt werden, der im Berichtsvorlagenbeispiel weiter oben in diesem Abschnitt beschrieben wurde:

```
pdm_task report /reports/myrpt.rpt Smith Jane L
```

Wenn ein Argument leer ist, müssen Sie eine NULL-Zeichenfolge verwenden. Wenn z. B. Jane Smith über keinen zweiten Vornamen verfügt, lautet die Syntax folgendermaßen:

```
pdm_task report /reports/myrpt.rpt Smith Jane ""  
rpt_srv \reports\myrpt.rpt Smith Jane L
```

So zeigen Sie ein Dialogfeld an (nur UNIX)

Sie können den Parameter zum Umleiten von Berichtsausgaben (rptuiDsp) in die Berichtsbefehle einschließen, um ein Dialogfeld anzuzeigen. In dem Dialogfeld sind Optionen zum Drucken des Berichts in eine Datei, zum Anzeigen des Berichts in einem Xterm-Fenster oder zum Senden des Berichts an den Drucker verfügbar.

Beispiel:

```
pdm_task rptuiDsp report /reports/myrpt.rpt Smith Jane L
```

Im folgenden Beispiel wird der Titel „Inventarbericht“ zum Dialogfeld hinzugefügt:

```
pdm_task rptuiDsp report /reports/myrpt.rpt Smith Jane L "title:Inventarbericht"
```

Berichtsvorlagenreferenz

Sie können veränderliche Ausdrücke, Funktionen, und Anweisungen in einer Berichtsvorlage benutzen.

Variable Ausdrücke für Berichtsvorlagen

Veränderliche Ausdrücke definieren die Daten, die in einer Reportvorlage gedruckt oder angezeigt werden. Sie werden in ein Layout oder eine BLOCK-Anweisung eingeschlossen.

Syntax der veränderlichen Ausdrücke

Syntax gibt die Regeln an, die die Bildung der Anweisungen in einer Programmiersprache definieren. Die Struktur dieser Zeichenfolge lautet folgendermaßen:

Variablenname = *Ausdruck* [*Markierungen*]

Markierungen der veränderlichen Ausdrücke

Markierungen formatieren die Ergebnisse von variablen Ausdrücken. Verwenden Sie die folgenden Markierungen zum Formatieren von Textfeldern:

MULTILINE

Verwendet für die Anzeige mehrere Zeilen anstatt Text abzukürzen.

RIGHT

Richtet rechtsbündig aus.

Verwenden Sie die folgenden Markierungen zum Formatieren von numerischen Feldern:

BLANKZERO

Fungiert als "null-value"-Feld, in dem keine Null gedruckt wird.

BOOL

Konvertiert Null zu "no" und ungleich- Null zu "yes".

REAL

Wird als Gleitkomma angezeigt (Standardwert ist eine Ganzzahl).

ZEROFILL

Zeigt führende oder vorangestellte nullen

Verwenden Sie die folgenden Markierungen, um Datums- und Uhrzeitfelder zu formatieren:

DATUM

Zeigt nur das Datum an.

DAYS

Zeigt die Zeitdauer in Tagen an.

HOURS

Zeigt die Zeitdauer in Stunden an.

MINUTES

Zeigt die Zeitdauer in Minuten an.

SECONDS

Zeigt die Zeitdauer in Sekunden an.

TIME

Zeigt nur die Uhrzeit an.

Beispiel für veränderliche Ausdrücke

Folgende Zeile zeigt ein Beispiel für veränderliche Ausdrücke an:

```
desc = description MULTILINE
```

Anmerkungen zu veränderlichen Ausdrücken

Variablenamen müssen innerhalb von BLOCK-Anweisungen einmalig sein und dürfen keinem Spaltennamen in der SELECT-Klausel für den Block entsprechen. Variablenamen dürfen in unterschiedlichen BLOCK-Anweisungen wiederholt werden, jedoch nicht in derselben BLOCK-Anweisung.

Befolgen Sie diese Syntaxregeln, wenn Sie in Ihre Berichtsvorlage Ausdrücke einschließen:

- Verwenden Sie beliebige gültige C-Ausdrücke.
- Schließen Sie Variablen- und Spaltennamen nicht in Anführungszeichen ein.
- Schließen Sie Zeigenfolgekonstanten in einzelne oder doppelte Anführungszeichen ein.
- Sie können auf einen verschachtelten Block verweisen, der jedoch nur genau eine Zeile enthalten darf.
- Um einen Spaltennamen einzuschließen, der einem Schlüsselwort entspricht, stellen Sie dem Spaltennamen ein Backslash-Zeichen (\) voran. So ist z. B. ALIAS ein Schlüsselwort, während \alias ein Spaltenname ist.
- Verwenden Sie ein Dollarzeichen (\$), um auf Umgebungsvariablen (z. B. \$name) und auf Befehlszeilenargumente (z. B. \$n, wobei n der Position des Arguments in der Befehlszeile entspricht) zu verweisen.
- Um die Anzahl an Befehlszeilenargumenten anzugeben, verwenden Sie \$#. Der folgende Ausdruck bedeutet beispielsweise, dass das zusätzliche Argument als Argument verwendet wird, wenn die Anzahl an Befehlszeilenargumenten größer als eins ist. Stellen Sie andernfalls den Wert des Arguments auf eine leere Zeichenfolge ein. Die Berichtsvorlage selbst gilt als Befehlszeilenargument. Deshalb beträgt die Anzahl an Argumenten wenigstens eins.

```
$# > 1 ? $1 : "
```

- Verwenden Sie ##, um zwei Zeichenfolgen zu verketteten. Beispiel:

```
title = "This is the " ## "first line. "
```

```
long_name = fn
```

```
irst_name ## last_name
```

- Folgendes wird unterstützt:
 - (number)
 - (string)
 - (date_time)
 - (duration)
- Um in einem anderen Block auf einen Variablen- oder Spaltennamen zu verweisen, stellen Sie dem Namen den Blocknamen oder zwei Doppelpunkte voran. Beispiel:
blockname::column | variable-name

Berichtsvorlagenfunktionen

Sie können in Berichtsvorlagen die folgenden Funktionen verwenden:

is_null (*expr*)

Diese Funktion gibt „wahr“ zurück, wenn der Ausdruck den Wert „Null“ aufweist.

```
false = 0
true = is_null (false)
```

sqrt (*expr*)

Diese Funktion berechnet die Quadratwurzel des Ausdrucks.

```
nine = 9
three = sqrt (nine)
```

pow (*expr1*, *expr2*)

Diese Funktion potenziert *expr1* mit *expr2*.

```
two = 2
false = 3
eight = pow (two,three)
```

log (*expr*, *expr*)

Diese Funktion berechnet den natürlichen Logarithmus des Ausdrucks.

```
ten = 10
result = log (ten)
```

catname (*expr*, *expr*, *expr*)

Hiermit werden drei Zeichenfolgen, die den Namen eines Kontakts darstellen, gemäß der Regeln in der Feldformatdatei zu einer Zeichenfolge mit Kommata verkettet.

```
last = "Murphy"
first = "Fred"
middle = "P"
contact_name=catname (last, first, middle)
```

strlen (*Zeichenfolge*)

Diese Funktion gibt die Länge der Zeichenfolge zurück.

```
buffer = "A thirty character long string"
thirty = strlen(buffer)
```

strindex (string, pattern [, start_index])

Diese Funktion gibt den Index der ersten Musterübereinstimmung oder der nächsten Musterübereinstimmung nach start_index in der Zeichenfolge zurück. Gibt "-1" zurück, wenn keine Übereinstimmung vorliegt.

```
buffer = "A thirty character long string"
```

```
zero = strindex(buffer, " [A-Z] ")
```

```
two = strindex(buffer, " [a-z] ")
```

substr (string, pattern [, length])

Diese Funktion gibt den Teil der Zeichenfolge nach der ersten Musterübereinstimmung zurück. Die Länge ist definiert und begrenzt die Länge der Ausgabezeichenfolge. Gibt eine Zeichenfolge mit der Länge null zurück, wenn keine Übereinstimmung gefunden wird.

```
buffer = "A thirty character long string"
```

```
last_word = substr(buffer, " [a-z]*$ ")
```

```
first_capital_letter = substr(buffer, " [A-Z] ",
```

```
1)
```

substr (string, index [, length])

Diese Funktion gibt den Teil der Zeichenfolge nach dem Index zurück. Ihre Länge ist definiert und beschränkt die Länge der Ausgabezeichenfolge. Gibt eine Zeichenfolge mit der Länge null zurück, wenn keine Übereinstimmung gefunden wird.

```
buffer = "Summary: The network card displays a
```

```
code of ... "
```

```
summary = substr(buffer, 9)
```

```
30_char_summary = strindex(buffer, 9, 30)
```


Die verbleibenden Funktionen (Pseudofunktionen) werden für Datenblöcke und nicht für variable Ausdrücke verwendet. Diese Funktionen werden für gewöhnlich in BLOCK-Anweisungen eingefügt, um Informationen über die Daten von verschachtelten BLOCK-Anweisungen abzurufen.

count (*block-name*)

Gibt die Anzahl an Zeilen in dem Block zurück, der in der BLOCK-Anweisung angegeben ist. Bei dem Block-namen muss es sich um eine einfache Zeichenfolge handeln.

```
BLOCK sample ("SELECT id FROM Contact") {  
  entries = count (sample)  
}
```

sum (*block-name, expr*)

Führt den Ausdruck für jede Zeile des angegebenen Blocks aus und summiert das Ergebnis.

```
BLOCK sample ("SELECT actual_cost, est_cost FROM Change_Request") {  
  difference = sum (sample, est_cost-actual_cost)  
}
```

average (*block-name, expr*)

Führt den Ausdruck für jede Zeile des Blocks aus und gibt den Durchschnittswert des Ergebnisses zurück.

```
BLOCK sample ("SELECT actual_cost, est_cost FROM Change_Request"){  
  avg_difference = average (sample, est_cost-actual_cost)  
}
```

prev (*expr*)

Gibt den vorherigen Wert des Ausdrucks zurück. Diese Funktion muss mit Sorgfalt verwendet werden, damit der letzte Wert nicht fälschlicherweise überschrieben wird.

downtime (*sla_schedule, expr1, expr2 [, delay-block, expr, expr]*)

Ruft eine Berechnung der SLA-Ausfallzeit auf. Das erste Argument muss eine Zeichenfolge sein, die eine Arbeitsschicht identifiziert. Die anderen Argumente entsprechen der Start- und Endzeit:

expr1 gibt das Startdatum und die Startzeit des Ereignisses an.

expr2 gibt das Enddatum und die Endzeit des Ereignisses an.

Im folgenden Beispiel ruft die BLOCK-Anweisung "wrkshft" den Ablaufplan der Schichten und die BLOCK-Anweisung "evt_dly" die Verspätungen ab, während die downtime-Funktion diese Datensätze verwendet, um die Ausfallzeit zu berechnen.

```
BLOCK attev ("SELECT start_time, fire_time, event_tmpl, obj_id FROM
Attached_Events")

{
BLOCK evt ("SELECT persid, sym, work_shift FROM Events ", "WHERE persid = ?",
attev::event_tmpl) {}
BLOCK wrkshft ("SELECT sched FROM Bop_Workshift", "WHERE persid = ?",
evt::work_shift) {}

BLOCK evt_dly ("SELECT start_time, stop_time FROM Event_Delay", "WHERE obj_id =
?", attev::obj_id) {}
total_downtime = downtime(wrkshft::sched,
attev::start_time, attev::fire_time,
evt_dly,
evt_dly::start_time, evt_dly::stop_time);
}
```

deref (column-name)

Gibt die Zeichenfolgendarstellung des Zeigers an, indem eine automatische Suche in der entsprechenden Tabelle ausgeführt wird.

```
BLOCK chg ("SELECT organization FROM Change_Request") {
org = deref (organization)
}
```

Da diese Pseudofunktion Suchläufe einschließt, ist sie nur gültig, wenn sie als einziges in dem Ausdruck angegeben ist. Folgendes ist z. B. gültig:

```
model = deref (nr_model)
```

Folgendes ist demgegenüber nicht gültig:

```
model = "model" ## deref (nr_model)
```

Hinweis: Vorwärtsverweise auf Variablen oder Blöcke ist nicht zulässig.

BLOCK-Anweisungen für Berichtsvorlagen

Mit Blockanweisungen werden die Datenbanktabellen, aus denen Daten abgerufen werden, definiert. Sie können Aktionen enthalten, die an den abgerufenen Daten ausgeführt werden sollen.

Syntax der BLOCK-Anweisungen

Syntax gibt die Regeln an, die die Bildung der Anweisungen in einer Programmiersprache definieren. Die Struktur dieser Zeichenfolge für BLOCK lautet folgendermaßen:

```
BLOCK blockname (
    "SELECT [ALIAS,] field_name[, field_name ...]
    FROM table_name[, table_name ...] "
    [,"WHERE where_clause"][, arguments,] )
    [SORT "sort clause"]
{
output program statements
}
```

Parameter der BLOCK-Anweisungen

blockname

Identifiziert den Block. Jeder *blockname* muss einmalig sein.

SELECT-Klausel

Folgt auf *blockname* und wird von Anführungszeichen begrenzt. Listet die Spalten auf, aus denen Daten abgerufen werden, gefolgt von dem Schlüsselwort FROM, gefolgt von den Tabellen, aus denen die Spalten abgerufen werden. Diese Klausel ist erforderlich. Es folgt ein Beispiel, in dem drei Tabellen angegeben sind:

```
"SELECT open_date, chg_ref_num \
last_name, first_name \
FROM Change_Request, \
ca_contact"
```

Sie können keinen SQL-Alias einschließen. Beispiel:

```
"SELECT open_date As OpenDate"
```

WHERE-Klausel

(Optional) Folgt auf die SELECT-Klausel und qualifiziert die Informationen weiter. Dies kann eine Zeigenfolgekonstant oder ein Ausdruck sein, die eine Zeichenfolge bewertet. Wenn die WHERE-Klausel eine leere Zeichenfolge ist, werden alle Datensätze zurückgegeben. WHERE-Klauseln können Ersatzargumente enthalten, die auf Variablen oder Befehlszeilenargumente verweisen und die Syntax eines Fragezeichens (?) verwenden. So kann z. B. die folgende WHERE-Klausel auf die vorausgegangene SELECT-Klausel folgen:

```
"WHERE #Change_Request.open_date >= ? \
AND #Change_Request.active_flag = 1 \
AND #ca_contact.last_name = ? ", $1"
```

Hinweis: Die WHERE-Klausel muss von der SELECT-Klausel getrennt sein, da die WHERE-Klausel ein Ausdruck sein kann, der eine Zeichenfolge bewertet, während die SELECT-Klausel ausschließlich eine Zeichenfolgenkonstante ist. Dadurch erhalten Sie mehr Flexibilität und weitere Möglichkeiten zur Bearbeitung von Daten für die Erstellung Ihres Berichts.

SORT-Klausel

Folgt optional den SELECT- und den WHERE-Klauseln und sortiert die abgerufenen Datenzeilen. Die SORT-Klausel ist wie die SQL ORDER BY-Klausel formatiert. Beispiel:

```
SORT "open_date"
```

Anweisungen für das Ausgabeprogramm

Steuert die Ausführung des Berichts. Wenn sie eingeschlossen ist, druckt die HEADER-Anweisung vor der Datenabfrage den Kopfzeilentest für den Block. Danach wird die Datenabfrage ausgeführt. Werden Daten zurückgegeben, werden die Anweisungen mit einer Ausnahme in der Reihenfolge ausgeführt, in der sie geschrieben wurden. Blockfunktionen wie sum und average verhalten sich so, als ob sie sich am Ende des Ausgabeprogramms befinden. Ihre Werte sind tatsächlich erst dann stabil, wenn die Ausführung für den nächsten Datensatz beginnt.

Wichtig! Das Ausgabeprogramm hängt vom Erfolg der Datenabfrage ab. Wenn die Abfrage keine Daten zurückgibt, wird das Ausgabeprogramm mit Ausnahme der HEADER-Anweisung nicht ausgeführt.

Beispiel für BLOCK-Anweisung

Bei dieser BLOCK-Anweisung wird angenommen, dass ein Argument übergeben wird, das eine Ganzzahl gleich der Priorität des Change enthält. Die WHERE-Klausel überprüft zunächst die Anzahl der übergebenen Argumente (\$#). Wenn ein Argument verfügbar ist, wird es für die Bewertung des Ausdrucks verwendet, um die WHERE-Klausel zu erstellen. Andernfalls wird eine leere WHERE-Klausel ersetzt („“).

```
BLOCK chg ("SELECT priority FROM Change_Request",  
$# > 1 ? "WHERE priority =" ## $1 : "" ) {}
```

Beispiel für FOOTER-Anweisung

Folgende Zeilen zeigen ein Beispiel für eine FOOTER-Anweisung an:

```
FOOTER {  
    Zusammenfassung – Informationen:  
        Total Failures: [Fail_count >  
        Total Downtime: [Downtime >  
}
```

Anmerkungen zur BLOCK-Anweisung

HEADER, HEADER2, FUSSZEILE, DRUCK und veränderliche Ausdrücke können in geschweifte Klammern gestellt werden. Alle Anweisungen werden für jede ausgewählte Zeile ausgeführt.

Hinweis: PAGE HEADER- und PAGE FOOTER-Anweisungen können nicht in BLOCK-Anweisungen eingefügt werden.

FOOTER-Anweisungen für Berichtsvorlagen

Diese Layoutanweisung fügt Informationen am Ende von Berichtsabschnitten ein.

Syntax der FOOTER-Anweisung

Syntax gibt die Regeln an, die die Bildung der Anweisungen in einer Programmiersprache definieren. Die Struktur dieser Zeichenfolge für FOOTER lautet folgendermaßen:

```
FOOTER {parameters}
```

Parameter der FOOTER-Anweisung

Die Parameter lauten folgendermaßen:

CD

Eine vordefinierte Variable, die zur Anzeige des aktuellen Datums verwendet wird.

CT

Eine vordefinierte Variable, die zur Anzeige der aktuellen Uhrzeit verwendet wird.

PG

Eine vordefinierte Variable, die zur Anzeige der aktuellen Seitenzahl verwendet wird.

column | variable-name

Dieses Feld kann eine Variable von einem früheren variablen Ausdruck oder ein Verweis auf eine Spalte in der SQL-Klausel einer BLOCK-Anweisung sein.

literal-text

Jeder Text, der keine vordefinierte Variable oder ein Spalten- oder Variablenname ist, wird als Text interpretiert. Text, den Sie in der FOOTER-Anweisung einschließen, wird genau an der Position angezeigt, an der Sie ihn einfügen.

Anmerkungen zur FOOTER-Anweisung

FOOTER-Anweisungen werden am unteren Rand von Berichtsabschnitten gedruckt. Eine typische Verwendung ist die Darstellung von Zusammenfassungen oder Statistiken. Sie können FOOTER-Anweisungen in BLOCK-Anweisungen einschließen.

Der Inhalt eines Felds nimmt genau den Platz ein, der durch die eckigen Klammern angegeben wird. Alle überflüssigen Zeichen werden gekürzt. Sie können ein Feld jedoch mit einer spitzen Klammer (>) schließen, um zuzulassen, dass sein Inhalt sich in seiner Gesamtheit zum rechten Rand hin ausdehnt.

Um auf eine Variable oder einen Spaltennamen in einer anderen BLOCK-Anweisung zu verweisen, verwenden Sie folgende Syntax:

```
blockname::column | variable-name
```

HEADER-Anweisungen für Berichtsvorlagen

Diese Layoutanweisung fügt Informationen am Anfang von Berichtsabschnitten ein.

Syntax der HEADER-Anweisung

Syntax gibt die Regeln an, die die Bildung der Anweisungen in einer Programmiersprache definieren. Die Struktur dieser Zeichenfolge für HEADER lautet folgendermaßen:

```
HEADER {parameters}
```

Parameter der HEADER-Anweisung

Eine Liste der zulässigen Parameter für diese Anweisung finden Sie zusammen mit Erläuterungen unter "[PAGE HEADER-Anweisungen für Berichtsvorlagen](#)" (siehe Seite 553)".

Beispiel der HEADER-Anweisung

Folgende Zeilen zeigen ein Beispiel für eine HEADER-Anweisung an:

```
HEADER {  
    Kontakt – Übersichtsbericht  
    Kontaktname   Kontakt-Alias   Organisation  
}
```

Anmerkungen zur HEADER-Anweisung

HEADER werden am Anfang von Berichtsabschnitten gedruckt und können in BLOCK-Anweisungen eingeschlossen werden. HEADER werden üblicherweise verwendet, um Abschnitt- und/oder Spaltenüberschriften darzustellen.

Der Inhalt eines Felds nimmt genau den Platz ein, der durch die eckigen Klammern angegeben wird. Alle überflüssigen Zeichen werden gekürzt. Sie können ein Feld jedoch mit einer spitzen Klammer (>) schließen, um zuzulassen, dass sein Inhalt sich in seiner Gesamtheit zum rechten Rand hin ausdehnt.

Hinweis: Wenn die Druckanweisung für eine MULTILINE-Variable mit einer spitzen Klammer rechts (>) geschlossen wird, werden die Zeichen an einem Leerzeichen umgebrochen, um innerhalb des Feldes zu bleiben, das durch die linke eckige Klammer ([) und die rechte spitze Klammer (>) definiert wurde. Auch wenn die Variable nicht MULTILINE ist, werden durch die spitze Klammer rechts (>) alle Daten, unabhängig von ihrer Länge, in der aktuellen Zeile angezeigt.

Um auf eine Variable oder einen Spaltennamen in einer anderen BLOCK-Anweisung zu verweisen, verwenden Sie folgende Syntax:

blockname::column | variable-name

HEADER2-Anweisungen für Berichtsvorlagen

Diese Layoutanweisung fügt HEADER-Informationen des jeweiligen Berichtsabschnitts oben auf jeder folgenden Seite ein, wenn sich der Berichtsabschnitt über mehrere Seiten erstreckt.

Syntax der HEADER2-Anweisung

Syntax gibt die Regeln an, die die Bildung der Anweisungen in einer Programmiersprache definieren. Die Struktur dieser Zeichenfolge für HEADER2 lautet folgendermaßen:

HEADER2 {*parameters*}

Parameter der HEADER2-Anweisung

Eine Liste der zulässigen Parameter für diese Anweisung finden Sie zusammen mit Erläuterungen unter "[HEADER2-Anweisungen für Berichtsvorlagen](#)" (siehe Seite 551)".

Beispiel der Header2-Anweisung

```
HEADER2 {  
    Kontakt – Übersichtsbericht (Fortsetzung)  
    Kontaktname    Kontakt-Alias    Organisation  
}
```

Anmerkungen zur Header2-Anweisung

HEADER2-Anweisungen können in BLOCK-Anweisungen eingeschlossen werden.

Der Inhalt eines Felds nimmt genau den Platz ein, der durch die eckigen Klammern angegeben wird. Alle überflüssigen Zeichen werden gekürzt. Sie können ein Feld jedoch mit einer spitzen Klammer (>) schließen, um zuzulassen, dass sein Inhalt sich in seiner Gesamtheit zum rechten Rand hin ausdehnt.

Um auf eine Variable oder einen Spaltennamen in einer anderen BLOCK-Anweisung zu verweisen, verwenden Sie folgende Syntax:

blockname::column | variable-name

PAGE FOOTER-Anweisungen für Berichtsvorlagen

Diese Layoutanweisung fügt Informationen unten auf jeder Berichtsseite ein.

Syntax der PAGE FOOTER-Anweisung

PAGE FOOTER {*parameters*}

Parameter der PAGE FOOTER-Anweisung

Mit der Ausnahme, dass Sie keine Spalten- und Variablennamen verwenden können, sind die Parameter für diese Anweisung genau dieselben wie für FOOTER. Eine Liste der zulässigen Parameter für diese Anweisung finden Sie zusammen mit Erläuterungen unter [PAGE FOOTER-Anweisungen für Berichtsvorlagen](#) (siehe Seite 552).

Beispiel für eine PAGE FOOTER-Anweisung

```
PAGE FOOTER {  
    Page Number: [PG>  
}
```

Anmerkungen zu Parametern für eine PAGE FOOTER-Anweisung

Der Inhalt eines Felds nimmt genau den Platz ein, der durch die eckigen Klammern angegeben wird. Alle überflüssigen Zeichen werden gekürzt. Sie können ein Feld jedoch mit einer spitzen Klammer (>) schließen, um zuzulassen, dass sein Inhalt sich in seiner Gesamtheit zum rechten Rand hin ausdehnt.

Um auf eine Variable oder einen Spaltennamen in einer anderen BLOCK-Anweisung zu verweisen, verwenden Sie folgende Syntax:

blockname::column | variable-name

PAGE HEADER-Anweisungen für Berichtsvorlagen

Diese Layoutanweisung fügt Informationen oben auf jeder Berichtsseite ein.

Syntax der PAGE HEADER-Anweisung

Syntax gibt die Regeln an, die die Bildung der Anweisungen in einer Programmiersprache definieren. Die Struktur dieser Zeichenfolge für PAGE HEADER lautet folgendermaßen:

```
PAGE HEADER {parameters}
```

Parameter der PAGE HEADER-Anweisung

Mit der Ausnahme, dass Sie keine Spalten- und Variablennamen verwenden können, sind die Parameter für diese Anweisung genau dieselben wie für FOOTER. Eine Liste der zulässigen Parameter für diese Anweisung finden Sie zusammen mit Erläuterungen unter [PAGE FOOTER-Anweisungen für Berichtsvorlagen](#) (siehe Seite 552).

Beispiel der PAGE HEADER-Anweisung

```
PAGE HEADER {  
    Date of Report: [CD>  
    Time of Report: [CT>  
}
```

Anmerkungen zur PAGE HEADER-Anweisung

PAGE HEADER werden oben auf jeder Berichtsseite gedruckt. Sie können zwar an einem beliebigen Punkt in der Berichtsvorlage definiert, aber nicht in eine BLOCK-Anweisung eingeschlossen werden.

Der Inhalt eines Felds nimmt genau den Platz ein, der durch die eckigen Klammern angegeben wird. Alle überflüssigen Zeichen werden gekürzt. Sie können ein Feld jedoch mit einer spitzen Klammer (>) schließen, um zuzulassen, dass sein Inhalt sich in seiner Gesamtheit zum rechten Rand hin ausdehnt.

Um auf eine Variable oder einen Spaltennamen in einer anderen BLOCK-Anweisung zu verweisen, verwenden Sie folgende Syntax:

```
blockname::column | variable-name
```

PRINT-Anweisungen für Berichtsvorlagen

Diese Layoutanweisung fügt Daten in einen Berichtsabschnitt ein.

Syntax der PRINT-Anweisung

Syntax gibt die Regeln an, die die Bildung der Anweisungen in einer Programmiersprache definieren. Die Struktur dieser Zeichenfolge für PRINT lautet folgendermaßen:

```
PRINT {parameters}
```

Parameter der PRINT-Anweisung

Eine Liste sowie Erklärungen zu den gültigen Parametern für diese Anweisung finden Sie unter FOOTER.

Beispiel für eine PRINT-Anweisung

```
PRINT {  
[num ] [desc          ] [pr]  [stat] [catgry] [asgn          ]  
}
```

Anmerkungen zur PRINT-Anweisung

Fügen Sie die PRINT-Anweisung an der Stelle ein, an der die Daten für einen Berichtsabschnitt in dem Bericht angezeigt werden sollen. Sie können PRINT-Anweisungen in BLOCK-Anweisungen einschließen.

Der Inhalt eines Felds nimmt genau den Platz ein, der durch die eckigen Klammern angegeben wird. Alle überflüssigen Zeichen werden gekürzt. Sie können ein Feld jedoch mit einer spitzen Klammer (>) schließen, um zuzulassen, dass sein Inhalt sich in seiner Gesamtheit zum rechten Rand hin ausdehnt.

Hinweis: Wenn die Druckanweisung für eine MULTILINE-Variable mit einer spitzen Klammer rechts (>) geschlossen wird, werden die Zeichen an einem Leerzeichen umgebrochen, um innerhalb des Feldes zu bleiben, das durch die linke eckige Klammer ([) und die rechte spitze Klammer (>) definiert wurde. Auch wenn die Variable nicht MULTILINE ist, werden durch die spitze Klammer rechts (>) alle Daten, unabhängig von ihrer Länge, in der aktuellen Zeile angezeigt.

