

CA Asset Portfolio Management

Implementierungshandbuch (Implementation Guide)

Version 12.8



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.

Verweise zu CA Technologies-Produkten

Dieser Dokumentensatz bezieht sich auf die folgenden CA Technologies-Marken und -Produkte:

- CA Asset Converter
- CA Asset Portfolio Management (CA APM)
- CA Business Intelligence
- CA Client Automation
(früher CA IT Client Manager)
- CA CMDB
- CA Embedded Entitlements Manager (CA EEM)
- CA-Management-Datenbank (CA MDB)
- CA Process Automation™
- CA Service Catalog
- CA Service Desk Manager
- CA Software Asset Manager (CA SAM)
- CA SiteMinder®

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 9

Überblick	9
Zielgruppe	9
CA APM-Standardadministrator	10

Kapitel 2: Planen 11

Installationsplanung	11
Konfigurieren von Oracle	13
Konfigurieren von SQL Server	18
Überprüfen der Installation der Internetinformationsdienste	19
Entfernen von CA iTechnology iGateway	19
Installieren des Java Development Kit (JDK)	21
Installationstypen	21
Standardinstallation	22
Konfiguration der Standardinstallationskomponenten	22
Demo-Installation	24
Anwenderdefinierte Installation	24
Anwenderdefinierte Konfiguration von Installationskomponenten	25
Web-Farmen	26
Konfigurieren der Server in einer Web-Farm	27

Kapitel 3: Aktualisieren 29

So führen Sie ein Upgrade von Version 11.3.4 durch	29
Installieren Sie den kumulativen Patch 14 oder höher für die Version 11.3.4	30
Anhalten der Dienste	30
Deinstallieren der Version 11.3.4	30
Installieren von Version 12.8	31
So führen Sie ein Upgrade von Version 12.6 aus	31
Anhalten der Dienste	31
Deinstallieren der Version 12.6	32
Installieren von Version 12.8	34
So führen Sie ein Upgrade von Version 12.6.05 aus	34
Anhalten der Dienste	34
Deinstallieren der Version 12.6.05	35
Installieren von Version 12.8	36

Kapitel 4: Wird installiert **37**

Implementieren der Software	37
Installationsphasen	37
Phase vor der Installation: Installieren des Installations-Manager	38
Phase 1: Installieren von CCC und Auswählen des Installationstyps	39
Phase 2: Festlegen des erforderlichen Servers	40
Phase 3: Konfigurieren der Komponenten und Installieren des Produkts	40
Phase 4: Stellen Sie die Installation auf den zusätzlichen erforderlichen Servern fertig.	52
Aktualisieren der Apache Tomcat-Konfigurationsdatei	54
Konfigurieren von AMS für Sichere Netzwerkkommunikation	55
Konfigurieren des AMS für den Namen Ihres Domain Name System (DNS)	56
Konfigurieren des AMS mit Teiid	56
Konfigurieren des Export-Service für Sichere Netzwerkkommunikation	57
Starten der Dienste	58
Starten der Web-Schnittstelle	59
Überprüfen der Installation	60
Deinstallieren von CA APM	61

Kapitel 5: So migrieren Sie CA APM-Daten von Version 11.3.4 auf Version 12.8 **63**

So migrieren Sie CA APM-Daten von Version 11.3.4 auf Version 12.8	63
Überprüfen der Voraussetzungen	67
Starten des CA APM-Migrations-Toolkit	73
Ausführen der Prä-Migrationsberichte	73
Angaben der Umbenennungskonfiguration des Asset	82
Ausführen des Migrationshilfsprogramms	83
Ausführen der Post-Migrationsberichte für manuelle Migrationen	89
Migrationsberichtsdaten zur Referenz und Analyse	91
Starten der CA APM-Webschnittstelle	96
Ausführen von manuellen Migrationen	97
Ausführen einer Verifizierung der Post-Migration	115
Fehlerbehebung	115

Kapitel 6: Implementieren der Mandantenfähigkeit **119**

Mandantenfähigkeit	119
Service Provider	120
Mandantenfähigkeit - Funktionsweise	120
Auswirkung auf die Benutzeroberfläche	122
Mandantenanwender	122
Implementieren der Mandantenfähigkeit	123

Aktivieren der Mandantenfähigkeit	124
Verwaltung von Mandant, untergeordnetem Mandant und Mandantengruppen	125
Definieren eines Mandanten	125
Aktualisieren eines Mandanten	126
Aktivieren eines Mandanten	127
Initialisieren eines neuen Mandanten	128
Definieren von Mandantengruppen	128
Aktualisieren von Mandantengruppen	128
Mandantenhierarchien	129
Definieren von untergeordneten Mandanten	130
Aktualisieren von untergeordneten Mandanten	131
Systemverwaltete Mandantengruppen	131