Um auf eine Variable oder einen Spaltennamen in einer anderen BLOCK-Anweisung zu verweisen, verwenden Sie folgende Syntax:

```
blockname::column | variable-name
```

Anpassen von Crystal Reports

Bevor Sie einen der aufgeführten Berichte anzeigen können, gelten die folgenden Bedingungen:

- Crystal Reports müssen für den Crystal Report Selector verfügbar sein. Kopieren Sie sie deshalb in das Crystal-Verzeichnis "\$NX_ROOT/bopcfg/rpt".
- Ihr Datenbankclient muss aktiviert sein und ausgeführt werden, d. h. die Verbindung zum Datenbankserver auf demselben oder einem anderen Rechner muss aufgebaut sein. Wenn Sie zum Ausführen von Crystal Reports oder Access-Berichten einen CA SDM-Client verwenden, muss ein Datenbankclient für die spezifische Datenbank installiert und mit dem Datenbankserver verbunden sein, damit diese Berichte ausgeführt werden können.

Nachdem Sie anwenderspezifische Crystal Reports erstellt haben, führen Sie folgende Schritte aus:

1. Kopieren Sie anwenderspezifische Crystal Reports in das folgende Crystal-Verzeichnis:
`$NX_ROOT/bopcfg/rpt`
2. Fügen Sie die Dateinamen der anwenderspezifischen Crystal Reports zur folgenden Konfigurationsdatei hinzu:
`crystal.cfg`

Sie können dann auf die Crystal Reports zugreifen, indem Sie in der Task-Leiste auf „Start“ klicken und anschließend „Berichterstellung“, „Service Desk-Berichterstellung (Crystal Reports)“ aus dem CA SDM-Menü wählen (das über das Menü „Programme“ aufgerufen werden kann). Das Fenster für die Service Desk-Berichterstellung (Crystal) wird angezeigt.

Wichtig! CA SDM-Clients können nicht aktualisiert werden. Wenn Sie also Crystal Reports auf dem CA SDM-Server erstellen und verwenden und später einmal Ihre CA SDM-Version aktualisieren möchten, müssen Sie alle anwenderspezifischen Berichte in ein anderes Verzeichnis kopieren, damit sie nicht verloren gehen. Nach der Aktualisierung können Sie die Berichte zurück in das Crystal-Verzeichnis "\$NX_ROOT/bopcfg/rpt" kopieren und die Datei "crystal.config" ändern, so dass Report Selector auf sie zugreifen kann.

Kapitel 10: Füllen von CA CMDB

Dieses Kapitel enthält folgende Themen:

[Füllen der Datenbank](#) (siehe Seite 557)

[Füllen der Datenbank durch GRLoader](#) (siehe Seite 557)

[Importieren von Daten mit GRLoader](#) (siehe Seite 558)

[Familien- und Klassenzuweisungen](#) (siehe Seite 558)

[Laden von CA APM-Daten](#) (siehe Seite 559)

Füllen der Datenbank

Sie müssen die CMDB mit CIs und Beziehungen Ihrer IT-Infrastruktur füllen, um die Anwendung effektiv nutzen zu können. Sie können die CMDB manuell mit Daten füllen, indem Sie den integrierten Configuration Item-Editor, GRLoader, verwenden, oder indem Sie Elemente aus anderen Asset-Verwaltungstools importieren.

Hinweis: Weitere Informationen zum CI-Editor finden Sie in der *Online-Hilfe*.

Füllen der Datenbank durch GRLoader

Führen Sie folgende Aufgaben durch, um die Datenbank durch das Laden von CIs und Beziehungen aufzufüllen:

1. Konvertieren Sie Eingabedaten, die Informationen über CIs und deren Beziehungen enthalten, in XML oder in eine Kalkulationstabelle.
2. Das CA CMDB-GRLoader-Programm verwendet die XML-Daten als Eingabe.
3. GRLoader lädt die Daten in die Datenbank.

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

Weitere Informationen:

[Importieren von Daten mit GRLoader](#) (siehe Seite 558)

Importieren von Daten mit GRLoader

Importieren Sie Daten, indem Sie das in CA SDM enthaltene Programm "GRLoader" verwenden, das CIs erstellt, die auf Daten in einer XML-Datei oder Excel-Kalkulationstabelle basieren.

Gehen Sie wie folgt vor:

1. Wählen Sie im Menü "Start" die Option "Ausführen".
2. Geben Sie **cmd** ein.

Ein DOS-Eingabefenster wird geöffnet.

3. Geben Sie folgenden Befehl ein:

```
Grloader -u <username> -p <password> -s http://<ca_sdm_servername>:8080  
-i <xml_document or spreadsheet>
```

GRLoader erstellt unter Verwendung der Daten in der XML-Datei CIs. Wenn während dieses Vorgangs Fehler gefunden werden, wird eine Fehlerdatei erstellt, in der die CIs aufgelistet werden, die nicht importiert werden konnten, sowie die Ursache des Problems.

Der GRLoader-Import ist abgeschlossen.

4. Starten Sie CA SDM, und überprüfen Sie, ob die CI-Daten korrekt eingefüllt wurden.
5. Starten Sie CMDB Visualizer, um zu überprüfen, ob die Beziehungsdaten korrekt eingefüllt wurden.

Die Daten sind importiert und verifiziert.

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

Familien- und Klassenzuweisungen

Wenden Sie ein Klassifizierungsschema auf jedes CI an. Mit diesem Schema werden jedem CI die folgenden Attribute zugewiesen:

- Familie – eine Auflistung von CIs, die ähnliche Attribute haben
- Klasse – eine Untergruppe von CIs innerhalb einer Familie

Sie können Zuweisungen folgendermaßen erstellen:

- Füllen Sie Herstellerdaten auf, die für jedes Hardware-Asset die Familie und Klasse angeben.
- Fügen Sie in den entsprechenden Spalten der Eingabedatei nicht leere Werte für Familie und Klasse ein.

Der GRLoader importiert kein CI, das beim Laden die Familie und Klasse nicht zu einer vorhandenen Familie und Klasse auflösen kann.

Laden von CA APM-Daten

Die Eingabe in das Ladeprogramm CA Asset Portfolio Management (CA APM) besteht in erster Linie in einer Tabelle oder Ansicht, die einen Auszug der zu importierenden CA APM-Daten enthält. Diese Daten sind in einer Datenbanktabelle oder Ansicht mit dem Namen "CMDB_Export_Asset_Data" enthalten. In einigen Fällen befinden sich die Daten, die in die MDB importiert werden sollen, in der gleichen Datenbank wie das Ziel. Häufig sind die zu importierenden Daten jedoch in einer anderen Datenbank abgelegt, zum Beispiel beim Importieren von Daten von Tochtergesellschaften. In beiden Fällen müssen Sie eine Ansicht in der Datenbank erstellen, in der sich auch die Quelldaten befinden.

Die Ansicht der CA APM-Daten beinhaltet nicht die Attribute "family" und "class" und kommt möglicherweise aus einem System mit einem anderen Klassifizierungsschema. Wenn die Quelle der Asset-Daten zum Beispiel ein anderes Unternehmen ist, kann ein anderes Klassifizierungssystem gelten.

Die Tabelle "CA_MODEL_DEF" beinhaltet eine Liste von Modellen, die mit den Daten in "CMDB_Export_Asset_Data" verglichen werden. Wenn es eine Übereinstimmung gibt, werden die Familie und Klasse des Modells dem zu importierenden Asset zugewiesen. Gibt es keine Übereinstimmung, müssen Sie ein neues Modell für das Asset definieren. Es empfiehlt sich, entweder Einträge aus der Quelltable "CA_MODEL_DEF" in die Ziel-MDB zu kopieren, oder die Tabelle "CA_MODEL_DEF" mit Einträgen für alle neuen Hardwarekomponenten und Modellnummern zu aktualisieren.

Kapitel 11: Benutzen des MDR Launcher

Dieses Kapitel beschreibt das Definieren von MDRs, Importieren von Daten, Zuordnen von Cls zu ihrer Quelle und Anzeigen von föderierten Daten für ein CI.

Dieses Kapitel enthält folgende Themen:

[Der MDR Launcher](#) (siehe Seite 562)

[MDR-Terminologie](#) (siehe Seite 563)

[MDR-Zuordnung](#) (siehe Seite 564)

[Starten von MDR](#) (siehe Seite 564)

[CMDBf Viewer](#) (siehe Seite 565)

[Definieren eines MDR für CA CMDB](#) (siehe Seite 565)

[Zusammenschlüsse unter Verwendung von GRLoader](#) (siehe Seite 574)

[Zuordnen zwischen MDR-ClS und CA CMDB-ClS](#) (siehe Seite 576)

[Konfigurieren von MDRs für CMDBf Viewer](#) (siehe Seite 578)

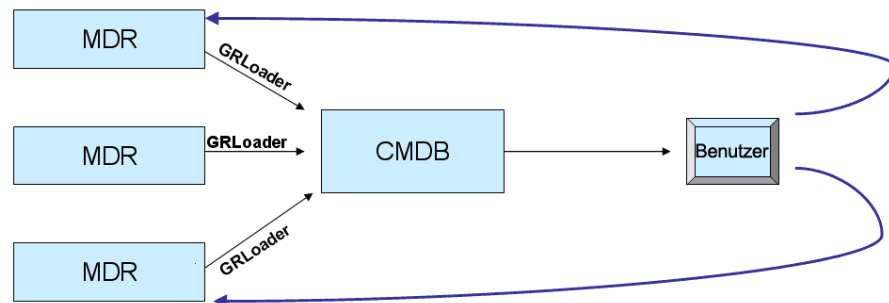
[Starten der MDR-Webbrowser-Schnittstelle](#) (siehe Seite 578)

[Integration von CA Cohesion](#) (siehe Seite 579)

Der MDR Launcher

Einer der Hauptgründe für die Implementierung einer CA CMDB besteht in der Zusammenfassung von Daten aus verschiedenen Datenquellen (MDRs genannt). Ein CI muss jedoch stets eine Referenz enthalten, die auf seinen MDR-Ursprung zurückverweist.

CA CMDB umfasst Funktionen zum Importieren und Laden von CIs und zur Verbindung der CIs mit ihrem Ursprung. Darüber hinaus können Sie, wie im folgenden Diagramm dargestellt, mühelos zurück in das System navigieren, aus dem das CI stammt, wenn Sie CIs in der CA CMDB mit MDR Launcher anzeigen.



Wenn Sie mit MDR Launcher arbeiten, können Sie geschlossene Change Management-Prozesse wie den folgenden implementieren:

1. Erstellen Sie einen Change-Datensatz.
2. Implementieren Sie die Änderung.
3. Prüfen Sie die Änderung, indem Sie die MDR-Quelle überprüfen.
4. Aktualisieren Sie die CMDB, um die Änderung anzuzeigen.

In Bezug auf den Problem Management-Prozess können Sie mit MDR Launcher Folgendes tun:

1. Ein Problem erkennen.
2. Die Schwere und Verbreitung des Problems erkennen, indem Sie die CI-Beziehungsdaten verwenden, um zu bestimmen, welche abhängigen CIs betroffen sind.
3. Mögliche Ursachen des Problems bestimmen, indem Sie übergeordnete CIs untersuchen.
4. Wenn nötig eine gründliche Analyse durchführen, indem Sie die sehr ausführlichen Informationen verwenden, die im MDR zur Verfügung stehen und über das MDR Korrekturen vornehmen.

MDR-Terminologie

Folgende Begriffe werden bei der CMDB-MDR-Integration verwendet:

Ein Management Data Repository (MDR) stellt Software oder Daten dar, die Quellinformationen zu einem CI enthalten. Ein MDR enthält normalerweise mehr unbearbeitete CI-Informationen als die CMDB, die eine verwaltete Teilmenge dieser Daten enthält.

In einer *MDR-Klasse* ("MDR_CLASS") werden MDRs zusammengefasst, die von der CA CMDB auf ähnliche Weise verarbeitet werden. Es gibt drei besondere MDR-Klassen: "**COHESION**", "**GLOBAL**", und "**cmdbf**".

Ein *MDR-Name* ("MDR_NAME") ist der Name, den ein MDR verwendet, um auf sich selbst zu verweisen. Stellen Sie sicher, dass die Kombination "mdr_name" und "mdr_class value" im Unternehmen eindeutig ist.

Eine Föderierte Asset-ID (FEDERATED_ASSET_ID) ist ein eindeutiges MDR-Kennzeichen für ein CI.

Unterschiedliche CI-Familien verwenden normalerweise jeweils unterschiedliche MDRs als Datenanbieter. Ein einzelnes CI kann jedoch mehrere MDR-Datenanbieter haben. Beispiel:

CI-Familie	MDR_KLASSE
Kontakt	Personalsystem
	Telefonverzeichnis
	Single Sign-On-Authentifizierungssystem
Document	Dokumentverwaltungssystem
Klimaanlage	Dokumentverwaltungssystem
	Vertragsverwaltungssystem
	Klimaanlagenkontrollsystem
Mainframe	Bandverwaltungssystem
	DASD-Verwaltungssystem
	Leistungsverwaltungssystem
	Jobplaner
Speicherung	Speicherverwaltungssystem
	Anlagenverwaltungssystem
Standort	Anlagenverwaltungssystem
	Fortbildungskalender
	Büroverzeichnis

CI-Familie	MDR_KLASSE
Netzwerk	Netzwerkmanagement-Systeme Problem-Management-System

In jeder MDR-Klasse können verschiedene MDRs sein, und jedes MDR kann Daten zu mehreren CIs liefern. Ein vorhandenes CI kann Daten von null oder mehr MDRs erhalten. Ein CI kann auch unabhängig Daten erhalten. Ein Mainframe-CI kann zum Beispiel über Daten verfügen, die von Disk Management-System 1 geliefert wurden, während ein anderes Mainframe-CI über Daten verfügen kann, die von Disk Management-System 2 und Jobplaner 2 geliefert wurden. CA CMDB verwaltet die Beziehungen zwischen CIs und allen mit diesen verbundenen MDRs.

MDR-Zuordnung

Jedes MDR kennzeichnet auf eindeutige Weise die von ihm verwalteten CIs. Diese Bezeichner werden selten für alle MDRs synchronisiert. Bei der Referenzierung eines bestimmten Kontakt-CIs kann es zum Beispiel vorkommen, dass verschiedene MDRs die Personalausweisnummer, Telefonnummer, Führerscheinnummer oder Mitarbeiternummer verwenden, um auf die gleiche Person zu verweisen. Die Verbindung dieser unterschiedlichen Kennungen mit derselben eindeutigen, in der MDB verwalteten Kennung (UUID) nennt man *Zuordnung*. Die Zuordnung erfolgt automatisch, wenn beim Import von Daten mit GRLoader das CI die Tags <mdr_name> <mdr_class> und <federated_asset_id> enthält. Die Zuordnung kann außerdem manuell über die Verwaltungsfunktionen der Benutzeroberfläche vorgenommen werden. Ein CI, mit dem keine Zuordnungen verbunden sind, nennt man *unverbunden*. Jedes CI ist automatisch globalen MDRs zugeordnet, die den UUID als "federated_asset_id" verwenden.

Starten von MDR

Wenn Sie ein CI mit Hilfe der CA CMDB-Benutzeroberfläche anzeigen, können Sie direkt auf eine Reihe von Schaltflächen klicken, um eine MDR-Benutzeroberfläche zu starten. Es gibt je eine Schaltfläche pro MDR-Zuordnung für das Fokus-CI. Dieser Start wird üblicherweise verwendet, wenn Sie überprüfen möchten, ob ein Change erfolgreich war, oder wenn Sie zusätzliche Informationen zu einem CI erhalten möchten, die nicht durch die CMDB gesammelt werden.

CMDBf Viewer

CA SDM stellt den CMDBf-Viewer bereit, um die Ergebnisse der CI-Föderation in den MDRs anzuzeigen. Klicken Sie auf einer CI- Detailseite (oder in der CI-Liste in dem CI-Kontextmenü) auf den CMDBf-Viewer, um die CI-Attribute der föderierten CMDBs und MDRs parallel anzuzeigen. Auf der Seite der föderierten Ansicht können Sie auf "Abrufen" klicken, um die Information der föderierten MDRs zu aktualisieren. Zur besseren Lesbarkeit können CA CMDB-Metadatendateien MDR-Attributnamen und CA CMDB-Attributnamen abstimmen.

Hinweis: Diese Funktion erfordert MDRs, die Abfragen unterstützen. Konfigurieren Sie die MDR-CMDBf-Endpunkte entsprechend, um ihre Ergebnisse in der föderierten Ansicht anzuzeigen. Weitere Informationen finden Sie im *Implementierungshandbuch*.

Definieren eines MDR für CA CMDB

Bevor Sie den CMDBf-Viewer verwenden, müssen Sie das MDR für CA CMDB definieren.

So definieren Sie ein neues MDR für CA CMDB

1. Navigieren Sie auf der Registerkarte "Administration" zu "CA" > "CMDB" > "MDR-Management" > "MDR-Liste".
2. Klicken Sie auf "Neu erstellen".

Die Seite "Create New MDR Definition" wird angezeigt.

3. Füllen Sie die folgenden Felder aus:

Mandant

Gibt den Mandanten an, dem dieses MDR gehört (wenn mehrere Mandanten installiert sind).

Button Name

Die Beschriftung der MDR-Schaltfläche, die auf der Seite "CI – Detail" angezeigt wird. Dieser Name muss für jedes MDR eindeutig sein. Erforderlich für "launch in context" und CMDBf-Viewer.

MDR-Name

Gibt die Zeichenfolge für den Abgleich mit den XML-Daten an, die in das Feld "mdr_name" gesendet werden. Das MDR kann jede beliebige Zeichenfolge verwenden; am üblichsten ist aber der Hostname. Dieser Name bildet zusammen mit "mdr_class" einen eindeutigen Namen für das MDR. Erforderlich für "launch in context" und CMDBf-Viewer.

MDR-Klasse

Die Klasse, die mit den Daten übereinstimmen muss, die im Feld "mdr_class" in der XML gesendet werden. Für diesen Namen kann eine beliebige Zeichenfolge verwendet werden. Er muss jedoch zusammen mit dem Feld "mdr_name" eine eindeutige Kennung für das MDR bilden. Globale MDRs werden mit der MDR-Klasse "GLOBAL" definiert.

- CA Cohesion ACM-MDRs müssen eine COHESION-MDR-Klasse aufweisen. So werden automatisch die Felder "Pfad", "Parameter" und "URL to be launched" (zu startende URL) auf die erforderlichen CA Cohesion ACM-Werte für das Starten im Kontext festlegt.
- MDRs aus CA Asset Portfolio Management r11.3.4 müssen einen MDR-Namen für APM sowie eine MDR-Klasse für GLOBAL aufweisen. So werden die Felder "Pfad", "Parameter" und "URL to be launched" (zu startende URL) auf die erforderlichen CA Asset Portfolio Management r11.3.4-Werte für das Starten im Kontext festlegt.
- CA APM r12.5-MDRs müssen den MDR-Namen "ITAM" und die MDR-Klasse "GLOBAL" angeben. So werden die Felder "Pfad", "Parameter" und "URL to be launched" (zu startende URL) auf die erforderlichen CA APM r12.5-Werte für das Starten im Kontext festlegt.
- Für den CMDBf-Viewer muss die MDR-Klasse "cmdbf" sein.

Aktiv

Zeigt an, ob die MDR-Definition aktiv oder inaktiv ist. Inaktive MDR-Definitionen werden logisch gelöscht, können jedoch mit Hilfe der Suchfunktion wieder aktiviert werden.

Eigentümer

Der für dieses MDR verantwortliche Kontakt.

Beschreibung

Gibt eine Beschreibung in Freitext an.

Hostname

Gibt den Hostnamen, den DNS-Namen oder die IP-Adresse des Hosts an, der den Webserver enthält, auf dem sich die zu startende Webseite befindet. Für den kontextabhängigen Start erforderlich.

Port

Der vom MDR-Webserver verwendete TCP/IP-Port für die Bedienung von Webseiten. Standard ist Port 80. Für den kontextabhängigen Start erforderlich.

Pfad

Der Teil der URL, der vor dem Fragezeichen (?) steht. Diese Informationen finden Sie in der MDR-Dokumentation.

- Für "mdr_class" von Cohesion ist der Wert automatisch auf "CAisd/html/cmdb_cohesion.html" eingestellt und kann nicht geändert werden.
- Wenn für "mdr_name" "APM" und für "mdr_class" "GLOBAL" festgelegt wurde, wird der Wert automatisch auf "apm/frmObject.aspx" gesetzt und kann nicht geändert werden.
- Für den MDR-Namen (mdr_name) von ITAM und für die MDR-Klasse (mdr_class) von GLOBAL wird der Wert automatisch auf ITAM/Pages/Asset.aspx gesetzt. Dieser Wert kann nicht geändert werden.

Parameter

Der Anteil der URL, der nach dem Fragezeichen (?) steht. Die entsprechenden Informationen sind in der MDR-Dokumentation enthalten.

- Für die mdr_class von Cohesion ist der Wert automatisch auf "hostname={hostname}+port={port}+family={family}+name={name}+secret={password}+federated_asset_id={federated_asset_id}" eingestellt und kann nicht geändert werden.
- Wenn für "mdr_name" "APM" und für "mdr_class" "GLOBAL" festgelegt wurde, wird der Wert automatisch auf "ObjectID={cmdb_asset_id}&obj=11&FUNCTION=1&WinID=OBFASSET{cmdb_asset_id}&WinContainerID=" gesetzt und kann nicht geändert werden.
- Für den MDR-Namen (mdr_name) von ITAM und für die MDR-Klasse (mdr_class) von GLOBAL wird der Wert automatisch auf ParentClass=Asset&assetid={cmdb_asset_id}&TicketID={itam_ticketid} gesetzt. Dieser Wert kann nicht geändert werden.

Anwender-ID

Die MDR-Anwenderanmeldung, falls erforderlich. Dieser Wert wird in die URL anstelle von {Anwender-Id} eingefügt. Ist nichts angegeben, wird standardmäßig die Anwender-ID der Person angegeben, die gerade angemeldet ist.

Für CA Cohesion ACM ist "Gemeinsamer geheimer Schlüssel" der Schlüssel, um auf CA Cohesion ACM zuzugreifen, wenn erforderlich. Dieser Wert wird in die URL anstelle von {Kennwort} eingefügt.

Hinweis: Weitere Informationen über das Definieren des MDR, finden Sie im *Implementierungshandbuch zu CA Cohesion ACM*.

Shared Secret

Gibt Informationen an, die von CA CMDB und dem MDR gemeinsam verwendet werden. Dieser Wert wird in die URL anstelle von {Kennwort} eingefügt. Bei CA Cohesion ACM-MDRs muss der Wert mit "com.cendura.security.oneclickauth.secret" übereinstimmen. Weitere Informationen zum Erstellen eines freigegebenen Kennworts finden Sie im *CA Cohesion ACM Implementation Guide* (Implementierungshandbuch) unter "Integrating with CA CMDB" (Integration mit CA CMDB). Für CMDBf-Viewer erforderlich.

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.

URL to be Launched

Standardwert von "http://{Hostname}:{Port}/{Pfad}?{Parameter}". Bei einigen MDRs kann dieser Wert gegebenenfalls geändert werden, um MDR-spezifische Aspekte zu berücksichtigen. Für den kontextabhängigen Start erforderlich.

Wenn für "mdr_name" "APM" und für "mdr_class" "GLOBAL" festgelegt wurde, lautet der Wert "http://{Hostname}:{Port}/{Pfad}?{Parameter}".

Wenn für "mdr_name" "ITAM" und für "mdr_class" "GLOBAL" festgelegt wurde, lautet der Wert "http://{Hostname}:{Port}/{Pfad}?{Parameter}".

Für Die MDR-Klasse (mdr_class) von Cohesion ist der Standardwert `http://cmdb_hostname:cmdb_port/{path}?{parameters}`.

wobei:

cmdb_hostname ist der Hostname, DNS-Name oder die IP-Adresse des CA CMDB-Webservers. Standardeinstellung ist der Hostname, der gerade auf den CA CMDB-Webserver zugreift.

cmdb_port ist der TCP/IP-Port des CMDB-Webservers. Standardmäßig wird die Nummer des aktuellen Ports verwendet, der derzeit auf den CA CMDB-Webserver zugreift.

Hinweis: Wenn Sie SSL-Unterstützung für Cohesion aktiviert haben, muss die URL wie folgt lauten:

"http://hostname:port/{Pfad}?{Parameter}+https=yes"

Informationen zur Aktivierung der HTTPS-Unterstützung durch "CA Cohesion ACM" finden Sie in der CA Cohesion ACM-Online-Hilfe im Thema zum Erstellen des HTTPS-Zertifikats und Aktivieren von HTTPS.

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".

4. Klicken Sie auf "Speichern".

Das MDR ist definiert.

MDR URL-Definitionen

Die zu startende URL hat den Standardwert `http://{hostname}:{port}/{path}?{parameters}`. Dieser kann gegebenenfalls geändert werden, um etwaige MDR-spezifische Aspekte zu berücksichtigen. Die URL ist für den "kontextuellen Start" erforderlich.

Wenn APM oder ITAM für "mdr_name" und GLOBAL für "mdr_class" festgelegt wurde, lautet der Standardwert:

`http://{hostname}:{port}/{path}?{parameters}`

Für "mdr_class" von Cohesion ist der Standardwert:

`"http://cmdb_hostname:cmdb_port/{Path}?{Parameters}"`

cmdb_hostname

Gibt den Hostnamen, DNS-Namen oder die IP-Adresse des CA CMDB-Webservers an. Standardmäßig ist dies der aktuelle Hostname, der derzeit auf den CA CMDB-Webserver zugreift.

cmdb_port

Gibt den TCP/IP-Port des CA CMDB-Webservers an. Standardmäßig ist dies die aktuelle Port-Nummer, die verwendet wird, um auf den CA CMDB-Webserver zuzugreifen.

Wenn Sie die SSL-Unterstützung für CA Cohesion ACM aktiviert haben, muss die URL wie folgt lauten:

`"http://hostname:port/{Pfad}?{Parameter}+https=yes"`

Hinweis: Weitere Informationen über die HTTPS-Unterstützung von CA Cohesion ACM finden Sie in der Online-Hilfe zu CA Cohesion ACM.

MDR-Start-URL

Die MDR-Start-URL hat den folgenden Standardwert:

`http://{hostname}:{port}/{path}?{parameters}`

Sie können diesen Ausdruck ändern, um MDR-spezifische Überlegungen zu berücksichtigen. Die URL ist für den "kontextuellen Start" erforderlich.

- Für "mdr_name" von APM und "mdr_class" von GLOBAL lautet der Standardwert:

`http://{hostname}:{port}/{path}?{parameters}`

- Für "mdr_class" von Cohesion ist der Standardwert:

`"http://cldb_hostname:cldb_port/{Path}?{Parameters}"`

cldb_hostname

Hostname, DNS-Name oder die IP-Adresse des CA CMDB-Webservers.
Standardmäßig ist dies der Hostname, der derzeit auf den CA CMDB-Webserver zugreift.

cldb_port

TCP/IP-Port des CA CMDB-Webservers. Standardmäßig ist dies die aktuelle Port-Nummer, die verwendet wird, um auf den CA CMDB-Webserver zuzugreifen.

Wenn Sie SSL-Unterstützung für CA Cohesion ACM aktiviert haben, muss die URL wie folgt lauten:

`"http://hostname:port/{Pfad}?{Parameter}+https=yes"`

Hinweis: Weitere Informationen über die HTTPS-Unterstützung von CA Cohesion ACM finden Sie in der Online-Hilfe zu Cohesion.

Definieren von Startparameter für URL-Ersetzungen

Beim Definieren eines MDR können die folgenden Parameter verwendet werden, um dessen URL für die Anzeige zu erstellen. Diese Parameter werden zur Laufzeit durch die entsprechenden Werte ersetzt. Diese Variablen müssen in den oben genannten Feldern angegeben werden.

hostname ist der MDR-Hostname aus der MDR-Definition.

alarm_id ist die IP-Adresse des ausgewählten CI.

federated_asset_ID ist die eindeutige Kennung des ausgewählten CI im MDR.

cmdb_asset_id ist die Asset-ID für das CI.

port ist der MDR-Port aus der MDR-Definition.

userid ist die Anwender-ID aus der MDR-Definition. Ist nichts angegeben, wird standardmäßig die Anwender-ID der Person angegeben, die gerade angemeldet ist.

password ist das freigegebene Kennwort aus der MDR-Definition.

mdr_name ist der MDR-Name aus der MDR-Definition.

mdr_class ist die MDR-Klasse aus der MDR-Definition.

class ist die Klasse des ausgewählten CI.

family ist die Familie des ausgewählten CI.

path ist der Pfad aus der MDR-Definition.

name ist der Name des ausgewählten CI.

model ist das Modell des ausgewählten CIs.

manufacturer ist der Hersteller des ausgewählten CIs.

itam_ticketid ist die Ticket-ID, die in CA APM einzutragen ist.

Beispiel: Starten eines MDR

Ein CA CMDB-Anwender zeigt ein Server-CI mit dem Namen server1 an, das eine Zuordnung zu einer intern entwickelten Anwendung mit dem Namen Comet hat. Comet kennzeichnet server1 eindeutig als server:server1.

Comet wird durch die folgenden Eigenschaften als MDR definiert:

- Hostname: CometServer
- Port: 80
- Pfad: index.php
- Parameter: item={federated_asset_id}
- Start_url: http://{hostname}:{port}/{path}?{parameters}

Wenn der Anwender in CA CMDB auf der Registerkarte "Attribute" des server1-CI auf die Schaltfläche "Comet" klickt, wird über ein Webbrowser-Fenster die folgende URL geöffnet:

`http://CometServer:80/index.php?item=server:server1`

Parameter für die URL-Ersetzungen

Beim Definieren eines MDR können Sie die folgenden Parameter verwenden, um dessen URL für die Anzeige zu erstellen. Diese Parameter werden zur Laufzeit durch die entsprechenden Werte ersetzt. Diese Variablen müssen in den MDR-Felddefinitionen angegeben werden.

{hostname}

Der MDR-Hostname aus der MDR-Definition.

{alarm_id}

Die IP-Adresse des ausgewählten CI.

{federated_asset_ID}

Eindeutige Kennung des ausgewählten CI im MDR.

{cmdb_asset_id}

Asset-ID für das CI.

{port}

Die MDR-Portnummer aus der MDR-Definition.

{userid}

Die Benutzer-ID aus der MDR-Definition. Ist nichts angegeben, wird standardmäßig die Benutzer-ID der Person angegeben, die gerade angemeldet ist.

{password}

Das freigegebene Kennwort aus der MDR-Definition.

{mdr_name}

Der MDR-Name aus der MDR-Definition.

{mdr_class}

Die MDR-Klasse aus der MDR-Definition.

{class}

Die Klasse des ausgewählten CI.

{family}

Die Familie des ausgewählten CI.

{path}

Der in der MDR-Definition beschriebene Pfad.

{name}

Der Name des ausgewählten CI.

{model}

Gibt den Namen des ausgewählten CI an.

{manufacturer}

Gibt den Hersteller des ausgewählten CI an.

Beispiel: Verwenden von Parametern für die URL-Ersetzungen

Ein CA CMDB-Benutzer zeigt ein Server-CI mit dem Namen server1 an, das eine Zuordnung zu einer intern entwickelten Anwendung mit dem Namen Comet hat. Comet kennzeichnet server1 eindeutig als server:server1.

Comet wird durch die folgenden Eigenschaften als MDR definiert:

- Hostname: CometServer
- Port: 80
- Pfad: index.php
- Parameter: item={federated_asset_id}
- Start_url: http://{hostname}:{port}/{path}?{parameters}

Wenn der Benutzer in CA CMDB auf der Registerkarte "Attribute" des server1-CI auf die Schaltfläche "Comet" klickt, wird über ein Webbrowser-Fenster die folgende URL geöffnet:

`http://CometServer:80/index.php?item=server:server1`

Zusammenschlüsse unter Verwendung von GRLoader

Bei der Arbeit mit GRLoader müssen folgende XML-Tags für jedes CI im XML-Dokument aufgefüllt sein. Diese Tags gelten für jede MDR-Familie.

- `<mdr_name>`
- `<mdr_class>`
- `<federated_asset_id>`

Hinweis: CA Cohesion ACM gibt "mdr_name", "mdr_class" und "federated_asset_id" automatisch vor.

Sind diese Informationen nicht in der XML-Datei vorhanden, ist die Ausführung des "kontextuellen Starts" nicht möglich, da der Ursprung des CI nicht bestimmt werden kann.

Um die Quelle eines CI zu identifizieren, können Sie die XML-Datei ändern, bevor sie in GRLoader eingegeben wird. Sie können die XML-Datei mit einem Texteditor ändern und eine globale Veränderung vornehmen, oder Sie können diese Aufgabe programmgesteuert erledigen.

Hinweis: Weitere Informationen zur MDR-Identifizierung und zu GRLoader finden Sie im *technischen CA CMDB-Referenzhandbuch*.

Föderieren eines CI

Wenn CIs in CA CMDB geladen werden, bevor ihr entsprechendes MDR definiert wurde, sind sie unverbunden. Das bedeutet, dass sie noch nicht mit einem MDR verbunden sind und den "kontextuellen Start" noch nicht unterstützen.

So föderieren Sie ein CI

1. Definieren Sie das erforderliche MDR.
2. Führen Sie einen der folgenden Schritte aus:
 - Ordnen Sie das CI manuell zu.
 - Führen Sie erneut den CA Cohesion ACM-Bericht aus, der das CI erstellt hat, und geben Sie im Bericht die Option "Aktualisierung bestehender CIs zulassen" an.

Hinweis: Weitere Informationen zu CA Cohesion ACM-Berichten finden Sie im *CA Cohesion ACM-Produkthandbuch*.

3. Führen Sie GRLoader erneut aus, und geben Sie dieselbe Eingabedatei an, die auch zur Erstellung der CIs verwendet wurde.

Die Abstimmungs-Engine von CA CMDB führt die Informationen des MDR mit den bestehenden CIs zusammen.

4. Erstellen Sie ein XML-Dokument, das das CI und sein MDR beschreibt, und starten Sie GRLoader im Aktualisierungsmodus.

Die Abstimmungs-Engine von CA CMDB führt die neuen Informationen mit dem bestehenden CI zusammen. Das bestehende CI ist verbunden.

Beispiel: Angeben der Lokation eines CI

Sie müssen sicherstellen, dass die Abstimmungs-Engine über genügend Informationen verfügt, um das CI zu finden, das aktualisiert werden soll. In dem folgenden Beispiel wurden zur besseren Lesbarkeit End-Tags entfernt und Leerzeichen eingefügt.

```
<ci>
  <name>          server3
  <mac_address>
  <serial_number>
  <asset_num>
  <dns_name>
  <mdr_name>      mdr_one
  <mdr_class>     Cohesion
</ci>
```

Definieren von mehreren MDRs für ein CI mit GRLoader

Mit GRLoader können Sie mehrere MDRs für ein CI definieren.

Wenn Sie mehrere MDRs für ein einzelnes CI definieren möchten, kann das XML-Dokument den <ci>-Knoten wiederholen. Dabei kann jeder duplizierte <ci>-Knoten einen anderen "mdr_name" und eine andere "mdr_class" angeben. Mit anderen Worten, jedes MDR kann seine Attribute liefern, und zwar unabhängig von anderen MDRs, die Daten an das CI liefern.

Beispiel: Definieren von mehreren MDRs für ein CI

Wenn MDR1 und MDR2 beide Daten an das server2-CI liefern, dann sollte das XML-Dokument ungefähr wie im folgenden Beispiel aussehen. In dem Beispiel wurden zur besseren Lesbarkeit End-Tags entfernt und Leerzeichen eingefügt.

```
<ci>
  <name>      server2
  <mdr_name>  mdr1
  <mdr_class> Cohesion
  <diskspace> 500 gb
  <disktype>  SCSI-3
</ci>
<ci>
  <name>      server2
  <mdr_name>  mdr2
  <mdr_class>Service Assure
  <sla>
</ci>
```

CA CMDB stimmt die beiden obigen CIs mit demselben CI ab und verbindet beide MDRs mit diesem einzelnen CI.

Hinweis: GRLoader benötigt eine oder zwei Ausführungen, um die CIs zu importieren.

Zuordnen zwischen MDR-CIs und CA CMDB-CIs

Nachdem Sie ein CI manuell über die Option "Datei" > "Neues CI" definiert haben, müssen Sie die Zuordnung zwischen diesem CI und dem CI in dem föderierten MDR manuell definieren. Sie haben zwei Möglichkeiten, ein CI mit einem MDR zu verbinden:

- Bearbeiten des CI.
- Verwenden des Knotens "Föderierte CI-Zuordnung" auf der CA CMDB-Registerkarte "Administration".

So erstellen Sie eine Zuordnung durch Bearbeiten des CI

1. Zeigen Sie die Seite "CI-Detail" des CI an, das Sie mit einem MDR verbinden möchten.
 2. Klicken Sie auf "Bearbeiten".
 3. Zeigen Sie die Registerkarte "Attribute" an.
 4. Klicken Sie auf "MDR hinzufügen".
- Das CI wird dem MDR zugeordnet.

So erstellen Sie mit Hilfe der Seite "Föderierte CI-Zuordnung" eine Zuordnung:

1. Klicken Sie auf die Registerkarte "CA CMDB-Administration".
2. Öffnen Sie den Management Data Repository-Knoten.
3. Wählen Sie den Knoten "Föderierte CI-Zuordnung".

Die Liste der Föderierten Configuration Item-Zuordnungen wird angezeigt.

4. Klicken Sie auf "Neu erstellen".

Die Seite "Neue föderierte CI-Zuordnung erstellen für" wird angezeigt.

5. Verknüpfen Sie das CI mit dem MDR, indem Sie die Felder "Federated CI Mapping" ausfüllen:

Name des Konfigurationselements

Der Name, der verwendet wird, um das CI zu identifizieren.

Föderierte Anlagen-ID

Die Zeichenfolgenkennung, die vom Quell-MDR verwendet wird, um dieses CI zu identifizieren. Die Kennung wird von der MDR-Software bestimmt.

MDR-Name

Der Name, mit dem das MDR (und seine MDR-Schaltfläche) bezeichnet werden.

Aktiv

Zeigt an, ob diese Zuordnung aktiv oder inaktiv ist. Zuordnungen können nur deaktiviert, aber nicht gelöscht werden.

6. Klicken Sie auf "Speichern".

Die Zuordnung zwischen diesem CI und dem CI im verbundenen MDR ist definiert.

Konfigurieren von MDRs für CMDBf Viewer

Bevor Sie den CMDBf-Viewer verwenden können, müssen Sie die föderierten MDR-Provider so einrichten, dass sie auf den CMDBf-Abfragedienst verweisen.

- Externe MDRs müssen einen Abfragedienst bereitstellen, der die "InstanceIdConstraint"-Abfrage verarbeiten kann.
- Der Schaltflächenname, der MDR-Name und die MDR-Klasse sind erforderlich, damit die Schaltfläche für den CMDBf-Viewer auf der CI-Detailseite angezeigt werden kann.
- Die MDR-Klasse muss als "**cmdbf**" definiert werden.
- Für CA CMDB muss der CMDBf-Namespace auf "**http://cmdb.ca.com/r1**" festgelegt werden. Informationen zu anderen CMDBs und MDRs finden Sie in der entsprechenden Dokumentation.
- Ein Zeitlimit ist optional. Der Standardwert ist zehn (10) Sekunden.
- Damit in der föderierten Ansicht eine funktionierende Abrufschaltfläche angezeigt wird, müssen Sie den CMDBf-Endpunkt, die Benutzer-ID und den gemeinsamen geheimen Schlüssel definieren.

Hinweis: Ein vorhandenes CA CMDB-System kann als CMDBf-Provider eingerichtet werden, indem ein CMDBf-Endpunkt "http://servername:port/axis/services/QueryPort" angegeben wird. Dabei gilt:

- Hostname ist der Computer, auf dem CA CMDB installiert ist (lokaler Host oder Computername).
- Port ist der Port, für den CA CMDB konfiguriert ist.

Starten der MDR-Webbrowser-Schnittstelle

Nachdem eine Zuordnung zwischen einem CI und einem MDR erstellt wurde, wird automatisch eine Schaltfläche auf der Registerkarte "Attribute" platziert. Wenn mit diesem CI mehrere MDRs verbunden sind, werden mehrere Schaltflächen angezeigt.

Wenn Sie auf eine MDR-Schaltfläche klicken, wird eine neue Seite geöffnet, und die komplett ersetzte, in der MDR-Definition definierte MDR-URL wird angezeigt.

Beispiel: Starten von CA Cohesion

Wenn ein CI korrekt mit seinem MDR verbunden wurde, wird eine Cohesion-Schaltfläche auf der Registerkarte "Attribute" angezeigt. Sollte keine Schaltfläche auf der Registerkarte "Attribute" angezeigt werden, überprüfen Sie die Zuordnung für das angezeigte CI. Stellen Sie sicher, dass es eine Zuordnung für dieses CI gibt und dass das Ziel-MDR über eine URL verfügt, die aufgerufen werden kann. Wenn Sie auf die Schaltfläche klicken, um das MDR zu öffnen, wird über ein neues Fenster die Ziel-URL geöffnet und CA Cohesion gestartet.

Integration von CA Cohesion

Beachten Sie Folgendes beim Integrieren von CA Cohesion ACM in CA CMDB:

- Integrieren von Cohesion in CA CMDB

Hinweis: Weitere Informationen zur Integration von Cohesion in CA CMDB finden Sie unter "Integration mit CA CMDB" im *CA Cohesion ACM-Implementierungshandbuch*.

- Importieren von CIs aus einem Cohesion-MDR

Hinweis: Informationen zum Importieren von CIs aus einem Cohesion-MDR finden Sie in der Online-Hilfe, auf die Sie über die Registerkarte für Berichtsvorlagen in den CA Cohesion ACM-Berichten zugreifen.

- Kontextuelles Starten von Cohesion-MDRs

Damit die Integration des kontextuellen Starts mit CA Cohesion ACM bestmöglich funktioniert, sollten Sie über die CA CMDB-Registerkarte "Administration" das Cohesion-MDR definieren, *bevor* Sie den Cohesion CMDB-Bericht ausführen.

Hinweis: Da CA Cohesion ACM keine eindeutige föderierte Asset-ID für NIC- oder Dateisystem-CIs unterstützt, wird MDR Launcher für NIC- oder Dateisystem-CIs nicht von Cohesion unterstützt. Aus diesem Grund zeigt ein auf Cohesion basierendes NIC- oder Dateisystem-CI selbst bei erfolgreichem Import keine Schaltfläche für den MDR Launch an.

Kapitel 12: Verwalten von Webservices

Wichtig! Weitere Informationen zu Webservices finden Sie im technischen CA SDM-Referenzhandbuch.

Dieses Kapitel enthält folgende Themen:

[Verwalten von Webservices](#) (siehe Seite 581)
[CA SDM-Komponenten](#) (siehe Seite 582)
[Tipps für SOAP-Webservices-Clients](#) (siehe Seite 582)
[Konfiguration der SOAP Webservices](#) (siehe Seite 585)
[Sicherheit von Webservices](#) (siehe Seite 587)
[Fehlerbehandlung in SOAP](#) (siehe Seite 589)
[Installation von Webservices](#) (siehe Seite 593)
[Externe Spezifikationen](#) (siehe Seite 594)
[Objekte](#) (siehe Seite 613)
[ITIL Methodology](#) (siehe Seite 618)
[Verwenden der Webservices](#) (siehe Seite 621)

Verwalten von Webservices

Bei *Webservices* handelt es sich um einen Satz von Datenaustauschstandards für die Kommunikation zwischen Produkten, die sich in unterschiedlichen Betriebsumgebungen befinden können. Dies verhält sich analog zum Browsen im Internet vom PC aus: Es kann auf alle Remote-Websites zugegriffen werden, unabhängig davon, ob diese sich auf Solaris-, AIX-, Windows- oder anderen Hosts befinden. Auf die gleiche Weise können Produkte mithilfe von Webservices über HTTP mit unterschiedlichen Servern kommunizieren, und zwar unabhängig von der Betriebsumgebung. So kann z. B. eine Microsoft Office-Anwendung mit einem Programm auf einem UNIX-Server kommunizieren, und eine Java-Serverseite hat Zugriff auf einen Server, der unter Windows gehostet wird. Dank dieser plattformunabhängigen Kommunikation sind umfassende Integrationsmöglichkeiten gegeben.

Web Services nutzt diese Technologie, so dass mit nahezu allen Produkten der Zugriff auf CA SDM und Knowledge Management möglich ist. Webservices-Clients können Tickets erstellen, Assets aktualisieren, die Knowledge Base durchsuchen und vieles mehr.

CA SDM-Komponenten

CA SDM stellt die Installationsdateien für diese Version von J2EE-Webservices im folgenden Verzeichnis bereit:

```
"<NX_ROOT>/sdk/websvc/R11"
```

Hinweis: "<NX_ROOT>" gibt den Stamminstallationspfad für CA SDM an.

Tipps für SOAP-Webservices-Clients

Das Beispiele-Verzeichnis der CA SDM-Installation stellt ein Beispiel für eine Java-Client-Anwendung für Webservices bereit. Dieses Beispiel unterstützt die Entwickler mit der Entwicklung von Webservices-Client-Anwendungen.

Für viele Webservices-Methoden sind Arrays als Eingabeparameter erforderlich. Zum Beispiel ist bei der Methode "createIssue()" ein leeres Array für "propertyValues" zulässig. Gelegentlich sind Arrays optional, jedoch muss für den Service ein leeres Array angegeben werden. Wenn Sie Visual Studio .NET für den Zugriff auf Webservices verwenden, geben Sie ein leeres Array aus einem der folgenden Arrays an:

In C#:

```
String[] emptyArray = new string[0];
```

In Visual Basic .NET:

```
Dim emptyArray As String() = {}
```

Java

```
Array<String> opMsk = new Array<String>();  
attr.setString(new String[0]);  
"Array<String>" ist eine proprietäre Klasse.
```

Sie können dann "emptyArray" an Array-Parameter übergeben, für die leere Arrays zulässig sind.

Hinweis: Die CA SDM-Webservices verwenden die Apache-Implementierung von Standards, die vom World Wide Web-Konsortium (W3C) festgelegt wurden. Im Idealfall sollte ein Client in jeder beliebigen Betriebsumgebung auf die Dienste zugreifen können, wobei sich die Implementierungen verschiedener Anbieter jedoch unterscheiden. Viele Programmierungsumgebungen bieten ein Tool zur Erzeugung von Proxy-Klassen aus einer Web Services Description Language (WSDL)-Beschreibung.

Weitere Informationen:

[Java-Clients](#) (siehe Seite 583)

Java-Clients

In "TableOfContents.doc" unter "\$NX_ROOT/samples/sdk/websvc" sind mehrere Java-Beispielprogramme aufgelistet.

Jedes Beispielprogramm enthält Hinweise zur Kompilierung und Ausführung anhand der Skriptdateien "run_java_test.bat.txt" (Windows) bzw. "run_java_test_sh.txt" (UNIX). Diese Skripts zeigen, wie "org.apache.axis.wsdl.WSDL2Java" zum Generieren der clientseitigen Stub-Dateien für CA SDM-Webservices verwendet wird.

Wenn Axis 1.4 verwendet wird, ist der Parameter "-w" erforderlich, damit die Stub-Dateien korrekt generiert werden. Wenn WSDL2Java entsprechend den Anweisungen ausgeführt wird, werden die Stub-Dateien im Unterverzeichnis "com/ca/www/UnicenterServicePlus/ServiceDesk" generiert. Die folgenden Dateien werden generiert:

- ArrayOfInt.java
- ArrayOfString.java
- ListResult.java
- USD_WebService.java
- USD_WebServiceLocator.java
- USD_WebServiceSoap.java
- USD_WebServiceSoapSoapBindingStub.java

Importieren Sie diese Klassen mit der folgenden Anweisung:

```
import com.ca.www.UnicenterServicePlus.ServiceDesk.*;
```

Viele Webservices-Methoden haben Parameter vom Typ "ArrayOfString", einer proprietären Klasse. Zum Beispiel sind das "attrVals" der "createRequest()" -Methode, "propertyValues" und Attributparameter "ArrayOfString"-Parameter.

Um die Werte in einer "ArrayOfString"-Variablen festzulegen, instanziiieren Sie die Variable, und verwenden Sie dann "setString()" folgendermaßen:

```
ArrayOfString attrVals = new ArrayOfString();  
attrVals.setString(new String[]{"customer", customerHandle, "description",  
"description text"});
```

So wird die Variable auf leer festgelegt:

```
attrVals.setString(new String[0]);
```

Verwenden Sie eine Variable des Typs "ListResult", einer weiteren proprietären Klasse, als Rückgabewert für die Listenmethoden "doQuery()", "getRelatedList()", "getNotificationsForContact()", "getPendingChangeTaskListForContact()" und "getPendingIssueTaskListForContact()". Ein "ListResult" enthält "listHandle"- und "listLength"-Elemente, die wie im Beispiel gezeigt mit "getListHandle()" und "getListLength()" abgerufen werden können:

```
ListResult doQueryResult = new ListResult();
doQueryResult = USPSD.doQuery(sid, "iss", "active = 1");
int listHandle = doQueryResult.getListHandle();
int listLength = doQueryResult.getListLength();
```

Die "getListValues()" -Methode verwendet "listHandle", wobei die Werte aus einer Teilmenge der Liste abgerufen werden.

Der Parameter "Handles" der "freeListHandles()" -Methode ist ein "ArrayOfInt", eine weitere proprietäre Klasse. Rufen Sie "freeListHandles()" anhand des "listHandle" aus einem "ListResult" auf:

```
ArrayOfInt handleList = new ArrayOfInt();
handleList.setInteger(new java.lang.Integer []{ new java.lang.Integer(listHandle)
});
USPSD.freeListHandles(sid, handleList);
```

Einige Methoden haben Pass-By-Reference-Parameter des Typs "javax.xml.rpc.holders.StringHolder". So hat z. B. "createRequest()" zwei Parameter diesen Typs, "NewRequestHandle" und "NewRequestNumber".

```
StringHolder NewRequestNumber = new StringHolder();
StringHolder NewRequestHandle = new StringHolder();
String result;
result = USPSD.createRequest(sid, creatorHandle, attrVals, propertyValues, template,
attributes, NewRequestHandle, NewRequestNumber);
```

Das Handle und die Referenznummer (ref_num) der Anforderung können dem "NewRequestHandle.value" bzw. dem "NewRequestNumber.value" entnommen werden.

Konfiguration der SOAP Webservices

Sie können die SOAP-Webservices von CA SDM mit Einträgen in speziellen Webkonfigurationsdateien konfigurieren. Folgende Tabelle fasst die Namen und Beschreibungen der Konfigurationsoptionen zusammen:

Optionsname	Beschreibung
design_mode_stubs	Versetzt die Webservices in den <i>Design-Modus</i> (nur CA SDM).
require_secure_logon	Macht den Aufruf der Webmethoden „login()“ und „loginService()“ anhand eines sicheren Protokolls wie HTTPS erforderlich.
require_secure_connection	Macht den Aufruf jeder Webmethode anhand eines sicheren Protokolls erforderlich.
disable_user_logon	Deaktiviert die Webmethoden „login()“ und „loginService()“, sodass die Anmeldung nur mit der Methode „loginServiceManaged()“ möglich ist.

CA SDM hat den Integritätsschutz des ausgeführten Tomcat-Servers erhöht, indem die Länge der Attributwerte überprüft wird, die an Webservice-Methoden übergeben werden. Standardmäßig geben Webservices-Aufrufe einen Axis-Fehler zurück, wenn die Länge eines Attributwerts größer als 900 000 Byte ist.

Sie legen folgende Parameter in der Datei "deploy.wsdd" fest:

fatal_max_string_length

Legt die Länge des größten Attributwerts fest, der von einer Webservices-Methode akzeptiert wird.

Standard: 900.000 Byte

validate_parameters

Legt fest, ob die Attributwertlängenüberprüfung ausgeführt wird. Legen Sie den Parameter auf 0 fest, um die Validierung auszuschalten.

Standard "1" (aktiviert)

exception_methods

Zeigt eine kommasetrennte Liste von Webservices-Methoden, die von der Validierung der Attributwertlänge freigestellt sind.

Weitere Informationen:

[Erneute Bereitstellung der Webservices](#) (siehe Seite 586)

Erneute Bereitstellung der Webservices

Die neuen Konfigurationseinstellungen werden bei der erneuten Bereitstellung der Web Services von CA SDM wirksam. Führen Sie die folgenden Schritte aus, um die Webservices erneut bereitzustellen:

1. Öffnen Sie eine Eingabeaufforderung und konfigurieren Sie die Umgebungsvariable „CLASSPATH“ so, dass sie die erforderlichen Axis .jar-Dateien berücksichtigt, die unter <NX_ROOT>/java/lib angegeben werden.

Zur Einrichtung unter Windows führen Sie beispielsweise folgenden Befehl aus:

```
AXISHOME=%NX_ROOT%\java\lib
classpath=
%AXISHOME%\axis.jar;%AXISHOME%\jaxrpc.jar;%AXISHOME%\saa.jar;%AXISHOME%\commons-logging.jar;%AXISHOME%\commons-discovery.jar;%AXISHOME%\wsdl4j.jar;%AXISHOME%\log4j-1.2.8.jar;%classpath%
```

2. Gehen Sie in das Verzeichnis "<NX_ROOT>/sdk/websvc/R11" (bzw. "<NX_ROOT>/sdk/websvc/60" für Webservices der GA Version 6.0), und führen Sie folgende Befehle aus:

```
java org.apache.axis.client.AdminClient undeploy.wsdd
java org.apache.axis.client.AdminClient deploy.wsdd
```

3. Führen Sie Tomcat zurück, indem Sie den CA SDM-Dienst zurückführen. Unter Umständen können Sie vermeiden, das gesamte CA SDM-System herunterfahren zu müssen, indem Sie Tomcat durch die Anwendung folgender Befehle zurückführen:

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

Der Webservice wird erneut bereitgestellt.

4. Sie können dies überprüfen, indem Sie die Axis-Dienstliste unter dem folgenden standardmäßigen URL untersuchen:

```
http://<servername>:<port>/axis/services
```

Hinweis: Die genaue URL hängt von Ihren Installationseinstellungen ab.

Sicherheit von Webservices

Wenn Sie Webservices bereitstellen, sollten Sie sich mit den wichtigen Sicherheitsüberlegungen vertraut machen. Die Standardkonfiguration bei der Verwendung von HTTP ist unsicher, da sie für alle Daten in Webservice-Aufrufen verwendet wird, die zwischen Client und Server im Nur-Text-Format mit dem HTTP-Protokoll über ein Netzwerk übertragen werden. Eingeschlossen sind nicht nur Anwendungsdaten wie Ticket-Beschreibungen und Kontaktnamen, sondern auch Sitzungs-IDs für Web Services (SID). Je nach den verwendeten Anmeldemethoden für Web Service-Anwendungen können auch Kennwörter dazugehören.

Wir empfehlen, dass Administratoren, die Webservices bereitstellen, diesen Abschnitt gründlich lesen und zusätzliche Konfigurationsschritte auf der Anwendungs- und der Netzwerkebene ausführen, um die Sicherheit der Webservice-Umgebung zu gewährleisten.

Wichtig! Die Standardkonfiguration für Webservices mit HTTP ist unsicher und anfällig für Sicherheitsbedrohungen wie Kennwortermittlung, Session Fixation und Datenspionage.

Beim Bereitstellen von Webservices sind drei wichtige Sicherheitsüberlegungen zu berücksichtigen, die in einer Wechselbeziehung stehen:

- Welche Arten der Zugriffsauthentifizierung (Anwendungsebene) soll diese Bereitstellung unterstützen?
- Welche zusätzlichen Sicherheitsfunktionen auf Netzwerkebene erfordert diese Bereitstellung?
- Wie werden diese Erfordernisse durch die Web Services-Konfigurationsoptionen durchgesetzt?

Im Folgenden werden die einzelnen Sicherheitsfunktionen beschrieben:

- **Webservice-Authentifizierungsschemata auf Anwendungsebene** - Für den Zugriff auf Webservices muss eine Webservice-Clientanwendung mit der Webservice-Anwendung authentifiziert werden. Die Webservices bieten zwei Arten der Zugriffsauthentifizierung. Die erste erfordert die Angabe von Anwendername und Kennwort, während die zweite die PKI-Technologie (Public Key Infrastructure) nutzt. Für beide Arten wird die Zugriffssteuerungs- und -verwaltungskomponente in den Webservices unter Verwendung von Zugriffsrichtlinien herangezogen. Zugriffsauthentifizierung und Zugriffsverwaltung sind die wichtigsten Sicherheitsfunktionen von Webservices.

Die Authentifizierung über Anwendernamen/Kennwort kann mithilfe des folgenden Sicherheitskonfigurationsbefehls deaktiviert werden:

```
disable_user_login
```

Vor dem Aktivieren dieser Option muss der Administrator bestimmen, ob jeder Web Service-Client, für den ein Unternehmen den Zugriff auf Web Services anfordert, die alternative Authentifizierungsmethode (die PKI-basierte Anmeldemethode) tatsächlich unterstützt. Der Hauptvorteil der PKI-Technologie besteht darin, dass Webservices-Clientanwendungen keine *verwalteten* Systemanwenderkonten erfordern, d. h. ohne Verwaltung, Speicherung und Übertragung ihrer Kennwörter auskommen.

- **Sicherheitskonfiguration auf Netzwerkebene** - In beiden Authentifizierungsschemata - Anwendername/Kennwort und Public Key Infrastructure (PKI) - wird die von der jeweiligen Anmeldemethode zurückgegebene Sitzungskennung (sowie alle folgenden Informationen) bei Verwendung von HTTP im Nur-Text-Format übertragen. Des Weiteren wird bei Verwendung des Authentifizierungsschemas Anwendername/Kennwort das Kennwort ungeschützt (im Nur-Text-Format) von der Web Service-Client-Anwendung an die Web Services gesendet. Während der Produktentwicklung lagen keine Empfehlungen des W3C zu Standards für die Webservices-Sicherheit vor. Daher wird WS-Security von diesen Webservices-Implementierungen nicht zur Schaffung eines Sicherheitskontexts verwendet. Stattdessen werden Point-to-Point-Protokolle wie SSL/TLS (Secure Sockets Layer/Transport Layer Security) und andere Sicherheitsmechanismen auf Netzwerkebene (zum Beispiel IPSec) empfohlen, um den Austausch von Authentifizierungsdaten auf Anwendungsebene und nachfolgend von Sitzungs-IDs und Daten, der andernfalls im Nur-Text-Format stattfinden würde, zu schützen.

Wichtig! Beim Bereitstellen von Webservices wird SSL (oder HTTPS) empfohlen, um den Austausch von Authentifizierungsdaten auf Anwendungsebene und die nachfolgende Übertragung von Sitzungskennungen und Daten zu schützen.

- **Webservices- Konfiguration** - Um Administratoren zu ermöglichen, die Sicherheit der Kommunikationsprotokollebene auf der Ebene der Webservices-Anwendung zu erzwingen, werden die beiden folgenden Befehle zur Sicherheitskonfiguration unterstützt:

```
require_secure_login
```

Diese Sicherheitsfunktion macht SSL (oder HTTPS) für den Aufruf der Methoden „login()“ und „loginService()“ erforderlich. Diese Funktion bietet außerdem eine einfache Methode zum Schutz des Anwendernamens und des Kennworts, während der zusätzliche Aufwand einer Verwendung von SSL für alle anderen Webservices vermieden wird.

Wichtig! Wenn Sie den Befehl "require_secure_logon" verwenden, bestätigt die Webservices-Anwendung nicht, dass die Sicherheit der Kommunikationsprotokollebene für andere Methoden als "Login()" und "LoginService()" durchgesetzt wird. Falls keine anderen Vorsichtsmaßnahmen getroffen werden, ist es möglich, dass die anderen Webservices-Methoden auf unsichere Weise aufgerufen werden, woraus sich eine größere Anfälligkeit gegenüber Sicherheitsbedrohungen ergibt.

`require_secure_connection`

Diese Sicherheitsfunktion macht die Verwendung von SLL für den Zugriff auf jeden beliebigen Teil der Web Services erforderlich. Sofern HTTPS erforderlich ist, aber nicht verwendet wird, wird ein SOAP-Fault mit dem Code „UDS_SECURE_CHANNEL_REQUIRED“ zurückgegeben.

Hinweis: Weitere Informationen über die Konfiguration von SSL finden Sie in der Dokumentation zu J2EE-Servlet-Containern.

Weitere Informationen:

[Externe Spezifikationen](#) (siehe Seite 594)

Fehlerbehandlung in SOAP

Tritt bei einer Web Services-Methode ein Fehler auf, wird ein SOAP-Fault zurückgegeben. SOAP-Faults sind das standardmäßige Mittel zur Rückgabe von Ausnahmeinformationen für Web Services.

Diese Fehlermeldungen enthalten standardisierte <Message>- und <Code>-Elemente, wobei sich die hilfreichsten Informationen im <Detail>-Element befinden. Das <Detail>-Element enthält wiederum <ErrorCode>- und <ErrorMessage>-Elemente. Das <ErrorCode>-Element gibt einen numerisch kodierten Fehlercode zurück, der entweder für CA SDM oder Knowledge Management spezifisch ist. Das <ErrorMessage>-Element enthält eine Zeichenfolge in englischer Sprache, die den Fehler beschreibt. Die <ErrorMessage>-Elemente sind für die Unterstützung von Entwicklern besonders geeignet und zeigen Anwendern in der Regel hilfreichere Meldungen an.

Das folgende Beispiel veranschaulicht einen SOAP-Fault, der bei Angabe eines ungültigen Parameters in der Methode "getObjectValues()" in CA SDM ausgegeben wird:

```
<soap:Fault>
  <faultcode>soap:Client</faultcode>
  <faultstring>Error on fetch with attribute
list:persistent_id,first_name,last_nameParamErrorHere</faultstring>
  <detail>

<ErrorCode>1001</ErrorCode>

<ErrorMessage> Error on fetch with attribute list:
persistent_id,first_name,last_nameParamErrorHere </ErrorMessage>
  </detail>
</soap:Fault>
```

Wenn Sie einen Client auf Grundlage von Microsoft .NET-verwaltetem Code verwenden, führt ein fehlgeschlagener Web Services-Methodenaufruf zu einer „SOAPException“-Ausnahme. Alle Fehler unterbrechen den aufgerufenen Vorgang.

In einigen Fällen kann der Servlet-Container Fehler schreiben und daher in den Servlet-Container-Protokollen angezeigt werden. In anderen Fällen können Fehlerinformationen in die CA SDM-Protokolle geschrieben werden. Diese Protokolle befinden sich in den folgenden Unterverzeichnissen:

- Im Unterverzeichnis "/bopcfg/www/CATALINA_BASE/logs" der CA SDM-Installation
- Im Unterverzeichnis "/log" der CA SDM-Installation und für alle Protokolle mit dem Präfix "stdlog".

Hinweis: Es empfiehlt sich, diese Protokolle laufend zu überprüfen, da der Server eigene Fehler protokollieren könnte, ohne sie an die Webservices von CA SDM zu melden.

Sperrfehler

CA SDM-Objekte werden während den Aktualisierungen gesperrt. Methoden, die Objekte aktualisieren (z. B. „updateObject()“ oder „transfer()“), geben möglicherweise den folgenden Sperrfehlercode zurück:

UDS_LOCK_ERR

Dieser Code zeigt an, dass ein anderer Benutzer den Datensatz aktualisiert. Oftmals wird die Kennung des sperrenden Benutzers im Element „ErrorMessage“ zurückgegeben.

Zeitüberschreitungen

Wenn der CA SDM-Server stark ausgelastet ist, kann die Verarbeitung einer Methode einige Zeit in Anspruch nehmen. In seltenen Fällen gibt eine Methode überhaupt kein Ergebnis zurück, da keine Reaktion von einem separaten Vorgang erfolgt oder ein anderer Fehler aufgetreten ist. Als Schutz vor übermäßiger Belastung wird jede Webservices-Methode nach Überschreitung einer bestimmten Anzahl von Sekunden unterbrochen. Das Zeitlimit für Webservices-Methoden betrifft den CA SDM-Server, *nicht* jedoch einen Webserver, ein Netzwerk oder Ähnliches.

Hinweis: Die Webservices werden einige Sekunden verzögert, wenn nach Zurückführung des J2EE-Anwendungsservers zum ersten Mal auf sie zugegriffen wird. Dies geschieht aufgrund der Initialisierung der Anwendung, des Ladens von DLLs und von Bibliotheken usw. und erfolgt nur beim erstmaligen Aufruf einer Webservices-Methode. Alle nachfolgenden Aufrufe werden um einiges schneller zurückgegeben.

Bei einer solchen Zeitüberschreitung wird der folgende Fehlercode zurückgegeben:

UDS_TIMEOUT_ERR

Der Vorgang wird nicht abgebrochen! Der Server hat die Request möglicherweise empfangen und wird sie erfolgreich, wenn auch langsam verarbeiten. Ein solches Problem kann auftreten, wenn die Methode "*doSelect()*" zum Abrufen von mehreren 1 000 Datensätzen verwendet wird.

Hinweis: Informationen zur Methode "*doSelect*" finden Sie im *technischen CA SDM-Referenzhandbuch*.

Fehlercodes

Die folgende Tabelle gibt einen Überblick über die möglichen Werte für den <ErrorCode>-Wert in einem durch einen Webservices-Aufruf zurückgegebenen SOAP-Fault:

Fehlername	Wert	Beschreibung
UDS_OK	0	Erfolgreich.
UDS_FAILURE	1	Allgemeiner Fehler, überprüfen Sie die Systemprotokolle.

Fehlername	Wert	Beschreibung
UDS_BAD_PARAM	1000	Es wurde ein ungeeigneter Parameter an die Methode übergeben. Dieser Fehler tritt auf, wenn ein erforderlicher Parameter fehlt, der inkorrekte Typ übergeben oder ein ungültiger Wert verwendet wurde.
UDS_INTERNAL_ERR	1001	Weist darauf hin, dass ein interner Fehler aufgetreten ist. Eine Beschreibung befindet sich im Rückgabe-Array und in den Systemprotokollen.
UDS_LOCK_ERR	1002	Es wurde versucht, ein durch einen anderen Benutzer oder Prozess gesperrtes Objekt zu aktualisieren. Normalerweise wird in den Rückgabedaten die ID des für die Sperrung des Objekts verantwortlichen Kontakts angegeben.
UDS_UPDATE_ERR	1003	Ein Fehler ist bei der Aktualisierung eines Objekts aufgetreten. Vergewissern Sie sich, dass alle erforderlichen Attribute festgelegt wurden, und überprüfen Sie das Systemprotokoll.
UDS_CREATION_ERR	1004	Ein Fehler ist bei der Erstellung eines Objekts aufgetreten. Vergewissern Sie sich, dass alle erforderlichen Attribute festgelegt wurden, und überprüfen Sie die Systemprotokolle.
UDS_NOT_FOUND	1005	Eine Suchmethode konnte Übereinstimmungen oder ein angegebenes Objekt nicht finden. Dies kann der Fall sein, wenn eine ungeeignete oder ungültige Kennung an eine Methode übergeben wird.
UDS_SESSION_TIMEOUT	1006	Für die aktuelle Methode ist ein Zeitlimit abgelaufen, der >USDK>-Server ist womöglich überlastet oder die Methode an sich ist ungeeignet.
UDS_SERVER_GONE	1007	Die CA SDM-Serververbindung wurde unterbrochen, UDS-Methoden funktionieren nicht mehr und alle Listenverweise gehen verloren.
UDS_FETCH_ERR	1008	Ein Fehler ist während des Abrufs von Listendaten aufgetreten.
UDS_BAD_SESSION	1010	Es wurde eine ungültige SID verwendet.
UDS_CNTXT_TIMEOUT	1011	Zeitüberschreitung für die SID.
UDS_SECURE_CHANNEL_REQUIRED	1012	Die Webservices (oder eine Webservice-Methode) erfordern einen sicheren Kanal (z. B. SSL) für den Zugriff, aber es wird ein ungesicherter Kanal verwendet.

Fehlername	Wert	Beschreibung
UDS_SECURITY_VIOLATION	1013	Der versuchte Vorgang verletzt die CA SDM-Sicherheit und wurde abgebrochen.
UDS_OVER_POLICY_LIMIT	3002	Die versuchte Anfrage wurde wegen Überschreitung des in der Richtlinie definierten Limits abgelehnt.

Installation von Webservices

Abhängig von Ihrem Konfigurationstyp installiert CA SDM Webdienste für folgende Server:

- Konventionell: Sowohl Primärserver als auch Sekundärserver. Damit Webservice-Clients eine URL auf einem Sekundärserver verwenden können, fügen Sie dem Sekundärserver eine Web-Engine hinzu.
- Erweiterte Verfügbarkeit: Anwendungsserver

Webservices verwenden den standardmäßigen Objektmanager, der auf dem CA SDM-Server installiert ist. Um einen anderen Objektmanager zu verwenden, installieren Sie diesen, und stellen Sie im Optionsmanager die Option *webservice_domsrvr* ein.

Hinweis: Informationen zum Hinzufügen und Konfigurieren von Objektmanager, Web-Directors und Web-Engines finden Sie im *Administrationshandbuch*. Informationen zum Festlegen und Installieren der Option "webservice_domsrvr" finden Sie in der *Online-Hilfe*.

Aktivieren der Entwicklungszeit

Die Webservices von CA SDM umfassen eine Methodenkonfigurationsfunktion für Entwickler in der Java-Version. Ist diese aktiviert, ignorieren die Webservices den CA SDM-Server und geben simulierte Daten für Methodenaufrufe zurück, damit Webservices-Aufrufe ohne Ausführung eines CA SDM-Servers möglich sind.

Gehen Sie wie folgt vor:

1. Bearbeiten Sie "deploy.wsdd", um die Kommentare der Abschnitte für "design_mode_stubs" zu entfernen.
2. Kehren Sie die Bereitstellung um, und stellen Sie den Server erneut bereit.
3. Starten Sie den Anwendungsserver neu.

Die Entwicklungszeitfunktion wird aktiviert.

Hinweis: Die Entwicklungszeitfunktion gilt ausschließlich für die Webservices-Methoden von CA SDM.

Externe Spezifikationen

In CA SDM können Sie die Zugriffsberechtigung für Anwender und die für die Zugriffssteuerung und Verwaltung verfügbaren Funktionen angeben.

Benutzerzugriffsauthentifizierung

Die CA SDM-Webservices bieten zwei Zugriffsauthentifizierungsschemata. Sie sind mit der neuen Zugriffssteuerungs- und -verwaltungsfunktion verbunden, die eine Zugriffsrichtlinie verwendet.

Benutzername/Kennwort

Überprüft Benutzername/Kennwort, wie in Vorgängerversionen des Produkts beschrieben.

PKI-Technologie (Public Key Infrastructure)

Überprüft, ob die den Zugriff anfordernde Person im Besitz eines bestimmten Privatschlüssels ist.

Wichtig! Wenn Sie die Nutzung einer Anwendung vorsehen, die auf diese Version der Webservices von CA SDM zugreift, wird dringend empfohlen, zunächst eine Webservices-Zugriffsrichtlinie einschließlich ihres Codewerts in CA SDM zu definieren. Eine Standard-Zugriffsrichtlinie mit dem Richtliniencode DEFAULT steht zur Verfügung, wenn CA SDM installiert und konfiguriert wurde.

Weitere Informationen:

[Definieren einer Zugriffsrichtlinie](#) (siehe Seite 603)

Benutzername/Kennwort-Authentifizierung

Falls Sie die Zugriffsauthentifizierung anhand von Benutzername/Kennwort vorsehen, muss die Benutzeranwendung eine der zwei folgenden Webservices-Methoden aufrufen, um Zugriff auf die Webservices von CA SDM zu erhalten.

Hinweis: Der von Ihnen im Benutzernamenparameter festgelegte Anmeldebenutzer (nicht der in der Richtlinie angegebene Proxy-Kontakt) ist für die in einer Sitzung begonnenen Aktivitäten verantwortlich. Die gesamte Funktionsgruppensicherheit und Datenaufteilung wird für diesen Anmeldebenutzer erzwungen.

login (Benutzername, Kennwort)

Diese Methode gewährleistet die Rückwärtskompatibilität, wobei die Zugriffsauthentifizierung anhand des gleichen Benutzernamens und Kennworts erfolgt. Eine SID (Sitzungs-ID) wird nur bei Authentifizierung des Zugriffs zurückgegeben. Alle nachfolgenden Webservices-Aufrufe müssen diese SID einschließen. Die Standard-Zugriffsrichtlinie wird daraufhin auf alle nachfolgenden Webservices-Zugriffe angewendet, die durch diese SID gekennzeichnet sind.

Der Benutzername und das Kennwort sind erforderliche Felder, die im Nur-Text-Format definiert werden müssen.

loginService (Benutzername, Kennwort, Richtlinien)

Diese Methode ähnelt der oben erwähnten Anmeldefunktion insoweit, dass die Zugriffsauthentifizierung anhand des gleichen Benutzernamens und Kennworts erfolgt. Eine SID wird nur bei Authentifizierung des Zugriffs zurückgegeben. Es wird hierbei jedoch eine spezifische Zugriffsrichtlinie, die durch den dritten Parameter festgelegt wird, zur Steuerung und Verwaltung aller nachfolgenden Webservices-Zugriffe herangezogen. Bei fehlender Angabe im Richtlinienparameter findet automatisch die Standardrichtlinie Anwendung.

Der Benutzername und das Kennwort sind erforderliche Felder, die im Nur-Text-Format definiert werden müssen. Die Richtlinie ist erforderlich, der Parameter kann jedoch leer sein. Die Angabe muss im Nur-Text-Format erfolgen. Verwenden Sie den in einer Richtlinie verwendeten Richtliniencode.

Wie eine Anmeldung validiert wird, hängt vom zugewiesenen *Zugriffstyp* des Kontakts ab. Das Zugriffstypobjekt wird von CA SDM gehostet und legt den Validierungstyp fest. Sie können das Produkt verwenden, um den Zugriffstypdatensatz anzuzeigen, und Sie können auch die "getAccessTypeForContact()" -Webmethode verwenden, um beliebige Informationen zum Zugriffstypobjekt abzurufen.

Hinweis: Weitere Informationen zu Zugriffstypen finden Sie im *Administrationshandbuch*.

PKI-Authentifizierung (Public Key Infrastructure)

Falls Sie die Verwendung der PKI-Authentifizierung vorsehen, müssen Sie sich darüber bewusst sein, dass der Inhalt der Anmeldungsanfrage anhand eines privaten Schlüssels verschlüsselt wird, der nur anhand des entsprechenden öffentlichen Schlüssels entschlüsselt werden kann. Die Reaktion auf die Anmeldungsanfrage wird im Nur-Text-Format zurückgegeben.

Im Allgemeinen wird jeder Anwendung, die auf die Webservices von CA SDM zugreift, eine Richtlinie zugewiesen. Die Webservices von CA SDM speichern detaillierte Informationen über eine Richtlinie, einschließlich des öffentlichen Schlüssels eines digitalen Zertifikats. Eine Anwendung als "Besitzer" einer Richtlinie verwendet den privaten Schlüssel des digitalen Zertifikats und den Richtliniencode (als Richtlinien-ID) zur Zusammenstellung einer Anmeldungsanfrage.

loginServiceManaged (Policy, Encrypted_Policy)

Die Webservices von CA SDM führen die Benutzerauthentifizierung durch, indem die Richtlinie anhand des Nur-Text-Richtliniencodes gesucht, der mit der Richtlinie verbundene öffentliche Schlüssel des Richtlinienbesitzers abgerufen, der verschlüsselte Richtliniencode entschlüsselt, der entschlüsselte Inhalt mit dem Richtliniencode abgeglichen und schließlich eine Sitzung auf dem Backend-Server eröffnet wird. Die Sitzungs-ID (SID) im Nur-Text-Format wird zurückgegeben und kann für nachfolgende Methodenaufrufe verwendet werden. Nur der Richtlinienbesitzer verfügt über den privaten Schlüssel, der dem in CA SDM gespeicherten, zugewiesenen öffentlichen Schlüssel der Richtlinie entspricht.

Alle nachfolgenden Webservices-Aufrufe müssen die zurückgegebene Sitzungs-ID (SID) einschließen. Der in der Richtlinie festgelegte Proxy-Kontakt ist für alle während dieser Sitzung eingeleiteten Webservices-Aktivitäten verantwortlich. Die gesamte Funktionsgruppensicherheit und Datenaufteilung wird für den Proxy-Kontakt erzwungen.

Wichtig! Der Parameter „Encrypted_Policy“ sollte im BASE64-Textformat vorliegen. Die Benutzeranwendung muss geeignete Konvertierungen aus dem Binärformat durchführen.

Die Richtlinie ist ein erforderliches Feld. Wenn Sie sie definieren, verwenden Sie Nur-Text-Richtliniencode, wie in einer Richtlinie definiert. „Encrypted_Policy“ (die digitale Unterschrift des Richtliniencodes, die mit dem privaten Schlüssel des Richtlinienbesitzers verschlüsselt wird) ist erforderlich. Verwenden Sie bei der Definition von „Encrypted_Policy“ den Algorithmus SHA1 mit RSA, um die digitale Unterschrift abzurufen.

Implementieren von "loginServiceManaged" in Java

Im Folgenden wird gezeigt, wie Zertifikate generiert und anschließend für den Zugriff auf die CA SDM-Webservices verwendet werden.

Im folgenden Beispiel wird der Anmeldeprozess mit dem CA SDM-Zertifikat abgeschlossen. Im Anschluss werden zwei allgemeine Webservice-Aufrufe ausgeführt. Die Webservice-Methode "getBopsid()" ermöglicht den Abruf eines Token, das mit einem bestimmten Anwender verknüpft ist. Dieses Token kann für die Anmeldung über die Web-Schnittstelle von CA SDM als verknüpfter Anwender verwendet werden, ohne dass eine Kennworteingabe erforderlich ist. Auf diese Weise ist eine nahtlose Integration verschiedener Anwendungen möglich.

Wichtig! Das generierte BOPSID-Token verfällt nach 30 Sekunden und muss daher unverzüglich verwendet werden.

Wichtig! Es gibt ein bekanntes Problem beim Verwenden der Version 1.4 des AXIS-Tool. Weitere Informationen finden Sie in den *Versionshinweisen*.

Gehen Sie wie folgt vor:

1. Generieren Sie die Stub-Klassen mit AIXS Tool WSDL2Java. Weitere Informationen finden Sie im Abschnitt "Generieren von Stub-Klassen mit AXIS Tool WSDL2Java" aus der Datei "PKI_loginServiceManaged_JAVA_steps". Die Datei befindet sich im folgenden Verzeichnis:

```
$NX_ROOT/samples/sdk/websvc/java/test1_pki
```

2. Starten Sie den CA SDM-Service.
3. Führen Sie "pdm_pki -p DEFAULT" aus.

"DEFAULT.p12" wird im aktuellen Verzeichnis erstellt. Das Kennwort dieser Richtlinie entspricht dem Richtliniennamen (in diesem Fall DEFAULT).

Hinweis: Dieser Befehl fügt außerdem dem Feld "pub_key" (Attribut "public_key") in der Tabelle bzw. dem Objekt "sapolicy" den öffentlichen Schlüssel des Zertifikats hinzu.

4. Melden Sie sich bei CA SDM an
5. Wählen Sie auf der Registerkarte "Administration" die Option "SOAP-Webservices-Richtlinie", "Richtlinien" aus.

Das Fenster "SOAP-Webservices-Zugriffsrichtlinien - Liste" wird angezeigt.

6. Klicken Sie auf "STANDARD".

Das Fenster "SOAP-Webservices-Zugriffsrichtlinien - Detail" wird angezeigt.

7. Füllen Sie das Feld "Proxy-Kontakt" (in diesem Beispiel "ServiceDesk") aus, und überprüfen Sie, ob im Datensatzfeld "Schlüssel" der Richtlinie DEFAULT der Wert "Ja" angezeigt wird.
8. Kopieren Sie DEFAULT.p12 (aus dem Verzeichnis, wo der Befehl "pdm_pki" ausgeführt wird), die JSP-Datei *pkilogin.jsp* und die HTML-Datei *pkilogin.htm* (aus dem Verzeichnis "\$NX_ROOT/samples/sdk/websvc/java/test1_pki") in das folgende Verzeichnis:

\$NX_ROOT/bopcfg/www/CATALINA_BASE/webapps/axis

9. Öffnen Sie das HTML-Formular (aus dem Axis-Verzeichnis). Beispiel:
`http://localhost:8080/axis/pkilogin.htm`

Füllen Sie die gewünschten Felder aus.

Hinweis: Das Feld "Verzeichnis" gibt den Speicherort der Zertifikatdatei an. Ändern Sie den Pfad so, dass der korrekte Speicherort angegeben wird.

10. Klicken Sie auf "Anmelden".

Die Ergebnisseite wird geöffnet.

11. Klicken Sie auf die BOPSID-URL.

Wichtig! Klicken Sie sofort auf die URL! BOPSID verfügt über ein Token mit einer beschränkten Lebensdauer von etwa 30 Sekunden.

URLs, die eine BOPSID verwenden, haben folgendes Format:

`http://<server name>:<port>/CAisd/pdmweb.exe?BOPSID=<BOPSID value>`

Hinweis: Um die Methode "loginServiceManaged" für ein auf AIX ausgeführtes Java-Clientprogramm zu verwenden, müssen Sie u. U. einige Sicherheitsrichtliniendateien innerhalb von JAVA_HOME ersetzen. Wechseln Sie zu <http://www.ibm.com>, und suchen Sie nach "developerworks java technology security information AIX". Klicken Sie im Dokument "developerWorks : Java technology : Security" auf die Verknüpfung "IBM SDK Policy files". Laden Sie die uneingeschränkten Richtliniendateien "local_policy.jar" und "US_export_policy.jar" herunter. Ersetzen Sie die Originaldateien im Verzeichnis "JAVA_HOME/lib/security" durch diese Dateien.

Konfiguration für den PKI-Authentifizierungstyp

Um die Konfiguration für die PKI-Authentifizierung durchzuführen, muss zunächst eine Zugriffsrichtlinie erstellt werden. Der Prozessablauf ist wie folgt:

Erstellen einer Zugriffsrichtlinie

Der Administrator führt diese Aufgabe über das Produkt (nur Web-Schnittstelle) aus und weist als Teil des Verfahrens jeder Zugriffsrichtlinie einen eindeutigen Textcode zu.

Abrufen eines digitalen Zertifikats mit einem öffentlichen/privaten Schlüsselpaar und Zuweisen zur Zugriffsrichtlinie

Bei der PKI-Zugriffsauthentifizierung ist für eine Benutzeranwendung ein digitales Zertifikat mit einem öffentlichen Schlüssel und einem privaten Schlüssel erforderlich. Ein Administrator kann solch ein Zertifikat von einer Zertifizierungsstelle erwerben oder anhand von Sicherheitsprodukten, die digitale Zertifikate unterstützen. CA SDM umfasst ein serverseitiges Dienstprogramm, mit dem ein digitales Zertifikat generiert werden kann. Es befindet sich im Verzeichnis "<NX_ROOT>/bin/<cs>" und wird wie folgt aufgerufen:

```
pdm_pki -p policy_code [-l certificate file] [-f] [-h]
```

-p

Identifiziert einen eindeutigen Richtliniencode.

-f

Lässt zu, dass das Dienstprogramm den vorhandenen öffentlichen Schlüssel durch einen neuen ersetzt.

-l

Lädt den gespeicherten öffentlichen Schlüssel in ein X509 V3-Zertifikat.

-h

Zeigt Hilfe zum Befehlszeilenfenster an.

Wenn Sie ein digitales Zertifikat von einem Drittanbieter, CA Technologies oder anhand eines Sicherheitsprodukts erwerben, importieren Sie es an den Speicherort des CA SDM-Servers und weisen es anschließend einer Zugriffsrichtlinie zu. Der Administrator der Benutzeranwendung sollte eine digitale Zertifikatsdatei erwerben, die den Inhalt eines X509v3-Zertifikats im DER/ASN.1-Format aufweist.

Darüber hinaus sollte das Zertifikat nur den öffentlichen Schlüssel des Schlüsselpaars enthalten. Mit der Option „-l“ sollte der Administrator das Tool „pdm_pki“ aufrufen, um das Zertifikat zu laden. Das Tool lädt daraufhin das Zertifikat, extrahiert den öffentlichen Schlüssel, konvertiert ihn in das BASE64-Textformat und speichert ihn mit der durch den Richtliniencode angegebenen Zugriffsrichtlinie.

Wenn das Generieren des digitalen Zertifikats durch das Dienstprogramm "pdm_pki" erfolgt, ruft der Administrator den Befehl in CA SDM ohne die Option "-l" auf. Das Tool erzeugt daraufhin ein Schlüsselpaar aus öffentlichem und privatem Schlüssel (dies sind 1024 Bit lange RSA-Schlüssel). Der öffentliche Schlüssel wird in das BASE64-Textformat konvertiert und zusammen mit der durch den Richtliniencode festgelegten Zugriffsrichtlinie gespeichert. Es werden außerdem ein X509v3-Zertifikat für den öffentlichen Schlüssel sowie weitere Informationen erzeugt (die standardmäßige Passphrase wird als Richtliniencode verwendet). Schließlich wird das X509 V3-Zertifikat mit dem privaten Schlüssel in ein portables Standardzertifikatsformat für PKCS12 verpackt. Daraufhin wird es in einer Datei mit dem vom angewendeten Richtliniencode abhängigen Namen *Richtliniencode.p12* gespeichert. Diese Datei kann nun auf Clients exportiert werden.

Hinweis: Wurde eine Zugriffsrichtlinie bereits einem öffentlichen Schlüssel eines Zertifikats zugewiesen, müssen Benutzer beim Aufruf des Befehls "pdm_pki" die Option "-f" festlegen, um den vorhandenen durch einen neuen öffentlichen Schlüssel zu überschreiben.

Weitere Informationen:

[Definieren einer Zugriffsrichtlinie](#) (siehe Seite 603)

Anmelden bei Web Services

Im Folgenden wird der Prozessablauf für die Anmeldung bei den mit der PKI-Authentifizierung konfigurierten Webservices beschrieben:

Verfahren	Beschreibung
Laden des digitalen Zertifikats und Extrahieren des privaten Schlüssels	Das digitale Zertifikat muss in einem sicheren Speicher auf Benutzerseite abgelegt werden, wo es abgerufen und für die Anmeldung bei den Webservices verwendet werden kann. Beispiele für sichere Speicher: ■ Zertifikatsspeicher von Windows ■ Zertifikatsspeicher von Java (durch „java_keytool“ verwaltet) ■ Zertifikatsspeicher (von anderen CA Technologies-Sicherheitsprodukten erstellt). Eine Benutzeranwendung sollte in der Lage sein, das digitale Zertifikat zu laden und den privaten Schlüssel anhand geeigneter APIs je nach Benutzerumgebung zu extrahieren.

Verfahren	Beschreibung
Erzeugen einer digitalen Unterschrift des Nur-Text-Richtliniencodes mit dem privaten Schlüssel	Nachdem der private Schlüssel aus dem digitalen Zertifikat extrahiert wurde, kann er zur Erzeugung einer digitalen Unterschrift für den Richtliniencode verwendet werden. Bei der Erzeugung einer digitalen Unterschrift wird ein Digest eines Texts mit einem privaten Schlüssel verschlüsselt. Bei dem Digest-Algorithmus muss es sich um standardmäßiges SHA1 handeln, während der Verschlüsselungsalgorithmus RSA sein sollte. Außerdem muss die binäre digitale Unterschrift in das BASE64-Textformat konvertiert werden, bevor sie für Anmeldungen bei den Webservices verwendet werden kann. Abhängig von den Benutzerumgebungen sind geeignete API-Aufrufe zur Archivierung dieser Informationen zu verwenden.
Durchführen des Web Services-Aufrufs	Eine Benutzeranwendung sollte die Web Services-Methode „loginServiceManaged()“ zusammen mit dem Nur-Text-Richtliniencode sowie der digitalen Unterschrift im BASE64-Textformat aufrufen.
Abrufen der zurückgegebenen SID	Wenn die Zugriffsanforderung erfolgreich authentifiziert wurde, wird automatisch eine SID im Nur-Text-Format zurückgegeben.

Nachdem die SID erzeugt wurde, wird eine erfolgreiche Verbindung zwischen einer Webservices-Sitzung und einer Zugriffsrichtlinie hergestellt. Mit dieser SID kann die Benutzeranwendung auch andere Webservices-Methoden aufrufen, wobei der gesamte Zugriff auf Webservices von dieser Zugriffsrichtlinie gesteuert und verwaltet wird.

Sitzung und Autorisierung

Bei erfolgreicher Validierung wird eine SID zurückgegeben, die mit dem validierten Benutzernamen verbunden ist. Dabei spielt es keine Rolle, ob dies der für die Anmeldung angegebene Benutzername oder der in einer Richtlinie festgelegte Proxy-Kontakt ist. Aufgrund dieses Prozesses werden jedem CA SDM-Benutzer Sicherheitsberechtigungen zugewiesen, die in Ihrer Webservices-Anwendung erzwungen werden können.

Für einen Benutzer kann z. B. eine Datenpartition gelten, durch die die von ihm einsehbaren Anfragen eingeschränkt werden. Bei Verwendung einer SID zum Abrufen von Anfrageninformationen für diesen Benutzer sorgt das CA SDM-System dafür, dass die Datenpartition erzwungen wird.

Die Funktionsgruppensicherheit wird ebenfalls angewendet. Wenn ein Benutzer z. B. keinen Zugriff auf die Funktionsgruppe „Aufrufmanager“ hat, wird der Aufruf beliebiger Webservices-Methoden, wie z. B. zur Anzeige oder Erstellung von Anfragen, unterbunden, da der Zugriff auf die Funktionsgruppe "Aufrufmanager" verweigert wird.

Nach Abschluss der Anwendungsnutzung durch einen Benutzer ist die Gültigkeit der SID mit der Methode „Logout()“ aufzuheben.

Jede SID läuft nach einer bestimmten Inaktivitätsperiode ab. Dies bedeutet, dass eine SID abläuft, sobald das Intervall zwischen zwei Methodenaufrufen größer als ein bestimmter Zeitüberschreitungswert ist. Dieses Zeitlimitintervall wird im Optionsmanager eingestellt und durch folgende CA SDM-Option festgelegt:

```
'webservice_session_timeout'
```

Wird dieser Wert auf null (0) gesetzt, dann läuft eine SID niemals ab. Wenn diese Option fehlt oder nicht festlegt wird, gilt der Standardwert von einer Stunde. Wird eine Web Services-Methode mit einer abgelaufenen SID aufgerufen, wird beim ersten Mal ein Fehler mit dem Code „UDS_SESSION_TIMEOUT“ und bei jedem weiteren Mal ein Fehler mit dem Code „UDS_BAD_SESSION“ zurückgegeben.

Damit eine SID aktiv bleibt, muss eine beliebige Web Services-Methode vor Erreichen des Zeitüberschreitungswerts aufgerufen werden. Damit die SID ohne Verwendung des Servers aktiv bleibt, rufen Sie die Methode „serverStatus()“ auf.

Zugriffssteuerung und -verwaltung

Um das Risiko des Aufkommens übermäßig vieler Webservice-Tickets zu verringern und die Stabilität des CA SDM-Servers zu gewährleisten, wird in dieser Version der CA SDM-Webservices ein Zugriffssteuerungs- und -verwaltungssystem verwendet. Es dient hauptsächlich zur Verarbeitung übermäßiger Serviceaktivitäten, die von vertrauenswürdigen Benutzeranwendungen etwa infolge von Programmierfehlern oder Ausnahmen eingeleitet werden. Außerdem dient es als eine Barriere zur Unterbindung böswilliger Zugriffe auf CA SDM-Webservices. Der Administrator einer Webservice-Anwendung kann eine Zugriffsrichtlinie in CA SDM erstellen und definieren, mit der der Zugriff auf die Webservices von CA SDM aus der Webservice-Anwendung heraus gesteuert wird.

Hinweis: Es wird eine Standardzugriffsrichtlinie mit dem Code DEFAULT bereitgestellt. Die Standard-Zugriffsrichtlinie enthält keine Zugriffseinschränkungen und wird nur auf Sitzungen angewendet, die anhand von Anwendernamen und Kennwort authentifiziert werden.

Definieren einer Zugriffsrichtlinie

Um eine Zugriffsrichtlinie für SOAP-Webservices zu erstellen, muss ein Administrator eine Zugriffsrichtlinie definieren.

So definieren Sie die Zugriffsrichtlinie

1. Klicken Sie auf die Registerkarte "Administration".
2. Klicken Sie in der Baumstruktur links auf "SOAP-Webservices-Richtlinie", "Richtlinien".
Die Seite "SOAP-Webservices-Zugriffsrichtlinien - Liste" wird angezeigt.
3. Klicken Sie auf "Neu erstellen".
Das Dialogfeld "Neue SOAP-Webservices-Zugriffsrichtlinie erstellen" wird angezeigt.
4. Geben Sie die Informationen für die neue Zugriffsrichtlinie ein.

Hinweis: Der Standardwert "-1" in einem beliebigen Vorgangszähler weist darauf hin, dass für den entsprechenden Vorgang keine Einschränkungen gelten. Ein Wert von 0 (null) zeigt an, dass der entsprechende Vorgang unzulässig ist.

Symbol

(erforderlich) Gibt einen symbolischen Namen für die Zugriffsrichtlinie an.

Code

(erforderlich) Gibt den eindeutigen Text an, der diese Zugriffsrichtlinie identifiziert.

Status

(erforderlich) Gibt den Status einer Zugriffsrichtlinie an. Inaktive Richtlinien werden nicht verwendet.

Proxy-Kontakt

Gibt den Kontakt an, der für sämtliche Webservices-Vorgänge und die CA SDM-Sicherheit zuständig ist.

Standard

Gibt die Standardrichtlinie an. Legen Sie diese Richtlinie als die Standardrichtlinie fest. Es darf nur eine aktive Standardrichtlinie vorhanden sein. Durch die Erstellung einer neuen Standardrichtlinie verliert die aktuelle Standardrichtlinie automatisch ihren Standard-Status.

Schlüssel vorhanden

(schreibgeschützt) Gibt an, ob dieser Richtlinie ein öffentlicher Schlüssel zugewiesen wurde. Dieses Feld wird aktualisiert, sobald einer Richtlinie anhand des Programms "pdm_pki" ein öffentlicher Schlüssel zugewiesen wird.

Identitätswechsel zulassen

Identifiziert die Berechtigung "Identitätswechsel zulassen". Wenn dieses Feld festgelegt wird, kann der Richtlinienbesitzer die Webservices-Methode "impersonate()" aufrufen und eine neue Webservices-Sitzung im Namen des nachgeahmten Anwenders erstellen. Zusätzliche Zugriffsauthentifizierungen werden bei der Erstellung der Sitzung nicht durchgeführt. Allerdings lässt sich diese Methode nur dann erfolgreich aufrufen, wenn "access_level" im neuen Zugriffstyp für den Anwender kleiner oder gleich "grant_level" im Zugriffstyp des Proxy für den Anwender ist.

Beschreibung

Gibt die ausführliche Beschreibung dieser Zugriffsrichtlinie an.

Ticket-Erstellung

Gibt die Anzahl der pro Stunde zulässigen Ticketeinführungsvorgänge (Aufruf-Request, Change und Issue) an.

Objekt-Erstellung

Gibt die Anzahl der pro Stunde zulässigen CA SDM-Objekteinführungsvorgänge (abgesehen von Ticket-Objekten) an.

Objekt-Aktualisierungen

Gibt die Anzahl der pro Stunde zulässigen CA SDM-Objektaktualisierungsvorgänge an.

Anhänge

Gibt die Anzahl der pro Stunde zulässigen, mit Anhängen verbundenen Vorgänge an.

Datenabfragen

Gibt die Anzahl der pro Stunde zulässigen Datenabfragevorgänge an.

Wissen

Gibt die Anzahl der pro Stunde zulässigen wissensbezogenen Vorgänge an.

5. Klicken Sie auf "Speichern".

Die SOAP-Webservices-Richtlinie wird definiert.

Webservices-Methoden nach Kategorie

Jede CA SDM-Webservices-Methode gehört zu einer bestimmten Kategorie. Im Folgenden werden alle Kategorien mit ihren dazugehörigen Methoden aufgelistet:

Ticket-Erstellung

- createTicket()
- createQuickTicket()

- createRequest()
- createChangeOrder()
- createIssue()

Objekt-Erstellung

- logComment()
- createAsset()
- addAssetLog()
- createAssetParentChildRelationship()
- createObject()
- createWorkFlowTask()
- createActivityLog()
- notifyContacts()
- addBookmark()
- addComment()
- createFolder()

Objekt-Aktualisierungen

- addMemberToGroup()
- removeMemberFromGroup()
- closeTicket()
- createLrelRelationships()
- removeLrelRelationships()
- deleteWorkFlowTask()
- updateObject()
- transfer()
- escalate()
- attachChangeToRequest()
- detachChangeFromRequest()
- changeStatus()
- clearNotification()
- updateLrel()
- deleteBookmark()
- updateRating()

Anhänge

- createAttmnt()
- createAttachment()
- attachURLLink()
- deleteAttmnt()
- deleteComment()
- removeAttachment()

Datenabfragen

- impersonate()
- serverStatus()
- getBopsid()
- getConfigurationMode()
- getHandleForUserid()
- getAccessTypeForContact()
- getPermissionsGroup
- getObjectTypeInfoInformation()
- getRelatedList()
- getRelatedListValues()
- getGroupMemberListValues()
- getPendingChangeTasksForContact()
- getPendingIssueTasksForContact()
- getWorkFlowTemplates()
- getWorkflowTemplateList()
- getTasksListValues()
- getNotificationsForContact()
- getPolicyInfo()
- getAssetExtensionInformation()
- getLrelValues()
- getObjectValues()
- doSelect()
- doQuery()
- getPropertyInfoForCategory()

- `getValidTaskTransitions()`
- `getListValues()`
- `getListInfo()`
- `findContact()`
- `getAttmntInfo()`
- `getAttmntList()`
- `getBookmarks()`
- `getCategory()`
- `getComments()`
- `getContact()`
- `getDecisionTrees()`
- `getDocument()`
- `getDocumentTypes()`
- `getFolderInfo()`
- `getFolderList()`
- `getLrelLength()`
- `getPriorities()`
- `getRepositoryInfo()`
- `getStatuses()`
- `getTemplateList()`

Wissen

- `createDocument()`
- `deleteDocument()`
- `doSelectKD()`
- `faq()`
- `attmntFolderLinkCount()`
- `getAttmntListPerKD()`
- `isAttmntLinkedKD()`
- `getDocumentByIDs()`
- `getKDListPerAttmnt()`
- `getQuestionsAsked()`

- `modifyDocument()`
- `rateDocument()`
- `search()`

Wenn eine Zugriffsrichtlinie von CA SDM aktualisiert wird, werden die entsprechenden Richtlinieninformationen dynamisch durch die Webservices aktualisiert. Aktive Web Services-Sitzungen, die von dieser Richtlinie gesteuert werden, werden weiterhin von Konfigurationen in der Richtlinie gesteuert. Für neue Web Services-Sitzungen, die von dieser Richtlinie verwaltet und gesteuert werden, gelten die jeweils neuesten Konfigurationen.

Hinweis: Informationen zu den einzelnen Methoden finden Sie im *technischen CA SDM-Referenzhandbuch*.

Definieren von Fehlertypen

Fehlertypen werden zum Zeitpunkt der Erstellung von Tickets zugewiesen, wobei eine Zugriffsrichtlinie einen Satz dieser Fehlertypen definiert. Eine Benutzeranwendung, die die Webservices von CA SDM nutzt, kann systemnahe Webmethoden zur Ticket-Erstellung (Anfrage, Change oder Issue) verwenden. Dabei wird einer dieser Typen angegeben, um den im Ticket angesprochenen Fehler zu kategorisieren. Fehlertypen können nur mit der systemunabhängigen Methode `"createTicket()"` verwendet werden. Für systemnahe Methoden, z. B. `"createRequest()"`, werden keine Fehlertypen verwendet.

Weitere Informationen:

[Vereinfachter Webservices-Zugriff](#) (siehe Seite 611)

Webservices-Fehlertypen

Webservices von CA SDM stellen außerdem eine definierte Gruppe von Standardfehlertypen zur Verfügung, die für *jede* Richtlinie erstellt werden. Diese Standardtypen, als *interne* Fehlertypen bezeichnet, können deaktiviert, jedoch nicht gelöscht werden. Im Produkt können Sie auf der Seite "Webservices-Zugriffsrichtlinien - Detail" sehen, welche Standardfehlertypen bereitgestellt werden, wenn eine neue Richtlinie erstellt wird.

Die folgenden Informationen beschreiben die einzelnen internen Fehlertypen:

ACCESS_ERROR

Zeigt an, dass das System keine Verbindung zu einer Ressource aufnehmen oder eine Ressource nicht finden konnte, wie z. B. eine Datei, eine Website usw.

EXCEPTION_FATAL

Zeigt an, dass die Anwendung unerwartet herunterfährt.

EXCEPTION_RUNTIME

Zeigt an, dass der Anwendungscode auf eine Ausnahme gestoßen ist.

LOGIN_ERROR

Zeigt an, dass der Bediener keinen Zugriff auf die Anwendung erhalten hat.

Zusätzliche Fehlertypen

Der Administrator einer Zugriffsrichtlinie kann zusätzliche Fehlertypen hinzufügen, wie in den folgenden Informationen beschrieben:

Fehlertyp	Beschreibung
Ticket-Vorlage	Gibt eine Vorlage für einen Incident bzw. Fehler, Issue oder Change an, die Sie bei Meldung dieses Fehlertyps zur Erstellung eines Tickets verwenden. Hinweis: Der Kontakt, der der Richtlinienbesitzer ist, wird als Endbenutzer verwendet. Ticket-Typ und Ticket-Vorlagenname definieren die Ticket-Vorlage.
Standard	Zeigt an, ob dieser Fehlertyp der Standard für die Richtlinie ist. Pro Richtlinie ist nur ein Standard zulässig. Hinweis: Ein neuer Standardfehlertyp überschreibt den vorhandenen Standardfehlertyp, der der Richtlinie zugeordnet ist.
Aktiv	Stellt einen aktiven Fehlertyp dar. Hinweis: Durch einen inaktiven Typ werden keine Tickets erstellt.
Intern	Identifiziert das Feld als schreibgeschützt, das angibt, ob dieser Fehlertyp ein interner Standardfehlertyp ist.
Symbol	Gibt den symbolischen Namen des Fehlertyps an.
Code	Gibt die eindeutige Textkennung des Fehlertyps an.
Beschreibung	Eine ausführliche Beschreibung des Fehlertyps.
Duplikat-Behandlung	Definiert die Aktion, die durchzuführen ist, wenn das Produkt ein bereits vorhandenes, identisches Ticket entdeckt.

Fehlertyp	Beschreibung
Rückgabedaten	Gibt die benutzerdefinierte Rückgabemeldung an, die Sie für die Webmethode „createTicket()“ zur Rückgabe an Client-Anwendungen festlegen können. Rückgabedaten können zur Angabe einer Aktion, die von der Anwendung durchzuführen ist (Anwendungsdatenrückgabe), oder einer Meldung (Benutzerdatenrückgabe), die dem Endbenutzer angezeigt werden soll, verwendet werden.

Weitere Informationen:

[Ticketduplikatbehandlung](#) (siehe Seite 610)

Ticketduplikatbehandlung

Die Web Services-Zugriffsrichtlinie kann Ticketduplikate erkennen und behandeln, was zur Vermeidung eines übermäßigen Aufkommens von Tickets beiträgt. Bei einem erstellten Ticket handelt es sich potenziell um ein Duplikat, wenn alle der folgenden Bedingungen erfüllt sind:

- Mindestens ein Ticket des gleichen Typs (cr, lss oder chg) ist bereits vorhanden und AKTIV.
 - Das vorhandene Ticket wurde vom Web Service erstellt.
 - Das vorhandene Ticket wurde anhand der gleichen Richtlinie und des gleichen Fehlertyps wie das neu erstellte Ticket erstellt.
 - Das Erstellungsdatum des vorhandenen Tickets befindet sich innerhalb eines bestimmten Zeitraums (Beispiel: Es wurde vor weniger als 2 Tagen geöffnet).
- Hinweis:** Das Feld für das Erstellungsdatum wird anhand des maximalen Zeitintervalls für die Suche nach Duplikaten konfiguriert.
- Das Duplikat der ID entspricht der vom Benutzer beim Aufrufen der Methode „createTicket()“ angegebenen ID.

Benutzer können ebenfalls zur Vermeidung von Duplikaten beitragen, indem Sie Tickets auf Grundlage von dem Benutzer bekannten Kriterien als eindeutig oder unterschiedlich klassifizieren. Fügen Sie hierzu einen optionalen Zeichenfolgeparameter zum Webservices-Aufruf "createTicket" hinzu. Bei aktivierter Duplikatbehandlung wird der Zeichenfolgeparameter überprüft, nachdem andere Duplikatbehandlungskriterien zur Feststellung, ob dies ein eindeutiger oder doppelter Aufruf dieser Methode ist, betrachtet wurden.

Ergebnisse von Duplikat-Tickets

Führt die Ticketerstellung zu einem Duplikat, kann der vorhandene Fehlertyp zur Ausführung einer der folgenden Aktionen konfiguriert werden:

Neu konfigurierter Fehlertyp	Ergebnisse
Neues Ticket erstellen und Duplikat ignorieren	Es wird eine neue Ticketkennung und -nummer zurückgegeben (Standard).
Neues Ticket nicht erstellen, stattdessen ein Aktivitätsprotokoll zum vorhandenen Ticket hinzufügen	Die Ticketkennung und vorhandene Ticketnummer werden zurückgegeben.
Neues Ticket nicht erstellen, stattdessen einen Eintrag im CA SDM-Standardprotokoll hinzufügen	Die Ticketkennung und vorhandene Ticketnummer werden zurückgegeben.
Neues Ticket erstellen und als untergeordnetes Element an das vorhandene Ticket anhängen	Es wird eine neue Ticketkennung und -nummer zurückgegeben.

Vereinfachter Webservices-Zugriff

Die Webservices von CA SDM bieten einen gekürzten Satz von systemunabhängigen Webservices-Methoden, bei denen es sich um vereinfachte Versionen von vorhandenen Webservices-Methoden handelt. Die Mehrzahl der Benutzeranwendungen benötigt keinen kompletten Satz von Webservices-Methoden, um Service Desk-Dienste über die Webservices von CA SDM anzufordern. Dieser Satz von systemunabhängigen Webservices-Methoden ist eng mit benutzerdefinierten Zugriffsrichtlinien verbunden und verwendet in den Richtlinien definierte Standardparameter. Er lässt sich auch mit geringen Kenntnissen des CA SDM-Objektschemas verwenden. Daneben decken die systemunabhängigen Methoden einen häufig verwendeten Satz von CA SDM-Funktionen ab, die von den meisten Anwendungen mit Service-Erkennung benötigt werden.

Im Folgenden wird die Verwendung dieser systemunabhängigen Webservices-Methoden beschrieben:

createTicket (SID, Description, Error_Type, Userid, Asset, DuplicationID)

Sie müssen einen Fehlertyp für den berichteten Fehler angeben, wenn Sie diese Methode verwenden. Dieser Fehlertyp sollte die für das zu erstellende Ticket geeignete Ticket-Vorlage enthalten. Er sollte die Aktion definieren, die im Fall von Ticketduplikaten durchzuführen ist, und die Datenausgabe festlegen. Außerdem muss er der für die Benutzeranwendung definierten Zugriffsrichtlinie zugewiesen werden.

Wenn diese Methode aufgerufen wird, suchen die Webservices von CA SDM die aktuelle Zugriffsrichtlinie und den geeigneten Fehlertyp, die für die Ticketerstellung erforderlich sind. Im Folgenden wird die Sequenz aufgezeigt, in der die Webservices von CA SDM den geeigneten Fehlertyp suchen:

- Wenn ein spezifischer Fehlertypcode eingegeben wird und dieser einem Fehlertyp entspricht, der der Richtlinie zugewiesen ist, wird dieser Fehlertyp verwendet, ungeachtet dessen, ob er intern ist oder nicht.
- Wenn kein Fehlertyp festgelegt wird oder im vorherigen Schritt kein Fehlertyp gefunden werden konnte, wird der Standardfehlertyp verwendet, sofern einer für die Richtlinie definiert wurde.
- Wenn kein Standardfehlertyp für die Richtlinie definiert wurde oder der vorherige Schritt zu keinem Ergebnis führt, wird der für interne Fehlertypen definierte Standardfehlertyp verwendet.

Nachdem ein Fehlertyp definiert worden ist, wird er von den Webservices von CA SDM für die Erstellung eines Tickets verwendet. Der in der Zugriffsrichtlinie definierte Proxy-Benutzer wird für die Ticket-Erstellung herangezogen, wenn die Benutzer-ID leer ist, und es werden Anlageinformationen in das Ticket aufgenommen (sofern die Eingabe nicht leer ist). Nach Erstellung des Tickets geben die Webservices von CA SDM sowohl Benutzerdaten als auch Anwendungsdaten zurück, wie durch den Fehlertyp angegeben.

closeTicket (SID, Description, TicketHandle)

Benutzer können diese Funktion zum Schließen von offenen Tickets aufrufen. Dabei erhält ein offenes Ticket den Status „geschlossen“, und die Eingabebeschreibung wird in das Aktivitätsprotokoll aufgenommen.

logComment (SID, TicketHandle, Comment, Internal_Flag)

Fügt einen Eintrag mit dem Eingabekommentar zum Aktivitätsprotokoll für das offene Ticket hinzu.

getPolicyInfo (SID)

Ermöglicht es Benutzern, die Richtlinieninformationen zur Steuerung der aktuellen Webservices-Sitzung abzurufen. Sie können diese Informationen als einen Indikator der Serverkapazität für diese Benutzeranwendung verwenden. Benutzer können bei Bedarf ihre Webservices-Aufrufe entsprechend der Kapazität anpassen.

Durch diesen Satz vereinfachter Webservices-APIs entfällt für die meisten Benutzer der beachtliche Aufwand, der zum Verständnis des gesamten Satzes von Webservices-APIs und CA SDM-Schemata erforderlich ist. Deren Verwendung vereinfacht und beschleunigt den Vorgang der Erstellung von Anwendungen mit Service-Erkennung für die Benutzer.

Objekte

CA SDM behandelt jede Einheit, wie zum Beispiel einen Kontakt oder ein Issue, als ein *Objekt*. Diese systemunabhängigen Objekte werden in majic-Dateien (.maj) und mod-Dateien (.mod) auf dem CA SDM-Server im folgenden Verzeichnis definiert:

```
/bopcfg/majic
```

Angepasste Objekte werden im folgenden Verzeichnis definiert:

```
/site/mods/majic
```

Bei Objekten handelt es sich im Prinzip um systemunabhängige Schichten um eine Datenbanktabelle.

Der Typ eines Objekts (auch als *Factory* bezeichnet) definiert das Objekt. So gehören beispielsweise Anfrageobjekte zum Typ "cr". Jeder Objekttyp wird durch die „OBJECT“-Erklärung in einer majic-Datei definiert.

Hinweis: Alle im Lieferumfang von CA SDM enthaltenen Objekte werden im Technischen Referenzhandbuch zu CA SDM aufgeführt.

Ein Objekt hat *Attribute*, bei denen es sich im Wesentlichen um Spalten in einer Datenbanktabelle handelt (nicht zu verwechseln mit XML-Attributen). Die Webservices bieten viele Methoden für den Abruf von Werten für Attribute. Für viele Methoden ist die Angabe von Attributen für das Festlegen oder Abrufen von Werten erforderlich. Sie müssen dabei den Attributnamen verwenden, der dem Objekt in der majic- oder mod-Datei für das Objekt zugewiesen ist. Dieser kann vom tatsächlichen Datenbanknamen abweichen. Von Client-Sites aus können zusätzliche Attribute als Anpassung hinzugefügt werden.

Hinweis: Eine Liste aller Attribute für die einzelnen Objekte finden Sie im *Technischen Referenzhandbuch zu CA SDM*.

Die Webservices identifizieren ein Objekt eindeutig anhand seiner *Kennung*, wobei es sich um einen Zeichenfolgenwert in der Form *objektTyp:ID* handelt. "*objektTyp*" ist hierbei der (Factory)-Name des Objekttyps, während "ID" ein eindeutiger Wert ist. Der ID-Wert entspricht dem des Attributs "id", das Bestandteil eines jeden CA SDM-Objekts ist. Da dieses Attribut praktisch immer im DBMS indiziert ist, eignet sich die Verwendung des ID-Teils der Objektkennung besonders für die Formulierung effizienter Abfragen. Dieser Wert wird unabhängig vom Objekttyp in jedem Objekt in dem Attribut „persistent_id“ gespeichert.

Hinweis: In Vorgängerversionen handelte es sich bei dem ID-Teil der Kennung stets um eine Zeichenfolge aus Ganzzahlen. In Unicenter Service Desk r11.0 und höher kann der ID-Teil auch die Zeichenfolgendarstellung einer UUID aus üblicherweise 32 Zeichen sein.

In der folgenden Tabelle werden die Objekt- und Factory-Namen der Einheiten angegeben, die UUIDs verwenden:

Objektname	Factory-Name
Kontakt	cnt
Asset	nr
Organisation	org
Standort	loc
Unternehmen/Anbieter	ca_cmpny
Modell	mfrmod

Kennungen sind *eindeutig*, d. h., die Kennung eines bestimmten Objekts behält auch über Datenbankmigrationen hinweg stets ihren Wert. Auf Clients lässt sich dies bei der Arbeit mit relativ statischen Objekten, wie z. B. mit Status oder Kontakttypen, vorteilhaft verwenden.

Objektkennungen stellen den Schlüssel zur erfolgreichen Verwendung der Webservices von CA SDM dar. Für viele Methoden, insbesondere solche zur Datenaktualisierung, sind Kennungen unerlässlich. Die meisten Methoden, die Objektdaten zurückgeben, schließen auch die Kennung des Objekts ein.

Systemaktualisierungen und Zwischenspeicherung

In Webservices werden Informationen für Objekttypen im Cache gespeichert. Typinformationen werden nicht zwischengespeichert, bis zum ersten Mal auf den Typ verwiesen wird. Dies führt zu einer geringen Verzögerung.

Um Server- oder Zwischenspeicherungsverzögerungen zu vermeiden, können Sie einen vorläufigen Client zur Aktivierung der Webservices und Zwischenspeicherung häufig verwendeter Objekttypinformationen ausführen. Die einfachste Art der Zwischenspeicherung von Objekttypinformationen besteht in wiederholten Aufrufen von „GetObjectTypeInfo()“. Die für diese Vorgehensweise in Betracht zu ziehenden Objekttypen können Folgende sein:

Objekttyp	Definition
cr	Anforderung
chg	Änderungsauftrag
lss	Issue
cnt	Kontakt

Objekttyp	Definition
nr	Asset
wf	CA Workflow (Changes)
iss_wf	CA Workflow (Issues)
prp	Eigenschaft (für Änderungen und Issues)
prptpl	Eigenschaftsvorlage (für Änderungen und Issues)
cr_prp	Anfrageeigenschaft
cr_prptpl	Anfrageeigenschaftsvorlage

Fügen Sie jegliche zusätzlichen Objekttypen hinzu, auf die der Client-Code verweist.

Kategorien und Eigenschaften

Alle Anfrage-, Change- und Issue-Objekte verfügen über ein Kategorienfeld, das zur Klassifizierung von Tickets nach ihrem Wesen dient. Eine Kategorie kann Eigenschaftsobjekte aufweisen, die an das Ticket angehängt werden, wenn die Kategorie zugewiesen wird. Einige davon können als *erforderlich* gekennzeichnet sein, was bedeutet, dass ein Wert angegeben werden muss, bevor das Ticket gespeichert werden kann (dies gilt sowohl für Einfügings- als auch für Aktualisierungsvorgänge).

In den Webservices von CA SDM werden automatisch Standardwerte für alle mit den Webservices erstellten Tickets bereitgestellt. Der Standardwert (derzeit "-") stammt aus dem lokalisierten Meldungskatalog von CA SDM.

Wenn Sie Eigenschaftswerte zum Erstellungszeitpunkt festlegen müssen, stehen Ihnen drei Ticketerstellungsmethoden zur Verfügung: "createChangeOrder", "createIssue" und "createRequest". Jede hat einen Parameter, anhand dessen Sie Werte für jegliche Eigenschaften übernehmen können. Um zu erfahren, welche Eigenschaften angehängt werden, müssen Sie die mit der Kategorie verbundenen Eigenschaften ermitteln, die Sie dem Ticket zuweisen möchten. Am einfachsten lässt sich die Methode „getPropertyInfoForCategory()“ verwenden.

Hinweis: Weitere Informationen zur Methode "getPropertyInfoForCategory()" finden Sie im Technischen Referenzhandbuch zu CA SDM.

Um die gültigen Werte für eine Eigenschaft zu identifizieren, suchen Sie zuerst die Eigenschaftsvalidierungsregel für die entsprechende Eigenschaftsvorlage. Fordern Sie hierzu beim Aufrufen der Methode "getPropertyInfoForCategory" das Attribut "validation_rule" an. Rufen Sie dann den zugeordneten "validation_type" für diese Regel ab. Wenn der Typ "dropdown" ist, können Sie dann die Methode "getRelatedList" verwenden, um die dieser Regel zugeordneten Werte abzurufen. Verwenden Sie das BREL-Attribut "values" im Objekt "prpval_rule".

Hinweis: Weitere Informationen finden Sie im *Technischen Referenzhandbuch zu CA SDM*.

Um Eigenschaftswerte nach einem Aktualisierungsvorgang mit "updateObject()" festzulegen, müssen Sie nach erfolgter Aktualisierung die Eigenschaftsliste abfragen. "getRelatedList()" kann bei dieser Aufgabe helfen.

Die Validierung von Eigenschaftswerten durch Webservice-Methoden wird derzeit nicht unterstützt. Wenn Sie z. B. Eigenschaftswerte einer Validierungsregel mit einem Validierungstyp der Dropdown-Option zuweisen möchten, müssen Sie zusätzlichen Code schreiben, um die Eigenschaftswerte zu erstellen, während die Validierungsregel mit Dropdown-Option erstellt wird. Hängen Sie keinen Eigenschaftswert an eine Validierungsregel mit Kontrollkästchen-Option an.

Hinweis: Weitere Informationen zu Eigenschaftsvalidierungsregeln finden Sie im *Administrationshandbuch*. Informationen zum Erstellen von Eigenschaftsvalidierungsregeln über die CA SDM-Schnittstelle finden Sie in der *Online-Hilfe*.

XML-Objektrückgaben

Viele Webservices-Methoden geben eine XML-Darstellung von CA SDM-Objekten zurück. Die Webservices verwenden eine standardmäßige XML-Struktur, die mit dem folgenden Stammelement beginnt:

<UDSObject>

Das Format der XML-Darstellung wird in der folgenden Tabelle angegeben:

XML-Element	Typ	Beschreibung
<UDSObject>	N. rel.	Gibt den Stammknoten an.
<Handle>	Zeichenfolge	Gibt die Kennung des Objekts an.
<Attributes>	Sequenz	Gibt die Attributwerte an. Dies enthält keine oder mehrere Elemente für die Attributwerte des Objekts.

XML-Element	Typ	Beschreibung
<code><attrName0 DataType = "typeEnum"></code>	Zeichenfolge	Gibt "AttrName0" an, wobei es sich um einen Objektattributnamen handelt, wie in der majic-Datei (.maj) oder der mod-Datei (.mod) in CA SDM definiert. Für diesen Namen ist je nach verwendeter Web-Methode eine Punktnotation zulässig. Der Wert des Elements entspricht dem Wert des Attributs. Ein leeres Element weist auf einen Nullwert/leeren Wert für das Attribut dieses Objekts hin. Das "DataType"-Attribut ist eine Ganzzahl, die den Datentyp des Attributs in der CA SDM-Umgebung angibt.

Ein Abruf von „getObjectValues()“ kann z. B. Informationen zurückgeben, wie im Folgenden dargestellt:

```

<UDSObject>
  <Handle>cnt:555A043EDDB36D4F97524F2496B35E75</Handle>
  <Attributes>
    <Attribute DataType="2003">
      <AttrName>first_name</AttrName>
      <AttrValue>Vorname</AttrValue>
      <DisplayValue>Yaakov</DisplayValue>
    </Attribute>
    <Attribute DataType="2005">
      <AttrName>Organisation</AttrName>
      <AttrValue>342</AttrValue>
      <DisplayValue>Buchhaltungsabteilung</DisplayValue>
    </Attribute>
  </Attributes>
  <Lists>
    <List name="mylist1">
      <UDSObject>..</UDSObject>
      <UDSObject>..</UDSObject>
    </List>
  </Lists>
</UDSObject>

```

Einige Methoden, wie z. B. „doSelect()“, geben eine Sequenz von <UDSObject>-Elementen zurück, die sich innerhalb eines <UDSObjectList>-Elements befinden.

Der <Lists>-Abschnitt enthält keinen oder mehrere <List>-Knoten. Ein <List>-Knoten enthält keinen oder mehrere <UDSObject>-Knoten. <List>-Elemente werden im Allgemeinen nur dann zurückgegeben, wenn eine spezifische Anforderung für Listenwerte gestellt wird.

Wenn Sie eine Liste von Werten zurückgeben möchten, die mit einem bestimmten Objekt verbunden sind, verwenden Sie die Methode *"getRelatedListValues"*.

Erfolgt ein Request nur für eine Liste ohne Attributnamen, z. B. für "actlog", dann wird das ganze <UDSObject> im <List>-Abschnitt zurückgegeben.

Spezialisierte Methoden, wie etwa „getDocument()“, können sich hiervon unterscheiden. Erfolgt ein Request eines Attributs, wird der Datenbankwert zurückgegeben. Für SREL-Attribute ist dies nicht unbedingt sinnvoll. Bei Anforderung des "assignee"-Attributs eines Request wird eine Ganzzahl zurückgegeben, da der "REL_ATTR" des Kontakts (Fremdschlüssel) dessen ID ist. Bei Unicenter Service Desk r11.0 umfassen die Rückgabedaten für Attribute Elemente für das DBMS und den gemeinsamen Namenswert von SREL-Verweisen.

ITIL Methodology

Standardmäßig leisten die Webservices umfassende Unterstützung der ITIL-Methodologie. Anhand der ITIL-Funktionen von CA SDM-ITIL können Sie die ITIL-Methodologie nutzen.

Erstellen von Incidents oder Problemen

CA SDM- unterstützt die ITIL-Methodologie. Daher können bei Verwendung der Webservices von CA SDM Incidents und Probleme erstellt werden. Sowohl Incidents als auch Probleme befinden sich im "cr"-Objekt (Call_Req). Anhand des "type"-Attributs wird unterschieden, ob der Datensatz ein Incident, ein Problem oder eine Anfrage ist. Rufen Sie zur Erstellung eines Incidents, eines Problems oder einer Anfrage "createRequest" auf, und legen Sie den geeigneten Wert für das "type"-Attribut fest.

Das Typattribut ist ein Verweis (SREL) auf das „cr“-Objekt (Call_Req_Type), daher ist eine Kennung als Wert anzugeben.

Die folgenden Codebeispiele veranschaulichen, wie ein Incident oder Problem erstellt werden kann, indem die richtige "crt"-Objektkennung an die "createRequest"-Methode übergeben wird. Durch Festlegen des "type"-Attributs im Namen-Wert-Paar, das als ein Parameter an "createRequest" übergeben wird, wird das Ticket erstellt.

Beispiel: Syntax für ein Problem

```
attrVals = {"summary", "A new problem", "description", "new problem", "type",  
            "crt:181"}  
USPSD.createRequest(SID, creatorHandle, attrVals, template, new String[0], new  
String[0])
```

Beispiel: Syntax für einen Incident

```
attrVals = {"summary", "A new incident", "description", "new incident", "type",  
            "crt:182"}  
USPSD.createRequest(SID, creatorHandle, attrVals, template, new String[0], new  
String[0])
```

Weitere Informationen:

[Standardkennungen](#) (siehe Seite 622)

Abfragen zu Incidents oder Problemen

Um Incidents oder Probleme abzurufen, schließen Sie das Attribut "type" des "cr"-Objekts in die Where-Klausel ein. Das folgende Beispiel beschreibt eine Where-Klausel für den Abruf aller aktiven Incidents. Diese Where-Klausel lässt sich mit Methoden zur Abfrage nach „cr“-Objekten verwenden, wie z. B. „doSelect“ und „doQuery“:

```
type.id = 182 AND active = 1
```

Das "182" ist der ID-Teil der Kennung, die Incident-Typen darstellt.

Hinweis: Weitere Informationen finden Sie in der "crt"-Objekttabelle ("Call_Req_Type"), die in "[Standardkennungen](#)" (siehe Seite 622) beschrieben wird. Weitere Informationen über die Formulierung geeigneter Abfragen finden Sie unter "[WHERE-Klausel](#)" (siehe Seite 375)".

Anhängen eines Incident an ein Problem

Sie können einen oder mehrere Incidents einem Problem zuordnen. Das Problemattribut eines Incident ordnet den Incident einem Problem zu.

Beispiel: Zuordnen eines Incident zu einem Problem

Dieses Beispiel zeigt, wie ein neu erstellter Incident zu einem vorhandenen Problem zugeordnet wird.

Um den Incident dem Problem zuzuordnen, verwenden Sie "UpdateObject", um das Problemattribut des Incidents festzulegen. Der folgende Beispielcode legt das Problemattribut auf die Kennung eines vorhandenen Problem-Tickets:

```
attributeValues = {"problem", "cr:12346"}  
USPSD.UpdateObject(SID, incidentHandle, attributeValues, new String [0])
```

Anhängen eines Problems an einen Change

Incidents und Probleme können anhand der Methode "attachChangeToRequest" mit Changes verknüpft werden. Anhand des folgenden Beispielcodes wird die Verwendung dieser Methode zum gleichzeitigen Erstellen eines Change und dessen Anhängen an ein Problem dargestellt. In dem Beispiel ist "cr:12347" die Objektkennung des Problems. Es wird eine leere Kennung für den vierten Parameter übergeben, woraufhin die Methode einen Change erstellt:

```
USPSD.attachChangeToRequest(SID, creatorHandle, "cr:12347", "", new String[0],  
"activity description")
```

Konfigurationselemente

In der ITIL-Methodologie wird der Begriff "*Configuration Item*" (Konfigurationselement, CI) für die Bezeichnung von Software-, Hardware- und anderen IT-Ressourcen verwendet. Dieser Begriff bezieht sich auf das "nr"-Objekt, das in der CA Technologies-eigenen Ressourcendatenbanktablette gespeichert ist. Alle Methoden, die Asset-Objekte verwenden, arbeiten ebenfalls mit CIs. Es handelt sich lediglich um einen terminologischen Unterschied.

Verwenden der Webservices

Die Informationen in diesem Abschnitt beschreiben die Grundlagen zur Verwendung der Webservices von CA SDM. Beispielcode, in dem die Webservices verwendet werden, befindet sich im folgenden CA SDM-Installationsverzeichnis:

```
<NX_ROOT>/samples/sdk/websvc/java
```

Der Beispielcode wurde mit Apache Axis-for-SOAP-Messaging in Java geschrieben.

Anmeldungen

Bevor eine Webservices-Methode verwendet werden kann, muss eine SID (Sitzungs-ID) aus einer der folgenden Methoden abgerufen werden: "login()", "loginService()" und "loginServiceManaged()". Für die ersten beiden Methoden sind ein Benutzername und ein Kennwort erforderlich, die auf die gleiche Weise wie die CA SDM-Web-Schnittstelle validiert werden. Durch den Zugriffstyp des Kontakts wird die Validierungsmethode festgelegt. Für die dritte Methode ist ein Schlüsselpaar aus öffentlichem und privatem Schlüssel erforderlich, wobei anhand des privaten Schlüssels verschlüsselte Anmeldeanfragen nur mit dem öffentlichen Schlüssel entschlüsselt werden können und umgekehrt.

Weitere Informationen:

[Externe Spezifikationen](#) (siehe Seite 594)

Durchführen allgemeiner Aufgaben

Die Webservices stellen eine flexible und leistungsstarke API in CA SDM bereit. Für ihre Verwendung sind aber gewisse Kenntnisse der vom Produkt verwendeten Objektstruktur erforderlich:

1. Machen Sie sich mit den Informationen über Objekte und Attribute im *technischen Referenzhandbuch* vertraut.

In diesem Handbuch werden die Attribute der einzelnen Objekte im System aufgelistet, was sehr wichtig ist, da für viele der Webservices-Methoden Attributnamen erforderlich sind.

2. Gehen Sie die Webservices-Methoden durch, insbesondere die generischen. Wenn Ihre Anwendung beispielsweise alle Aktivitätsprotokolle für einen Request anzeigen muss, ermitteln Sie zunächst, auf welche Art die Aktivitätsprotokolle mit dem Request verbunden sind.

Im *technischen Referenzhandbuch* ist ersichtlich, dass für das Request-Objekt zwei Listen von Aktivitätsprotokollen vorhanden sind: "act_log" (nur nicht interne Protokolle) und "act_log_all" (alle Aktivitätsprotokolle).

3. Ermitteln Sie, welche Webservices-Methoden für Sie erforderlich sind. Um Listen abzurufen, die an ein Objekt angehängt sind, verwenden Sie „getRelatedList()“ oder „getRelatedListValues()“.

Standardkennungen

Einige im Produkt bereitgestellte Standarddaten werden häufig verwendet. Anstatt Kennungen für diese Objekte zu suchen, können Sie einige der häufiger verwendeten Kennungen in den folgenden Tabellen in Erfahrung bringen.

Hinweis: Während Kennungen unveränderlich sind, können die lesbaren Symbole bearbeitet werden.

Kontakttyp (Objektname: "ctp")

Kennung	Hinweis
ctp:2307	Der „Analyst“-Typ
ctp:2310	Der „Kunde“-Typ
ctp:2305	Der „Mitarbeiter“-Typ
ctp:2308	Der „Gruppe“-Typ

Auswirkung (Objektname:"imp")

Kennung	Hinweis
imp:1605	Auswirkung „Keine“
imp:1600	Niedrige Auswirkung „5“
imp:1601	Mittlere bis niedrige Auswirkung „4“
imp:1602	Mittlere Auswirkung „3“
imp 1603	Mittlere bis hohe Auswirkung „2“
imp:1604	Hohe Auswirkung „1“

Priorität (Objektname: "pri")

Kennung	Hinweis
pri:505	Nicht zugewiesene Priorität „Keine“
pri:500	Niedrige Priorität „5“
pri:501	Mittlere bis niedrige Priorität „4“
pri:502	Mittlere Priorität „3“
pri:503	Mittlere bis hohe Priorität „2“
pri:504	Hohe Priorität „1“

Schweregrad (Objektname: "sev")

Kennung	Hinweis
sev:800	Niedriger Schweregrad „1“
sev:801	Mittlerer bis niedriger Schweregrad „2“
sev:802	Mittlerer Schweregrad „3“
sev:803	Mittlerer bis hoher Schweregrad „4“
sev:804	Hoher Schweregrad „5“

Aufrufanforderungstyp (Objektname: "crt")

Kennung	Hinweis
crt:180	Anforderung
crt:181	Problem
crt:182	Incident (Störung)

Abfrage für einem Kontakt zugeordneten Anfragen, Issues oder Changes

Einer der häufigsten Vorgänge ist der Abruf der aktiven Anfragen, die einem Analysten (Zuständigen) zugewiesen sind. Sie können eine von mehreren Methoden verwenden, wie z. B. "doQuery()" (zum Abruf einer Listenreferenz) oder "doSelect()" (zum umgehenden Abruf der Werte). Unter der Annahme, dass die Kennung des Zuständigen bereits bekannt ist, ist folgende Where-Klausel zu verwenden:

```
assignee.id = U'<assigneeID>' AND active = 1
```

In dieser WHERE-Klausel ist "<assigneeID>" der ID-Teil einer Kontaktkennung, ein Wert wie z. B. "555A043EDDB36D4F97524F2496B35E75".

Diese Where-Klausel funktioniert für Anfragen, Changes und Issues, da sie alle die Attribute "assignee" und "active" aufweisen, die für alle drei Objekttypen die gleiche Bedeutung haben. Mit "active = 1" in der Where-Klausel werden Suchvorgänge auf aktive Anfragen beschränkt.

Die Markierung für aktive Elemente

Die meisten CA SDM-Objekte weisen das Feld "active" oder "delete_flag" auf. Hierbei handelt es sich um einen SREL-Verweis auf das Objekt „Active_Boolean_Table“ oder „Boolean_Table“. Ziehen Sie das Hinzufügen dieser Felder zu Ihren Abfragen in Betracht, um vom Systemadministrator als inaktiv markierte Objekte auszufiltern. Suchen Sie für Abfragezwecke nach „delete_flag = 0“, um aktive Datensätze zu finden, und „delete_flag = 1“, um inaktive Datensätze zu finden. Am Beispiel des folgenden Pseudocodes wird die Verwendung von "doSelect()" zum Abrufen von Werten für alle aktiven Anfragestatusobjekte veranschaulicht:

```
doSelect(SID, "crs", "delete_flag = 0", -1, new String[0]);
```

Um ein Objekt als aktiv oder inaktiv festzulegen, müssen Sie die Kennung des booleschen Objekts übergeben, die den Wert „True“ oder „False“ wiedergibt. Diese Kennungen sind unveränderlich und können damit bedenkenlos hartcodiert werden. Es handelt sich dabei um folgende Kennungen:

Active_Boolean_Table	Boolean_Table
actbool:4551 = 'Active'	bool:200 = 'False'
actbool:4552 = 'Inactive'	bool:201 = 'True'

Abrufen der Länge verbundener Listen

Beim Anfragen von Attributwerten aus einem Objekt, z. B. mit "getObjectValues()", können Sie die Länge der verbundenen Liste durch Anfragen des folgenden Attributs abrufen:

```
"<listName>.length"
```

Um beispielsweise die Anzahl der Aktivitätsprotokolle für eine bestimmte Anfrage zu erhalten, übergeben Sie Folgendes an "getObjectValues()":

```
"act_log_all.length"
```

Hinweis: Dies ist die einzige Möglichkeit der Verwendung von Listennamen bei diesen Methodentypen.

Representational State Transfer (REST) ist ein Softwarearchitekturstil für verteilte Hypermedia-Systeme wie das World Wide Web. Die CA SDM-REST-API ermöglicht es Anwendungen, Integrationen und Webentwicklern Benutzeroberflächen und Anwendungen für Geräte wie Tablet-Computer und Smartphones erstellen. Anwender wie Analysten, Mitarbeiter und Kunden können dann die Benutzeroberfläche oder die Anwendung auf diesen Geräten verwenden. Zum Beispiel können Anwendungsentwickler eine CA SDM-Benutzeroberfläche entwickeln, mit der Analysten Geräte verwenden können, um Tickets zu aktualisieren.

Die REST-API greift auf Ressourcen zu, indem ein Uniform Resource Identifier (URI) verwendet wird: Eine Zeichenkette, die einen Namen oder eine Ressource im Internet identifiziert. In CA SDM können Ressourcen Objekte sein, wie z. B. Tickets, Assets, Kontakte usw. Eine Anwendung, die die REST-API verwendet, wandelt eine HTTP-Request in einen URI um und analysiert die Antwort. Eine solche Identifizierung aktiviert eine Interaktion mit Darstellungen der Ressource über einem Netzwerk. Jede Request von Client zum Server enthält die gesamten Informationen, die notwendig sind, um die Request zu verstehen, und es wird kein gespeicherter Kontext auf dem Server verwendet.

Entwickler verwenden die REST-API direkt, um dem Server HTTP-Requests für die Ressource zu senden, die sie bearbeiten möchten. Entwickler benötigen nur eine HTTP-Client-Bibliothek, die mit den meisten Programmiersprachen verfügbar ist. Da die REST-API auf offene Standards basiert, können Sie eine beliebige Java-Programmiersprache verwenden, um darauf zuzugreifen.

Hinweis: Weitere Informationen zu REST-HTTP-Methoden finden Sie im *technischen Referenzhandbuch*.

REST und SOAP

CA SDM stellt REST- und SOAP-Webservices-APIs bereit. Die Zielgruppe für die REST-API ist ein Benutzeroberflächen-Client, während die Zielgruppe für die SOAP-API ein Programm ist. Bei REST-Services geht es um Ressourcen (Bearbeiten von Objekten, Ändern von Objektzuständen, Austauschen von Darstellungen und Verwenden von Hauptwörtern statt Verben). Bei SOAP-Services geht es um Services (Aufrufen von Methoden, Verwenden von Verben und Durchführen von Aktionen).

REST hat gegenüber SOAP folgende Vorteile:

- REST ist kompakt, HTTP-basiert und statusfrei (für Skalierbarkeit).
- REST unterstützt das Erstellen von Lesezeichen für Clients und Zwischenspeicherung.
- REST hält die Datenverkleinerung unverpackt.
- REST kann einfach von Front-End-Technologien wie "Web 2.0" und "AJAX" verwendet werden.
- REST unterstützt die Datenformate "XML" und "JSON".
- REST verbessert die Leistung.

REST Sicherheit

Die Sicherheit verwendet mehrere Authentifizierungsmechanismen einschließlich einer anwenderspezifischen Vorgehensweise, die freigegebene Geheimschlüssel verwendet.

Das Produkt unterstützt folgende Schemen für die Sicherheitsauthentifizierung:

- Geheimschlüsselauthentifizierung der REST-Webservices (verwendet SSL und HMAC für die Anmeldung)
- REST-Basisauthentifizierung (klartext-verschlüsselter Anwendername und Kennwort)
- REST BOPSID-Authentifizierung (validiert CA SDM-BOPSIDs)
- Externe (CA EEM) Artefakt-Authentifizierung (CA EEM-Artefakt-Token)

So funktioniert die Geheimschlüsselauthentifizierung

Die CA SDM-Geheimschlüsselauthentifizierung ist ein Prozess, der Folgendes überprüft:

- Die Identität des Request-Absenders.
- Es wird überprüft, ob der Sender ein registrierter Anwender ist.

Für die Geheimschlüsselauthentifizierung ist es erforderlich, dass jede Request Informationen zur Identität des Request-Absenders enthält. Die Request muss auch zusätzliche Informationen enthalten, die CA SDM verwenden kann, um die Authentizität des Anwenders zu überprüfen. Wenn die Request diesen Verifizierungstest besteht, wird die Request als authentisch bewertet. Während der Authentifizierung für eine Zugriffsschlüssel-Request geht CA SDM-Geheimauthentifizierung folgendermaßen vor:

1. Ein Zugriffsschlüssel wird einem Client zugewiesen. Der Zugriffsschlüssel identifiziert den für eine Request verantwortlichen Client und verwendet die Sitzungs-ID von CA SDM als Schlüsselwert. Da ein Zugriffsschlüssel als Request-Parameter gesendet wird, ist er nicht geheim. Jeder, der eine Request an CA SDM sendet, kann den Request-Parameter verwenden. Deswegen ist ein Geheimschlüssel erforderlich.

2. Ein Geheimschlüssel wird zugewiesen. Ein Geheimschlüssel ist eine alphanumerische Sequenz aus 40 Zeichen, die von CA SDM während der Anmeldung dynamisch generiert wird. Das Produkt verschlüsselt diesen Geheimschlüssel, bevor dieser in der Datenbank gespeichert wird.
3. Es werden vom Client angegebene Informationen verwendet (eine Request-Signatur, die den Geheimschlüssel verwendet), um den Client zu identifizieren und um zu überprüfen, ob die Request legitim ist. Diese Zusatzinformationen schützen Anwender vor Identitätswechsel und zeigen den Besitz eines freigegebenen Geheimschlüssels, der nur CA SDM und dem Request-Absender bekannt ist.

Webserviceoptionen

Diese Optionen steuern die Webservice-Sitzung:

rest_webservice_access_duration

Gibt die Anzahl der Stunden an, die der REST-Webservice-Zugriffsschlüssel vor Ablauf aktiv bleibt. Das Zeitlimit des Zugriffsschlüssels basiert nicht auf Inaktivitätszeit, sondern auf den Zeitraum seit der Erstellung des Zugriffsschlüssels. Nachdem der Zugriffsschlüssel die angegebene Dauer erreicht hat, endet der Zugriffsschlüssel, unabhängig davon, ob er verwendet wird.

Optional kann der REST-Client auch den Zeitraum für den Zugriffsschlüssel für den bestimmten Zugriffsschlüssel während der Zugriffsschlüssel-Request angeben. Um den Zeitraum anzugeben, legen Sie ihn direkt im Attribut "expiration_date" der Ressource "rest_access" als Inhaltsteil der POST-Request fest.

Gültiger Bereich: 1-8760 Stunden

Standard: 168

rest_webservice_disable_basic_auth

Deaktiviert Basisauthentifizierung in REST-Webservices.

Standardwert: Nein

rest_webservice_list_max_length

Gibt die maximale Anzahl der Zeilen an, die eine REST-Webservice-Abfrage zurückgibt.

Standard: 500

rest_webservice_list_page_length

Gibt die standardmäßige Anzahl der Zeilen an, die eine REST-Webservice-Abfrage pro Seite zurückgibt.

Gültiger Bereich: 1-500

Standard: 25

rest_webservice_resources_to_expose

Gibt die Liste von Majic-Factorys (Ressourcen) an, die CA SDM über REST-Webservices zur Verfügung stellt. Diese Option überschreibt das Standardverhalten. Standardmäßig stellt CA SDM alle Factorys über REST-Webservices zur Verfügung.

Wenn Sie keine Werte in diese Option eingeben, stellt das Standardverhalten eine beliebige Majic-Factory zur Verfügung, bei der die Eigenschaft "REST_OPERATIONS" nicht auf "NONE" festgelegt ist. Standardmäßig ist bei keiner Majic-Factory diese Eigenschaft auf "NONE" festgelegt.

Verwenden Sie die Eigenschaft "REST_OPERATIONS", um die bestimmten HTTP-CRUD-Methoden (CREATE, READ, UPDATE, DELETE) festzulegen, die CA SDM auf einer bestimmten Majic-Factory zur Verfügung stellt.

Standard: rest_access

Beispiel: rest_access, cnt, grp, cr, crs, pri, alg, urg, imp, pcat, org

hmac_algorithm

Gibt den Algorithmus an, den Sie verwenden, um die Signatur für "Custom/Secret Key Authentication" in REST-Webservices zu berechnen.

Standard: HmacSHA1

string_to_sign_fields

Gibt die Felder an, die Sie verwenden, um die Signatur für "Custom/Secret Key Authentication" in REST-Webservices zu berechnen, zusätzlich zu den Standardfeldern "REQUEST_METHOD", "REQUEST_URI" und "QUERY_STRING".

Standard: Leer

webservice_domsrvr

Gibt den Namen der Objekt-Engine an, die von den SOAP-Webservices verwendet wird. Falls diese Option nicht installiert ist, wird von den SOAP-Webservices "domsrvr" verwendet.

Der Wert der Option muss aus einer Zeichenfolge bestehen, die mit den Zeichen "domsrvr:" beginnt.

webservice_session_timeout

Legt den Wert für die Zeitüberschreitung (in Minuten) für SOAP-Webservice-Sitzungen fest. Wenn die Zeit zwischen aufeinanderfolgenden Web-Methoden-Aufrufe größer ist als der angegebene Wert, dann wird die Sitzungs-ID als abgelaufen markiert. Die Sitzung ist dann nicht mehr gültig.

Um Sitzungen vor dem Ablauf aufgrund von Aktivität zu bewahren, setzen Sie den Wert dieser Option auf 0 (Null). Andere Methoden, wie z. B. Abmelderroutinen, können Sitzungen weiterhin ungültig machen.

Hinweis: Diese Optionen erfordern einen Neustart des CA SDM-Servers.

Kapitel 13: Integration mit anderen Produkten

Sie können CA SDM mit einigen CA Technologies-Produkten integrieren; es wird hier jedoch nicht im Detail auf die Integration mit allen CA Technologies-Produkten eingegangen.

Hinweis: Ausführliche Informationen zur Integration von weiteren Produkten in CA SDM, die in diesem Abschnitt nicht enthalten sind, finden Sie im *CA Unicenter Service Desk Green Book zur Integration* unter "<http://ca.com/support>".

Dieses Kapitel enthält folgende Themen:

[CA Workflow-Integration](#) (siehe Seite 631)

[CA Portal-Integration](#) (siehe Seite 637)

[Integration von Mainframe-Produkten](#) (siehe Seite 643)

[Integration von CA Business Service Insight](#) (siehe Seite 646)

CA Workflow-Integration

Ein Workflow umfasst die Aufgaben, Verfahrensschritte, beteiligten Organisationen oder Einzelpersonen, erforderlichen Eingangs- und Ausgangsinformationen sowie die notwendigen Tools für die Verwaltung und Pflege jedes Schritts in einem Geschäftsprozess. Der Workflow-Service bietet eine umfassende Lösung zur Verwaltung der Geschäftsprozesse.

In allgemeinen Worten lässt sich der *Workflow* am besten als vollständige oder teilweise Automation eines Geschäftsprozesses beschreiben, bei dem Dokumente, Informationen oder Aufgaben von einem Teilnehmer an einen anderen übergeben werden, der anhand von Verfahrensregeln bestimmte Aktionen durchführt.

CA Workflow ist ein generisches, sehr leistungsfähiges und skalierbares Workflow Management-System, das Definition, Verwaltung und Ausführung von Workflows ermöglicht und somit eine umfassende Workflow-Lösung bietet.

CA Workflow ist über Webservices in CA SDM integriert.

CA Workflow-Komponenten

CA Workflow verwendet die folgenden Komponenten, die mit dem Workflow Embedding Kit geliefert werden:

- [Umgebung für Workflow-Entwurf](#) (siehe Seite 632)
- [Workflow-Server](#): (siehe Seite 634)
- [Worklist](#) (siehe Seite 634)

Die CA Workflow-Entwicklungsumgebung

Die CA Workflow-Entwicklungsumgebung dient zum Erstellen und Verwalten von Workflows. Die CA Workflow-Entwicklungsumgebung ist das wichtigste Tool zum Erstellen und Verwalten von Prozessdefinitionen und Workflow-Instanzen sowie zum Steuern der Interaktion von Workflow-Teilnehmern.

Ein Unternehmen erzeugt einen Geschäftsprozess, um die Ressourcen, die manuellen und automatisierten Aktivitäten sowie die Beziehungen zwischen den Aktivitäten zur Realisierung der Geschäftsziele zu bezeichnen. Durch die Festlegung von Aktivitäten eines Geschäftsprozesses in einer Prozessdefinition wird der Geschäftsprozess mit Hilfe des Workflows teilweise oder vollständig automatisiert. Diese Workflow-Aktivitäten umfassen gewöhnlich die Weitergabe von Formularen, Aufgaben oder Informationen von einer Ressource zu einer anderen, wobei es sich bei den Ressourcen um Menschen oder um Software handeln kann.

Eine Prozessdefinition ist eine Darstellung Ihres Geschäftsprozesses. Eine Prozessdefinition umfasst Knoten, Ereignisse, Rollen, Akteure, Tätigkeit sowie Kriterien für Start und Ende des Prozesses.

Während Prozessdefinitionen darstellen, was in Ihrem Geschäftsprozess geschehen soll, stellen Prozessinstanzen dar, was tatsächlich geschieht. Indem Sie eine Prozessdefinition ausführen, erstellen Sie eine Prozessinstanz. Sie können mehrere Prozessinstanzen derselben Prozessdefinition erstellen, die auch als Prozessdefinitions-Instanz bezeichnet wird.

Starten der CA Workflow-Entwicklungsumgebung (Windows)

Die CA Workflow-Entwicklungsumgebung können Sie jederzeit starten, um Workflows zu erstellen und zu verwalten. Um die CA Workflow-Entwicklungsumgebung zu starten, wählen Sie "Start", "Alle Programme", "CA", "Service Desk Manager", "CA Workflow IDE".

Hinweis: Sie können die CA Workflow-Entwicklungsumgebung auch starten, indem Sie auf die Datei "*ide.bat*" doppelklicken, die sich im Verzeichnis "`$NX_ROOT\site\Workflow\Client`" befindet. Wenn jedoch der IDE-Klassenpfad an bestimmte Anwendungsvoraussetzungen angepasst werden muss, müssen Sie den Parameter "APPCPATH" in "*ide.bat*" ändern und "*ide.bat*" zum Aufruf der IDE verwenden.

Starten der CA Workflow-Entwicklungsumgebung (Linux)

Die CA Workflow-Entwicklungsumgebung können Sie jederzeit starten, um Workflows zu erstellen und zu verwalten. Um die CA Workflow-Entwicklungsumgebung zu starten, führen Sie die Datei "*ide.sh*" aus, die sich im Verzeichnis "`$NX_ROOT/site/Workflow/Client`" befindet. Die CA Workflow IDE wird unter UNIX nicht unterstützt.

Hinweis: Um den Anwendungsvoraussetzungen zu entsprechen, enthält die Datei "*ide.sh*" den Parameter "APPCPATH", der zum Hinzufügen zum Klassenpfad geändert werden kann.

CA Workflow IDE-Parameter

Beim Zugriff auf die CA Workflow-Entwicklungsumgebung wird ein Anmeldefenster angezeigt. In diesem Anmeldefenster sind Benutzername, Kennwort und URL-Verbindung bereits angegeben. Für einen schnellen Zugriff auf die IDE können Sie das Anmeldefenster umgehen, indem Sie eine Kombination aus folgenden Befehlszeilenparametern verwenden:

```
-u <Benutzername>  
-p <Kennwort>  
-url <PM-URL>  
-t <Token für sichere eIAM-Sitzung>
```

Wahlweise können Sie die IDE aufrufen, indem Sie Benutzername und Kennwort (-u und -p) oder ein Token (-t) angeben. Das Token „-t“, eine Zeichenkette, bezieht sich auf eine exportierte sichere Sitzung (SafeSession), die auch als Artefakt bezeichnet wird. Dadurch können übergeordnete Produkte vorhandene SafeSessions auf einfache Weise wiederverwenden, ohne dass Benutzername und Kennwort erneut eingegeben werden müssen.

Der Parameter „-url“ ist erforderlich und muss übergeben werden unabhängig davon, ob die Benutzer/Kennwort-Methode (-u und -p) oder die Token-Methode (-t) verwendet werden.

Zum Beispiel [-u, -p, -url] oder [-t, -url]

Um diese Funktion zur Umgehung des IDE-Anmeldebildschirms zu nutzen, bearbeiten Sie entweder die Datei "ide.bat" (in Microsoft Windows) oder die Datei "ide.sh" (in Linux), um diese Parameter zur Liste der Parameter hinzuzufügen, die an den Java-Befehl übergeben werden.

Hinweis: Diese Funktion kann mit der Datei "ide.exe" nicht verwendet werden.

CA Workflow-Server

Der CA Workflow-Server macht die Ausführung zur Laufzeit und die Verwaltungsfunktionen für die Workflow-Prozesse transparent. Der CA WorkflowServer besteht aus den folgenden Komponenten:

- Akteuradapter ermöglichen die Erweiterung der Workflowaktivitäts-Funktionalität.
- Die Prozess-Engine führt die Prozessdefinitions-Instanzen aus.
- Der Prozessmanager verwaltet die Prozessdefinitionen und Prozessinstanzen.

Alle Workflow-Clients, der Prozess-Designer, die Worklist sowie die Java- und die Webservices-API nutzen die vom CA Workflow-Server bereitgestellten Dienste.

Worklist

Sie können die Worklist über einen Webbrowser aufrufen (zum Beispiel: `http://<hostname>:<portnummer>/wl`) oder über API-Aufrufe aus einem integrierten Produkt.

CA Workflow-Zugriff

CA SDM stellt für das Workflow-Management eine allgemeine Workflow Engine bereit. Das Workflow-System bietet eine grafische Workflow-Definitions Umgebung, intelligente Verzweigungsmechanismen sowie die Möglichkeit zur Interaktion mit Einzelpersonen, die für Genehmigungen nicht direkt auf die CA SDM-Anwendung zugreifen können. Sie können die CA Workflow-Authentifizierung verwenden und den CA Workflow-Gruppen [Anwender hinzufügen](#) (siehe Seite 636).

CA EEM und CA Workflow

Alle Anmeldungen bei CA Workflow werden von CA EEM authentifiziert. Für einen Benutzer muss ein CA EEM-Benutzerdatensatz vorhanden sein, damit er auf die CA Workflow-IDE oder die Worklist-Anwendung zugreifen kann. Der CA Workflow-Administrator, der während der CA SDM-Konfiguration festgelegt wurde, hat vollen Zugriff auf CA Workflow. Standardmäßig wird dieser Administrator von CA SDM für die CA Workflow-Integration verwendet. Dieses Benutzerkonto wird durch die Optionen „cawf_username“ und „cawf_password“ im Optionsmanager festgelegt. Sie müssen sicherstellen, 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.

Ressourcenklassen

CA Workflow verwendet CA EEM auch, um den Zugriff auf bestimmte CA Workflow-Funktionen einzuschränken. Der Zugriff wird von zwei Ressourcenklassen gesteuert:

IDE

Die IDE-Ressource umfasst eine einzelne Aktion mit dem Namen *login* für den Anmeldezugriff auf die IDE. Ein Benutzer muss die Berechtigung für diese Aktion besitzen, um sich bei der CA Workflow IDE-Anwendung anmelden zu können.

Verfahren

Die Prozess-Ressource umfasst eine einzelne Aktion mit dem Namen *start*, um eine Prozessinstanz zu starten. Ein Benutzer muss die Berechtigung für diese Aktion besitzen, um Prozesse innerhalb der Worklist-Web-Anwendung starten zu können. Alle Benutzer haben Zugriff auf die CA Workflow Worklist-Anwendung, um Aufgaben zu Arbeitselementen anzuzeigen und durchzuführen. Diese Berechtigung dient nur zum Starten neuer Instanzen aus der Worklist heraus.

Hinweis: Diese Ressourcenklassen werden mit der CA SDM-Anwendungsinstanz in CA EEM definiert. Wenn Sie sich bei der CA EEM-Web-Benutzerschnittstelle anmelden, müssen Sie die CA SDM-Anwendungsinstanz angeben, damit die hier vorgestellten Ressourcen, Richtlinien und Gruppen angezeigt werden.

Hinzufügen von Anwendern zu CA Workflow-Gruppen

Anwender, die sich bei IDE anmelden oder Prozessinstanzen starten müssen, benötigen eine entsprechende Berechtigung für die Ressourcen und die beiden Aktionen. Die CA SDM-Konfiguration fügt CA EEM zwei Richtlinien hinzu, die Zugriff auf diese Ressourcen gewähren. Es werden auch zwei Anwendergruppen mit Zugriffsrechten auf die Richtlinien hinzugefügt: CA Workflow-Administratoren und Initiatoren für CA Workflow-Prozesse. Anwender, die der Gruppe CA Workflow-Administratoren hinzugefügt werden, erhalten Zugriff auf die IDE. Anwender, die der Gruppe der Initiatoren für CA Workflow-Prozesse hinzugefügt werden, sind berechtigt, Prozesse aus der Worklist-Anwendung zu starten.

So fügen Sie Anwender den Gruppen auf dem Computer mit der CA EEM-Installation hinzu oder entfernen diese:

1. Führen Sie einen der folgenden Schritte aus:
 - Bei CA EEM r8.4 SP4 CR05 wählen Sie "Start", "Programme", "CA", "Embedded Entitlements Manager", "EEM-Benutzeroberfläche".
 - Bei CA EEM r12 CR02 wählen Sie "Start", "Programme", "CA", "Embedded Entitlements Manager", "Admin UI".

Das Anmeldefenster wird angezeigt.
2. Wählen Sie die CA SDM-Anwendung, und geben Sie den Anwendernamen und das Kennwort des CA EEM-Administrators ein.

Das CA EEM-Hauptfenster wird angezeigt.
3. Markieren Sie „Identitäten verwalten“
4. Wählen Sie die Anwendersuche, geben Sie Suchkriterien ein, und klicken Sie auf "Suchen".
5. Wählen Sie einen Anwender aus der Ergebnisliste aus.
6. In der Detailanzeige des Anwenders fügen Sie im Abschnitt „Mitgliedschaft in der Anwendungsgruppe“ Gruppenmitglieder hinzu, oder Sie löschen Mitglieder aus der Gruppe.

Wenn dieser Abschnitt nicht angezeigt wird, klicken Sie auf "Anwenderdetails hinzufügen".
7. Klicken Sie auf "Speichern".

Die Anwender werden den Gruppen hinzugefügt.

CA Portal-Integration

Sie können auf CA SDM-Komponenten über CA Management Portal und CA Portal zugreifen.

Hinweis: CA Management Portal und CA Portal werden nicht mit CA SDM geliefert und müssen daher separat erworben und lizenziert werden. CA SDM stellt nur die wichtigsten Informationen zum Zugriff auf CA SDM über die Portal-Administration bereit. Ausführliche Informationen finden Sie in der Online-Hilfe zur Server-Administration für *CA Portal* und *CA Management Portal*.

Überprüfen des Zugriffs auf die Web-Schnittstelle von CA SDM

Nach der Installation von CA SDM auf einem System müssen Sie darauf achten, dass Sie über den Tomcat-Server auf die Web-Schnittstelle zugreifen können. Damit die Portal-Integration funktioniert, muss die Web-Schnittstelle von CA SDM über Tomcat zugänglich sein.

Hinweis: Bei einer Installation von CA SDM auf einem LINUX-Server muss die Variable "LD_LIBRARY_PATH" auf "\$NX_ROOT/sdk/lib" festgelegt werden.

Installieren und Starten von CA Portal

Für ausführliche Informationen zum Installieren, Starten und Beenden von CA Portal finden Sie im *Handbuch "Erste Schritte"* für Ihre spezifische Installation.

Hinweis: Sie können CA Portal auf dem System, auf dem CA SDM installiert ist, oder auf einem separaten System installieren.

Integration von Portlets

Sie können das Produkt verwenden, um CA SDM-Portlets in das Portal einzuschließen.

So schließen Sie Portlets ein

1. Melden Sie sich bei CA SDM an, und klicken Sie auf der Registerkarte "Administration" im Optionsmanager auf "Suchen".

Das Fenster „Optionen – Liste“ wird angezeigt.

2. Klicken Sie auf "Portal_Safe_List".

Das Fenster „Portal_safe_list – Detail“ wird angezeigt.

3. Geben Sie in das Feld für den Optionswert *Servername:Portnummer* der Maschine ein, auf der das Portal installiert wurde.

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

4. Klicken Sie auf „Installieren“.
5. Starten Sie den CA SDM-Daemon neu.
6. Melden Sie sich bei CA Portal als Administrator an.
7. Erstellen Sie gültigen CA SDM-Benutzer. Weitere Informationen zum Erstellen von Benutzern finden Sie in der CA Portal-Dokumentation.

Hinweis: Das Kennwort, das bei der Erstellung dieses Benutzers im Portal verwendet wurde, kann von dem Kennwort abweichen, das derselbe Benutzer für die Anmeldung bei CA SDM verwendet, weil CA SDM die Benutzer bei dieser Integration unter Verwendung einer Kombination aus Benutzername, einer gültigen CA Portal-Sitzung und dem CA Portal-Installationswert authentifiziert, sofern dieser Wert in der Option "PORTAL_SAFE_LIST" vorhanden ist.

8. Markieren Sie "Knowledge" in der Hauptmenüleiste von CA Portal.
Die Seite „Knowledge“ wird angezeigt.
9. Markieren Sie „Bibliothek“ in der Leiste „Knowledge“ im linken Fensterbereich.
Im linken Fensterbereich wird der Bibliotheksbaum angezeigt.
10. Markieren Sie einen Order (oder erstellen ihn bei Bedarf und markieren ihn dann) im Bibliotheksbaum, und wählen Sie dann "Datei veröffentlichen" in der Leiste "Knowledge" des rechten Fensters.

Das Formular „Datei veröffentlichen“ wird geöffnet.

11. Geben Sie die folgende URL des CA SDM-Portlets in das Textfeld „Inhalt“ der Registerkarte „Allgemeine Informationen“ ein:

```
http://hostname:portnumber/CAisd/PortalServlet?USERNAME=$USER.username&PORTALSESSION=$SESSION$&PORTALINSTALL=portalhostname:portalportnumber
```

Hinweis: Ersetzen Sie "*hostname:portnumber*" in der URL durch den Namen und den Port des Webserver, auf dem sich CA SDM befindet. Ersetzen Sie *Hostname:des Portals:Portnummer des Portals* in der URL durch den Namen und den Port des Webserver, auf dem sich das Portal befindet.

12. Geben Sie "CA SDM" in das Textfeld "Titel" ein.
13. Klicken Sie auf „Erweitert“.

Die Seite „Erweiterte Eigenschaften“ des Formulars „Datei veröffentlichen“ wird angezeigt.

14. Geben Sie im Feld "MIME Content Type" *portal/variable-url* ein, und klicken Sie auf „Veröffentlichen“.

Der veröffentlichte Inhalt wird im markierten Bibliotheksordner angezeigt.

15. Konfigurieren Sie den Arbeitsplatz, um dieses Portlet anzuzeigen.
16. Melden Sie sich ab und wieder als der neu erstellte Benutzer an. Sie sollten automatisch bei CA SDM in dem Portlet angemeldet sein, das Sie gerade erstellt haben, ohne dass Sie sich erneut anmelden müssen.

Hinweis: Während der Ausführung von CA SDM im Portlet steht die Voreinstellung "Popups vermeiden" auf der Seite "Voreinstellungen" nicht zur Verfügung, und es wird ungeachtet der Voreinstellung stets ein Popup-Fenster verwendet.

Verbindung zum CA Portal-Server

Um die Verbindung zum CA Portal-Server herzustellen, öffnen Sie einen Webbrowser, und geben Sie folgende URL in die Adresszeile ein:

`http://<servername>:<port#>/servlet/portal`

<servername>

den Servernamen (oder die IP-Adresse) des Portalservers angibt.

<port#>

die Portnummer angibt, die der CA Portal-Server überwacht. Sie haben die Portnummer bei der Installation des CA Portal-Servers angegeben. Der Standardport ist 8080.

Konfigurieren von CA SDM für die Verwendung von SSL mit CA Portal

Hinweis: Für Produktionszwecke wird empfohlen, ein Zertifikat von einer vertrauenswürdigen Zertifizierungsstelle anzufordern.

Bevor Sie CA SDM für die Verwendung von SSL konfigurieren, überprüfen Sie, ob die Integration von CA Portal und CA SDM ohne SSL funktioniert. Wenn die Integration ohne SSL funktioniert, können Sie Portlets einschließen.

Weitere Informationen:

[Integration von Portlets](#) (siehe Seite 637)

Einrichten von SSL mit Hilfe eines selbst unterzeichneten Zertifikats

So richten Sie die CA SDM-Portalintegration mithilfe eines selbst unterzeichneten Zertifikats ein

1. Geben Sie in der Befehlszeile Folgendes ein:

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

Beantworten Sie die Aufforderungen angemessen und geben Sie für beide Kennwortaufforderungen "changeit" ein.

Dadurch wird das Zertifikat eingerichtet.

2. Bearbeiten Sie die Datei "server.xml" im Verzeichnis:

```
$NX_ROOT/bopcfg/www/CATALINA_BASE/conf
```

3. Entfernen Sie die Kommentarsymbole im folgenden Abschnitt, und speichern Sie die Datei:

```
<!--  
<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" /></Connector>  
-->
```

4. Fügen Sie das Attribut "keystoreFile" zur Datei "server.xml" hinzu. (Wenn Sie den Befehl in Schritt 1 ausführen, wird eine "keystore"-Datei im Stammverzeichnis des Benutzers erstellt. Fügen Sie dem Attribut „keystoreFile“ die Referenz hinzu, und speichern Sie die Datei. Ihre Datei "server.xml" sollte wie folgt aussehen:

```
<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="location/.keystore" />  
    </Connector>
```

5. Starten Sie CA SDM neu.
6. Verweisen Sie den Browser an <https://hostname:8443>, um die SSL-Funktion zu prüfen. Daraufhin sollte ein Dialogfeld mit einer Sicherheitswarnung eingeblendet werden. Klicken Sie auf „Ja“.

Hinweis: SSL verwendet den Port 8443

7. Ersetzen Sie das CA SDM-Portlet, damit HTTPS und Port 8443 verwendet werden.

`https://Hostname:8443/CAisd/PortalServlet?`

`USERNAME=$USER.Benutzername&PORTALSESSION=$SESSION&PORTALINSTALL=Portal-Hos
tname:Portal-Portnummer`

Herstellen einer Verbindung zu CA SDM, wenn CA Portal SSL verwendet

Sie können das Zertifikat des CA Portal-Servers importieren, damit (bei der Konfiguration von CA Portal zur Verwendung von SSL) eine vertrauenswürdige Verbindung zwischen CA SDM und CA Portal hergestellt werden kann.

So stellen Sie eine Verbindung zu CA SDM her, wenn das Portal SSL verwendet

1. Stellen Sie sicher, dass CA Portal konfiguriert ist und mit SSL funktioniert.

Hinweis: Informationen zum Überprüfungsprozess finden Sie in der CA Portal-Dokumentation.

2. Exportieren Sie das Zertifikat wie folgt von dem Computer, auf dem CA Portal installiert ist:

- a. Suchen Sie die Datei `server.xml` im folgenden Verzeichnis:

`PORTAL_Install_Dir\jakarta-tomcat-4.1.29\conf.`

- b. Notieren Sie das Verzeichnis und das Kennwort (`pwd`) von `keystore`, wie in den folgenden Zeilen von `server.xml` beschrieben. Das Standardkennwort ist *changeit* (in Kleinbuchstaben). Wenn Sie bei der Erstellung des Zertifikats während der Portal-Einrichtung ein benutzerdefiniertes Kennwort verwendet haben, müssen Sie das benutzerdefinierte Kennwort verwenden. Weitere Informationen finden Sie in der CA Portal-Dokumentation. In den folgenden Schritten und Beispielen wird *changeit* als Standardkennwort verwendet:

```
<!-- Define a SSL Coyote HTTP/1.1 Connector on port 8443 -->
<Connector className="org.apache.coyote.tomcat4.CoyoteConnector"
  port="8443" minProcessors="5" maxProcessors="150"
  enableLookups="true"
  acceptCount="100" debug="0" scheme="https" secure="true"
  useURValidationHack="false" disableUploadTimeout="true">
  <Factory className="org.apache.coyote.tomcat4.CoyoteServerSocketFactory"
    keystoreFile="c:\Program Files\CA\SC\Unicenter Management
Portal\UMPkeystore"
    keystorePass="changeit"
    clientAuth="false" protocol="TLS" />
</Connector>
```

- c. Navigieren Sie auf dem Portalserver zum JRE-bin-Verzeichnis ("`PORTAL_Install_Dir\jre\bin`"). So erhalten Sie Zugriff auf das Dienstprogramm "keytool", mit dessen Hilfe Sie das Zertifikat des PORTAL-Servers in eine Datei exportieren.

- d. Rufen Sie das Dienstprogramm "keytool" über den folgenden Befehl auf:
- ```
keytool -export -alias tomcat -file umpserver.cer -keystore "c:\Program Files\CA\SC\Unicenter Management Portal\UMPkeystore"
```

Geben Sie das Kennwort von keystore ein: *changeit*

Das Zertifikat befindet sich in der Datei <umpserver.cer>.

**Hinweis:** Achten Sie bei der Aufforderung zur Eingabe des Kennworts darauf, das in Schritt 2b abgerufene Kennwort zu verwenden. Im vorherigen Beispiel ist *changeit* das in Schritt 2b festgelegte Kennwort. Das Verzeichnis von keystore erhalten Sie ebenfalls aus Schritt 2b.

3. Importieren Sie das vom Server abgerufene Zertifikat auf den Computer mit der CA SDM-Installation. Verwenden Sie dafür wie im Folgenden beschrieben das Dienstprogramm "keytool":

- a. Navigieren Sie auf dem CA SDM-Computer zum Verzeichnis "JRE\bin", das sich im Allgemeinen an folgenden Speicherort befindet:  
C:\Program Files\CA\SC\JRE\bin.
- b. Das Zertifikat muss in die von der CA SDM Java Virtual Machine verwendete Zertifizierungsstelle importiert werden.

Beispiel für einen solchen Import: In diesem Beispiel ist der Speicherort der Zertifizierungsstelle die Folgende:

C:\Programme\CA\SC\JRE\1.4.2\_06\lib\security\cacerts

Wenn Sie zur Eingabe eines "*pwd*" aufgefordert werden, geben Sie "*changeit*" ein. Wenn die Aufforderung "*Trust this certificate*" (diesem Zertifikat vertrauen) angezeigt wird, geben Sie "Ja" ein.

```
Keytool.exe -import -alias tomcat -trustcacerts -file umpserver.cer
-keystore "C:\Program Files\CA\SC\JRE\1.4.2_06\lib\security\cacerts"
```

Geben Sie das Kennwort von keystore ein: *changeit*

Eigentümer: CN=ump001.ca.com, OU=unicenter, O=ca, L=islandia, ST=ny, C=us  
Aussteller: CN=ump001.ca.com, OU=unicenter, O=ca, L=islandia, ST=ny, C=us  
Seriennummer: 43ecb469

Gültig ab: Fr. 10. Feb. 10:42:33 EST 2006 bis: Do. 11. Mai 11:42:33 EDT 2006  
Certificate fingerprints: (Zertifikat-"Fingerabdrücke":)

MD5: A1:AF:AE:92:39:2E:53:D5:1C:6D:FE:44:68:61:DD:5C

SHA1:

66:3A:BC:77:32:81:60:89:70:B9:EF:FB:74:3D:93:74:CD:8E:E2:D2

Trust this certificate? (Diesem Zertifikat vertrauen?) [nein]: ja

Certificate was added to keystore (Zertifikat wurde zu keystore hinzugefügt)

**Hinweis:** Verwenden Sie bei der Aufforderung zur Eingabe des Kennworts das in Schritt 2b abgerufene Kennwort. Im vorherigen Beispiel ist *changeit* das in Schritt 2b festgelegte Kennwort.

4. Bearbeiten Sie die Datei "portal-xml-api.xml" in "\$NX\_ROOT\bopcfg\www\CATALINA\_BASE\webapps\CAisd\WEB-INF\xml\portal-xml-api.xml" wie folgt:
  - a. Ersetzen Sie "http" in der Zeile:
 

```
<!DOCTYPE PORTAL SYSTEM
"http://127.0.0.1:8080/servlet/media/xml/api/request.dtd">
```

 durch "https":
 

```
<!DOCTYPE PORTAL SYSTEM
"https://127.0.0.1:8080/servlet/media/xml/api/request.dtd">
```
  - b. Speichern Sie die Datei.
  - c. Wenn "Portal\_Safe\_List" installiert wurde, müssen Sie die Portnummer zu "8443" ändern, und der Computernamen muss den Domännennamen enthalten (z. B. "computername.ca.com:8443").

**Wichtig!** Der Domänenname muss im Computernamen enthalten sein, da das Portalzertifikat den Domännennamen einschließt. Weitere Informationen finden Sie in der CA Portal-Dokumentation.

5. Starten Sie den CA SDM-Server erneut.
6. Stellen Sie von CA Portal eine Verbindung zum CA SDM-Portlet her, und verwenden Sie dabei die folgende URL:

```
http://hostname:portnumber/CAisd/PortalServlet?USERNAME=$USER.username$&PORTALSESSION=$SESSION$&PORTALINSTALL=servername:8443
```

**Hinweis:** Ersetzen Sie "servername" in der URL durch den Namen des Webserver, auf dem sich CA Portal befindet. Der Servername ("servername") in dieser URL muss den Domännennamen enthalten, z. B. "Servername.ca.com:8443". Ersetzen Sie "hostname:portnumber" in der URL durch den Namen und den Port des Webserver, auf dem sich CA SDM befindet.

#### Weitere Informationen:

[Integration von Portlets](#) (siehe Seite 637)

## Integration von Mainframe-Produkten

CA SDM-Ergänzungsdaten (.dat-Datei) werden der Integration von Mainframe-Produkten zugeordnet.

## Laden von CA SDM-Ergänzungsdaten

Die CA SDM-Ergänzungsdaten (.dat-Datei) für die Integration von Mainframe-Produkten sind in einer Liste zusammengefasst, in der jeweils eine .dat-Datei einem Mainframe-Produktamen zugeordnet ist.

**Hinweis:** Der CA SDM-Server ist standardmäßig für die Verwendung der ITIL-Methodologie konfiguriert.

Um CA SDM-Ergänzungsdaten zu laden, um eine bestimmte Integration zu aktivieren, verwenden Sie `pdm_userload -f integXXX.dat`.

Die Datendateien befinden sich im Verzeichnis `$NX_ROOT\data\integrations\`.

**Hinweis:** Informationen zum Aktivieren der Anrufseite (Mainframe-Produktseite) der Integration finden Sie im Handbuch *CA Common Services for z/OS - CA Service Desk Integration Guide*.

## CA-Produkte, die gegenwärtig CAISDI nutzen

Die folgende Tabelle enthält die CA-Mainframe-Produkte, die gegenwärtig CAISDI nutzen, sowie die zugehörigen .dat-Dateien.

| CA-Produkt                                                  | Primäre Datendatei                | ITIL-Aktualisierungsdatei                   |
|-------------------------------------------------------------|-----------------------------------|---------------------------------------------|
| CA Advantage EDBC                                           | integEDBC.dat                     |                                             |
| CA 1 Tape Management                                        | integCA1.dat                      | itil_integCA1.dat                           |
| CA Allocate DASD Space and Placement                        | integAllocate.dat                 | itil_integAllocate.dat                      |
| CA Disk Backup and Restore                                  | integDisk.dat                     | itil_integDisk.dat                          |
| CA TLMS Tape Management (CA TLMS)                           | integTLMS.dat                     | itil_integTLMS.dat                          |
| CA Vantage Storage Resource Manager (CA Vantage SRM)        | integVantage.dat                  | itil_integVantage.dat                       |
| CA 7 Workload Automation (CA 7 WA)                          | integCA7.dat                      | itil_integCA7.dat                           |
| CA JARS Resource Accounting (CA JARS RA)                    | integJARS.dat<br>integJARSMVS.dat | itil_integJARS.dat<br>itil_integJARSMVS.dat |
| CA MIM Resource Sharing (CA MIM RS)                         | integMIM.dat                      | itil_integMIM.dat                           |
| CA OPS/MVS Event Management and Automation (CA OPS/MVS EMA) | integOPSMVS.dat                   | itil_integOPSMVS.dat                        |
| CA SYSVIEW Performance Management (CA SYSVIEW)              | integSysview.dat                  | itil_integSysview.dat                       |

|                                                                         |                    |                         |
|-------------------------------------------------------------------------|--------------------|-------------------------|
| CA NetMaster Network Management für TCP/IP (CA NetMaster NM für TCP/IP) | integNetMaster.dat | itil_integNetMaster.dat |
| CA NetMaster Network Management für SNA (CA NetMaster NM für SNA)       | integNetMaster.dat | itil_integNetMaster.dat |
| CA NetMaster Network Automation (CA NetMaster NA)                       | integNetMaster.dat | itil_integNetMaster.dat |
| CA NetMaster                                                            | integNetMaster.dat | itil_integNetMaster.dat |
| CA NetMaster Network Operations für TCP/IP (CA NetMaster NO für TCP/IP) | integNetMaster.dat | itil_integNetMaster.dat |
| CA NetMaster File Transfer Management (CA NetMaster FTM)                | integNetMaster.dat | itil_integNetMaster.dat |
| CA MICS Resource Management (CA MICS)                                   | integNeuMICS.dat   | itil_integNeuMICS.dat   |

## CA-Produkte, bei denen die Nutzung von CAISDI geplant ist

Die folgende Tabelle enthält die CA-Mainframe-Produkte, bei denen die Nutzung von CAISDI geplant ist, sowie die zugehörigen .dat-Dateien.

| CA-Produkt                                                | Primäre Datendatei  | ITIL-Aktualisierungsdatei |
|-----------------------------------------------------------|---------------------|---------------------------|
| CA 2E                                                     | integ2e.dat         |                           |
| CA Enterprise Workload Automation                         | integAutoSys.dat    |                           |
| CA Bundl                                                  | integBundl.dat      |                           |
| CA 11 Enterprise Workload Automation Restart and Tracking | integCA11.dat       |                           |
| CA Connect                                                | integConnect.dat    |                           |
| CA Datamacs                                               | integDatamacs.dat   |                           |
| CA Date Simulator                                         | integDate.dat       |                           |
| CA Deliver                                                | integDeliver.dat    | itil_integDeliver.dat     |
| CA Dispatch                                               | integDispatch.dat   | itil_integDispatch.dat    |
| CA FAVER VSAM Data Protection                             | integFaver.dat      |                           |
| CA FileAge                                                | integFileAge.dat    |                           |
| CA File Master Plus                                       | integFileMaster.dat |                           |
| CA Filesave RCS Automated Recovery                        | integFileSave.dat   |                           |
| CA Gen                                                    | integGen.dat        |                           |
| CA GSS (allgemeine Komponente)                            | integGSS.dat        |                           |

|                                            |                      |                       |
|--------------------------------------------|----------------------|-----------------------|
| CA InterTest                               | integInterTest.dat   |                       |
| CA JCLCheck Enterprise Workload Automation | integJCLCheck.dat    |                       |
| CA Jobtrac Job Management                  | integJobtrac.dat     | itil_integJobtrac.dat |
| CA LPD Report Convergence                  | integLPD.dat         |                       |
| CA Optimizer                               | integOptimizer.dat   |                       |
| CA Optimizer/II                            | integOptimizerII.dat |                       |
| CA Plex                                    | integPlex.dat        |                       |
| CA Scheduler Job Management                | integScheduler.dat   |                       |
| CA Spool Enterprise Print Management       | integSpool.dat       | itil_integSpool.dat   |
| CA SymDump                                 | integSymDump.dat     |                       |
| CA Verify                                  | integVerify.dat      |                       |
| CA View                                    | integView.dat        | itil_integView.dat    |

## Integration von CA Business Service Insight

CA Business Service Insight (CA BSI) ermöglicht es Ihnen, IT-Service-Performance zu verwalten, wie z. B. das Integrieren von Service- und Service-Level-Performance-Management und das Nutzen von Servicebewertungen und -vergleichen. CA BSI hilft Ihrer Organisation dabei festzustellen, inwieweit Services die Vorgaben in Service Level Agreements (SLAs) erfüllen. CA BSI stellt Service Desk-Analysten in CA SDM Service Level Management (SLM)-Informationen zur Verfügung, um Änderungen an verschiedenen IT-Services in der Organisation zu verwalten. Diese SLM-Informationen ermöglichen eine bessere Entscheidungsfindung und eine verbesserte IT-Bereitstellung.

Die CA BSI-Integration fügt Registerkarten hinzu, die auf CI-Detailformularen in CA SDM angezeigt werden. Die Berichte "Service Level Compliance and Modified Service Level by Metrics vs Target" stellen Informationen über CIs in Familie "Unternehmensservice" von CA SDM bereit. Der Bericht "Modified Service Level by Contract vs Target" stellt Informationen über die CIs für die Vertragsfamilie in CA SDM bereit.

**Hinweis:** Diese Registerkarten werden nur für Cls mit föderierten Asset-Zuordnungen zum CA BSI-MDR angezeigt.

Wenn Sie CA SDM in CA BSI integrieren, können Anwender Metrikdaten für Vertrags-ClS anzeigen, die einem CA BSI-MDR zugeordnet sind. Anwender müssen eine Vertragspartei (CA BSI-Entität) angeben, bevor sie den Request senden. Eine CA BSI-Einschränkung verhindert die ordnungsgemäße Anzeige von Metrikdaten für Vertragsparteien, deren Name bestimmte nichtalphanumerische Zeichen enthält. Wir empfehlen, alphanumerische Namen für Vertragsparteien zu verwenden und die Verwendung der folgenden Zeichen zu vermeiden:

reserviert = generische Trennzeichen / Untertrennzeichen

generische Trennzeichen = : / ? # [ ] @

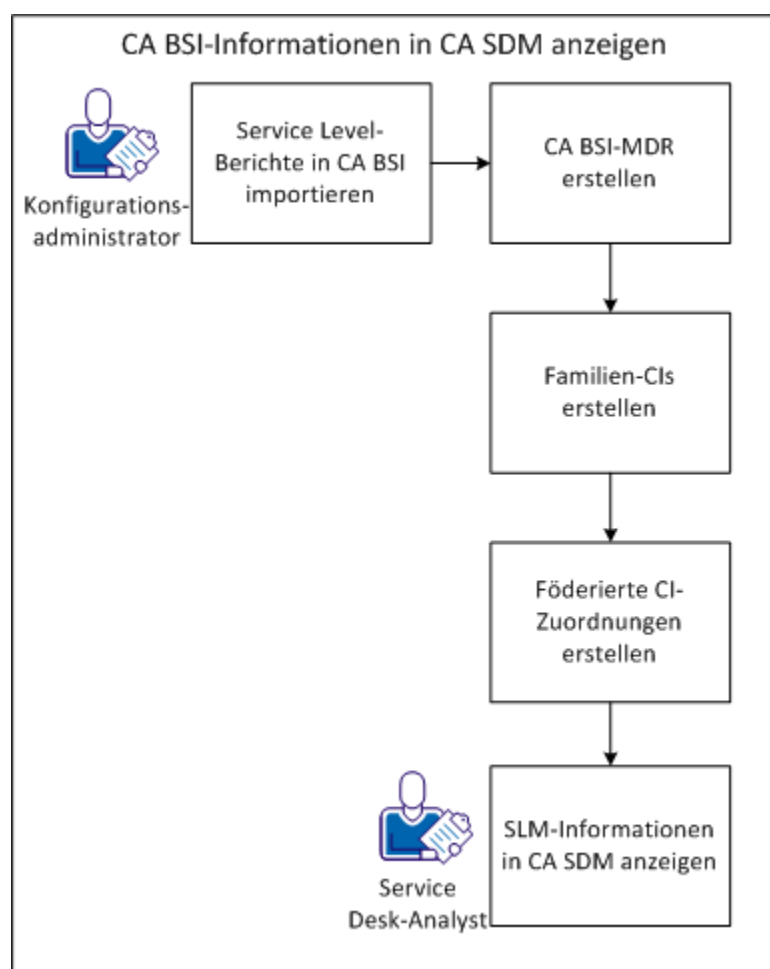
Untertrennzeichen = ! \$ & ' ( ) \* + , ; =

## Anzeigen von CA BSI-Informationen in CA SDM

Eine Organisation möchte die Verwaltung von Änderungen in IT-Services verbessern und beschließt, CA BSI und CA SDM zu integrieren. Mit der Integration kann CA BSI Informationen des Service Level Management (SLM) in CA SDM exportieren. Der Konfigurationsadministrator importiert die Berichte in CA BSI und konfiguriert CA SDM, sodass ein Service Desk-Analyst die SLM-Informationen anzeigen kann.

Service Desk-Analysten arbeiten mit diesen Informationen, um die Bereitstellung ihrer IT-Services zu verbessern.

Folgendes Diagramm erklärt, wie ein Konfigurationsadministrator CA BSI aktiviert, um SLM-Daten in CA SDM zu exportieren, sodass ein Service Desk-Analyst die Informationen anzeigen kann:



1. [Importieren von Service Level-Berichten in CA BSI](#) (siehe Seite 649).
2. [Erstellen eines CA BSI-MDR](#) (siehe Seite 649).
3. [Erstellen der Familien-CIs](#) (siehe Seite 650).



4. [Erstellen von föderierten CI-Zuordnungen](#) (siehe Seite 651).
5. [Anzeigen von SLM-Informationen in CA SDM](#) (siehe Seite 652).

## Importieren von Service Level-Berichten in CA BSI

CA BSI stellt standardmäßig den *Service Level Compliance-Bericht* bereit. Die Registerkarte "BSI-Service" wird auf den CI-Detailseiten in CA SDM angezeigt, und es wird die Anzahl der Überschreitungen und Verletzungen angezeigt. Sie importieren die Berichte *Modified Service Level by Metrics vs Target* und *Modified Service Level by Contract vs Target* in CA BSI.

### Gehen Sie wie folgt vor:

1. Kopieren Sie die Datei "\$NX\_ROOT/samples/BSI/bsireports.sql" in den CA BSI-Datenbankserver.  
  
Dieses Oracle-Skript enthält die Berichtsdefinitionen, die für die Integration zwischen CA BSI und CA SDM erforderlich sind.
2. Stellen Sie mit einem Anwender, der über die Rolle "SYSDBA" verfügt, eine Verbindung zur CA BSI-Oracle-Instanz her oder stellen Sie eine Verbindung als Datenbankeigentümer her.  
  
**Wichtig!** Dieser Anwender *muss* Aktualisierungsrechte für die Datenbank haben. Bestätigen Sie, dass Sie mit Ihrem Oracle-Datenbankadministrator über diese Berechtigungen verfügen.
3. Führen Sie das Skript "bsireports.sql" aus, und stellen Sie sicher, dass keine Fehler auftreten.  
  
Die Berichte sind für die CA SDM-Integration verfügbar.

## Erstellen eines CA BSI-MDR

Der Konfigurationsadministrator erstellt ein MDR für CA BSI in CA SDM. Dieses MDR stellt Informationen über den CA BSI-Server bereit, wie z. B. der Hostname und die ID des berechtigten Anwenders.

### Gehen Sie wie folgt vor:

1. Klicken Sie auf der Registerkarte "Administration" auf "CA", "CMDDB", "MDR-Management", "MDR-Liste".
2. Klicken Sie auf "Neu erstellen".
3. Geben Sie folgende Beispielinformationen an:
  - Geben Sie **BSI** für "Klassenname" an.
  - Geben Sie Beschriftungen für die Schaltfläche und die MDR-Namen ein.  
Geben Sie z. B. **BSI** ein.

- Geben Sie den Hostnamen des primären CA BSI-Servers ein.
- Geben Sie **sadmin** als Anwender-ID ein, und geben Sie **CA** für "Gemeinsamer geheimer Schlüssel" ein.

**Hinweis:** Diese Informationen hängen von Ihrem Anwendernamen und von Ihrer Organisation ab. Bestätigen Sie diese Informationen mit Ihrem CA BSI-Administrator.

- Löschen Sie alle Inhalte im Feld "Im Kontext zu startende URL".
4. Klicken Sie auf "Speichern", und schließen Sie das Fenster.

## Erstellen Sie der CIs in CA SDM

Erstellen Sie die CIs für den Unternehmensservice und die Vertragsfamilie in CA SDM. Diese CIs entsprechen CA BSI-Daten, die Sie in CA SDM anzeigen möchten. In diesem Beispiel erstellen Sie Service 1 und Vertrag 7.

### Gehen Sie wie folgt vor:

1. Klicken Sie auf der Registerkarte "Administration" auf "CA CMDB", "CIs - Liste".
2. Klicken Sie auf "Neu erstellen".
3. Geben Sie die folgenden Informationen an:
  - Geben Sie **Service 1** als Namen ein.
  - Geben Sie **Business-Service** als Klasse ein.
4. Klicken Sie auf "Fortsetzen".
5. Klicken Sie auf "Speichern", und schließen Sie das Fenster.
6. Erstellen Sie ein anderes CI mit folgenden Informationen:
  - Geben Sie **Vertrag 7** als Namen ein.
  - Geben Sie **Lizenzvereinbarung** als Klasse ein.
7. Klicken Sie auf "Fortsetzen".
8. Klicken Sie auf "Speichern", und schließen Sie das Fenster.

## Erstellen von föderierten CI-Zuordnungen

Erstellen Sie föderierte CI-Zuordnungen, um die Integration zwischen CA BSI und CA SDM fertigzustellen. Diese Zuordnung gibt Informationen über ein CI an. In diesem Beispiel ordnen Sie Service 1 und Vertrag 7 dem BSI-MDR zu.

### Gehen Sie wie folgt vor:

1. Klicken Sie auf der Registerkarte "Administration" auf "CA CMDB", "MDR-Management", "Föderierte CI-Zuordnung".
2. Klicken Sie auf "Neu erstellen".
3. Füllen Sie die folgenden Felder aus:
  - Geben Sie **Service 1** für "CI-Name" und "Föderierte Asset-ID" ein.
  - Geben Sie **BSI** für "MDR-Name" an.

**Wichtig!** Stellen Sie sicher, dass Sie die gleiche föderierte Asset-ID wie die Namen für Service und Vertrag in CA BSI eingeben.
4. Klicken Sie auf "Speichern", und schließen Sie das Fenster.
5. Erstellen Sie eine weitere Zuordnung, und füllen Sie folgende Felder aus:
  - Geben Sie **Vertrag 7** für "CI-Name" und "Föderierte Asset-ID" ein.
  - Geben Sie **BSI** für "MDR-Name" an.
6. Klicken Sie auf "Speichern", und schließen Sie das Fenster.

## Anzeigen von SLM-Informationen in CA SDM

Der Service Desk-Analyst zeigt SLM-Informationen an, um Änderungen in IT-Services innerhalb Ihrer Organisation zu verwalten. Sie möchten beispielsweise die Verletzungen analysieren, die für Service 1 angezeigt werden.

### Gehen Sie wie folgt vor:

1. Klicken Sie auf der Registerkarte "Administration" auf "CA CMDB", "CIs - Liste".
2. Suchen Sie nach den CIs des Unternehmensservice und der Vertragsfamilie, die Sie in CA BSI integriert haben.
3. Öffnen Sie eine Enterprise Service CI-Familie, um die Registerkarten "BSI-Service" und "BSI-Service nach Metrik" anzuzeigen.
4. Klicken Sie auf "BSI-Service", um Informationen zu Überschreitungen und Vertragsverletzungen aus *Service Level-Compliance*-Daten in CA BSI anzuzeigen.

Die Daten zu Überschreitungen und Vertragsverletzungen aus dem *Service Level-Compliance-Bericht* von CA BSI werden für Service 1 angezeigt.

5. Klicken Sie auf "BSI-Service nach Metrik", um den Bericht "Metrik", "Vertragsverletzung", "Konform" und "Ziel" aus den Daten von *Modified Service Level by Metric vs Target* in CA BSI anzuzeigen.
6. Öffnen Sie ein Vertragsfamilien-CI, das Sie in CA BSI integriert haben, und klicken Sie auf die Registerkarte "BSI-Vertrag nach Metrik".

**Hinweis:** Kontakt-CIs enthalten die Registerkarte "BSI-Vertrag nach Metrik". Diese Registerkarte enthält ein Textfeld, in dem Sie die Vertragspartei des Vertrags eingeben, um Informationen aus dem Bericht *Modified Service Level by Contract vs Target* in CA BSI abzurufen.

Sie haben jetzt CA BSI mit CA SDM erfolgreich integriert, um SLM-Informationen in CA SDM anzuzeigen.

# Kapitel 14: Beispiele-Verzeichnis

---

Dieses Kapitel enthält folgende Themen:

[Inhalt des Beispiele-Verzeichnisses](#) (siehe Seite 653)

## Inhalt des Beispiele-Verzeichnisses

Sie können mehrere Dateien im Verzeichnis "\$NX\_ROOT/samples" für die Verwendung mit verschiedenen externen Schnittstellen ändern. Diese Dateien sind in mehreren Unterverzeichnissen gruppiert. Die Dateien im Beispiele-Verzeichnis sind in ihrem Auslieferungszustand nicht ausführbar.

## Ändern des Meldungskatalogs

Um den Meldungskatalog zu ändern, führen Sie die folgenden Schritte aus:

1. Richten Sie sich nach dem Format von "pdm.xml", das sich in "\$nx\_root\bin" befindet.
2. Erstellen Sie eine angepasste Kopie von "pdm.xml" und platzieren Sie sie im Verzeichnis "\$nx\_root\msg\_catalog".
3. Fügen Sie Meldungen in den XML-Meldungsdateien aus dem vorherigen Schritt hinzu und/oder ändern Sie sie.

## call\_mgt

Enthält Beispiele für die Anpassung im Anfragemanagement.

### **gencr.frg**

Diese Datei kann in Verbindung mit "bop\_cmd" verwendet werden, um Anfragen von einer Befehlszeile aus zu erstellen. Es treten alle Benachrichtigungen und Aktivitätsprotokolleinträge auf, bei der Erstellung wird jedoch kein Anfrageformular auf dem Server angezeigt. Sie müssen den Parameter "-u" verwenden, um "gencr.frg" mit dem Hilfsprogramm "bob\_cmd" auszuführen. Lesen Sie unbedingt die Datei "gencr\_readme.txt", um die Syntax kennen zu lernen und die Datei bei Bedarf zu ändern. Die Datei sollte Verzeichnis "\$NX\_ROOT/site/mods/interp" abgelegt werden; erstellen Sie dieses Verzeichnis, falls es nicht vorhanden ist. Beispiel: bop\_cmd -d domsrvr -u nsm -f gencr.frg "gencr( 'Meine Beschreibung' )"

### **iss\_site.mod**

Dieses Datei kann verwendet werden, um bei Issues die Aktivitätsprotokollierung für Felder einzuschalten, die an den Einsatzort angepasst wurden. Diese Datei sollte in "\$NX\_ROOT/site/mods/majic<cs/>" gespeichert werden, nachdem sie für die Standort-Felder geändert wurde.

### **cr\_site.mod**

Dieses Datei kann verwendet werden, um bei Issues die Aktivitätsprotokollierung für Felder einzuschalten, die an den Einsatzort angepasst wurden. Diese Datei sollte in "\$NX\_ROOT/site/mods/majic<cs/>" gespeichert werden, nachdem sie für die Standort-Felder geändert wurde.

### **chg\_site.mod**

Dieses Datei kann verwendet werden, um bei Issues die Aktivitätsprotokollierung für Felder einzuschalten, die an den Einsatzort angepasst wurden. Diese Datei sollte in "\$NX\_ROOT/site/mods/majic<cs/>" gespeichert werden, nachdem sie für die Standort-Felder geändert wurde.

### **gencr\_readme.txt**

Diese Datei enthält Anweisungen zur Verwendung der Datei "gencr.frg"

### **chg\_site.spl**

Diese Datei kann geändert werden, um die Zuordnung der Attribute zu ändern, wenn Sie einen Change aus einer Anfrage erstellen. Diese Datei sollte im Verzeichnis "\$NX\_ROOT/site/mods/majic" gespeichert werden, nachdem Sie die entsprechenden Änderungen vorgenommen haben.

**audlog\_site.mod**

Diese Datei kann verwendet werden, um die Audit-Protokollierung für Felder einzuschalten, die an den Einsatzort angepasst wurden. Diese Datei sollte in "\$NX\_ROOT/site/mods/majic<cs/>" gespeichert werden, nachdem sie für die Standort-Felder geändert wurde.

**Notify\_add.spl (nur UNIX)**

Diese Datei kann verwendet werden, um den Protokollagenten der Anfrage, den Zuständigen und der Gruppe zur Benachrichtigungsliste der Anfrage hinzuzufügen. Diese Datei sollte in "\$NX\_ROOT/site/mods/majic<cs/>" gespeichert werden.

**Notify\_replace.spl (nur UNIX)**

Diese Datei kann verwendet werden, um den Protokollagenten der Anfrage, den Zuständigen und der Gruppe zur Benachrichtigungsliste der Anfrage hinzuzufügen. Diese Datei sollte in "\$NX\_ROOT/site/mods/majic<cs/>" gespeichert werden.

## Daten

Dieses Verzeichnis enthält Dateien, die das logische Datenmodell für die meisten Datenbanktabellen in CA SDM darstellen. Dieses Datenverzeichnis enthält auch Beispieldaten für Knowledge Management.

## macro\_lock

Diese Datei enthält ein SPEL-Fragment, das mithilfe des Befehls „bop\_cmd“ ausgeführt werden kann, um Sperrungen aufzuheben, die von Makros gesetzt wurden.

## Mehrere Mandanten

Dieses Verzeichnis enthält Beispieldateien für das Verwalten von mehreren Mandanten.

**Weitere Informationen:**

[Konvertieren einer vorhandenen Mandanten-Implementierung in das Mandantenobjekt](#)  
(siehe Seite 331)

[Füllen des Attributs "Mandant" in Tabellen](#) (siehe Seite 332)

## pdmconf

**web.xml.tpl**

**pdm\_startup.tpl**

**pdm\_edit\_usage\_notes.htm**

**alias\_install.bat**

**web.cfg.tpl**

**pdm\_startup.i.tpl**

**pdm\_edit.pl**

**README\_Dateien**

Alle diese Dateien werden von "pdm\_edit.pl" verwendet, um Startdateien für einen Primärserver und Sekundärserver zu erstellen, auf denen verschiedene Daemons laufen.

## Berichterstellung

Dieses Verzeichnis enthält Dokumentation und Beispiele für das Konfigurieren der Offline-Berichterstellung.

**Weitere Informationen:**

[Replizierte Datenbank für Offline-Berichterstellung](#) (siehe Seite 272)

## sdk

Dieses Verzeichnis enthält eine Beispieldatei zur Erzeugung von CA SDM-SOAP-Web Service-Aufrufen.

"TableOfContents.doc" erläutert weitere Einzelheiten zu verfügbaren Elementen. Das Dokument befindet sich im folgenden Verzeichnis:

\$NX\_ROOT\samples\sdk\websvc

In "PKI\_loginServiceManaged\_JAVA\_steps.doc" und "PKI\_loginServiceManaged\_PERL\_steps.doc" wird erläutert, wie ServiceDesk für Anmeldungen mit digitalen Zertifikaten konfiguriert wird. Sie befinden sich im folgenden Verzeichnis:

\$NX\_ROOT\samples\sdk\websvc\java\test1\_pki

Im Folgenden werden Beispiele und Speicherorte für PERL und JAVA aufgeführt:

- PERL-Beispiele

\$NX\_ROOT\samples\sdk\websvc\perl\test1\_pki

Beispiel: "loginServiceManaged()"-Webservice-Aufruf



- JAVA-Beispiele

\$NX\_ROOT\samples\sdk\websvc\java\test1\_pki

Beispiel: "loginServiceManaged()" - und "getBopsid()" -Webservice-Aufruf

\$NX\_ROOT\samples\sdk\websvc\java\test2\_basic

Beispiel: Kombiniertes "CreateRequest()" - und  
"CreateChangeOrder()" -Webservice-Aufruf

## Ansichten

Dieses Verzeichnis enthält Datenbankskripte, die für Migration, Verwaltung von mehreren Mandanten und für andere Prozesse verwendet werden.

**Weitere Informationen:**

[Hinweise zur Datenbank](#) (siehe Seite 29)

[Implementieren der Mandantenfähigkeit](#) (siehe Seite 309)



# Kapitel 15: Laden von ergänzendem Inhalten

---

Dieses Kapitel enthält folgende Themen:

[sd\\_content.dat](#) (siehe Seite 659)

## sd\_content.dat

Ergänzender Inhalt für CA SDM ist in "sd\_content.dat" verfügbar. Diese Daten-Datei enthält die Datensätze "Change-Kategorie" und "Ursachen". Um die Daten von einem Befehlsfenster zu laden, gehen Sie zu "\$NX\_ROOT/data" und führen Sie den folgenden Befehl aus:

```
pdm_load -f sd_content.dat
```