Kapitel 7: Integration mit anderen Produkten 133

CA Business Intelligence-Integration	133
Integration von CA APM und CA Business Intelligence	134
Berichtskonfigurationen und Produktupdates	135
CA EEM-Integration	136
CA CMDB-Integration	136
Integration in CA APM und CA CMDB	137
Nutzen Sie die Änderungshistoriendatensätze von Assets und Configuration Items gemeinsam.	138
Kategorisieren von Asset- und Configuration Item-Datensätzen	138
Definieren eines zusätzlichen Asset-Feldes	141
Definieren eines Ereignisses in einem gemeinsam genutzten Feld	143
Definieren eines Management Data Repository (MDR) von CA Service Desk Manager und CA CMDB	143
CA Process Automation-Integration	144
Konfigurieren des CA Process Automation-Benachrichtigungsprozesses	144
Importieren der Workflow-Provider-Benachrichtigungsprozessdateien	145
Konfigurieren des CA Process Automation-Mailservers	146
Ändern der CA Process Automation-Workflow-Prozessparameter	147
Gestatten der CA Process Automation-Verwendung für CA APM-Anwender	149
Erforderliche Indikatoren und mehrzeilige Textfelder für Parameter	150
CA Service Catalog-Integration	151

Kapitel 8: Implementieren von CA SAM mit CA APM 153

Überblick	153
CA APM- und CA SAM-Datensynchronisation	154
So implementieren Sie CA SAM mit CA APM	155
Überprüfen der Voraussetzungen	156
Überprüfen der Installation der Internetinformationsdienste	157
Installieren des CA SAM-Import- und Exportservices	158

Konfigurieren des CA SAM-Import- und Export-Services.....	158
Planen der Windows-Aufgabe für den Hardware-Import.....	160
Starten des CA APM-Event-Service	161
Aktivieren der Software Asset Management-Funktionen.....	161
Laden von CA APM-Daten in CA SAM	163
Empfehlungen zur Datenverwaltung	164
Manuelle Datensynchronisation	164
Datenverwaltung der Kostenstelle.....	165
Maßeinheiten des Inventars	166
Feldanforderungen für automatische Datensynchronisation	166
Assets mit nicht definierten Betriebssystemen	167
So deinstallieren Sie CA Software Compliance Manager	169

Kapitel 9: Fehlerbehebung 171

Fehlermeldung, dass die Installation nicht gestartet oder der angezeigte Server nicht gefunden wird	171
Browser-Fehlermeldung, dass Mandantenverwaltungs-Seite nicht angezeigt werden kann, wird angezeigt	171
Mandantenverwaltungs-Seite wird nicht angezeigt	172
Webserver benannt mit Unterstreichungszeichen	172
Anmeldung schlägt mit einem Anwendernamen fehl, der zusätzliche Zeichen enthält	172
WCF-Services schlagen fehl, wenn IIS 7 auf Windows 2008 installiert ist	173
Meldungen über fehlende Betriebssysteme werden in der Nachrichtenwarteschlange angezeigt	173

Kapitel 1: Einführung

Dieses Kapitel enthält folgende Themen:

[Überblick](#) (siehe Seite 9)

[Zielgruppe](#) (siehe Seite 9)

[CA APM-Standardadministrator](#) (siehe Seite 10)

Überblick

Dieses Handbuch bietet Ihnen Informationen, die Sie für eine erfolgreiche CA APM-Implementierung in Ihrem Unternehmen benötigen. Dazu gehören auch Anleitungen zum Durchführen der folgenden Aufgaben:

- Planen und Vorbereiten einer neuen Installation
- Installieren und Konfigurieren der notwendigen Produktkomponenten
- Integration mit anderen CA-Produkten

Hinweis: Die aktuellste Version der Versionshinweise mit den jeweils gültigen Systemvoraussetzungen finden Sie auf der [CA APM-Produktseite](#) auf CA Support Online.

Zielgruppe

Dieses Handbuch richtet sich an alle, die wissen möchten, wie CA APM installiert 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 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 APM erfolgreich in andere CA Technologies-Produkte zu integrieren.
- *Anwender* können bei Bedarf aufgrund der Informationen in diesem Handbuch das Produkt und die Komponenten installieren.

Um die Informationen in diesem Handbuch zu verwenden, müssen Sie Kenntnisse über das Windows-Betriebssystem haben und grundlegende administrative Aufgaben für Ihr Betriebssystem durchführen können.

CA APM-Standardadministrator

Ein CA APM-Standardanwender und eine Standardrolle "Systemadministrator" werden während der CA APM-Installation automatisch erstellt. Dieser Anwender verfügt über die vollständige Steuerung aller Aspekte des Produkts. Der Standardanwendername und das Standardkennwort für den CA APM-Anwender "Systemadministrator" lautet uapmadmin.

Hinweis: Aus Sicherheitsgründen empfehlen wir Ihnen, dass Sie das Standardkennwort ändern, nachdem Sie die Version 12.8-Installation fertiggestellt haben.

Nachdem die Installation abgeschlossen ist, stellen Sie sicher, dass alle Dienste gestartet wurden. Verwenden Sie dann die Anmeldeinformationen für den CA APM-Anwender "Systemadministrator", um die Webbenutzeroberfläche zu starten und zu überprüfen, ob das Produkt betriebsbereit ist.

Kapitel 2: Planen

Dieses Kapitel enthält folgende Themen:

[Installationsplanung](#) (siehe Seite 11)

[Installationstypen](#) (siehe Seite 21)

[Standardinstallation](#) (siehe Seite 22)

[Demo-Installation](#) (siehe Seite 24)

[Anwenderdefinierte Installation](#) (siehe Seite 24)

[Web-Farmen](#) (siehe Seite 26)

Installationsplanung

Verwenden Sie die folgenden Informationen zum Suchen und Sammeln von Informationen, die Sie beim Planen einer erfolgreichen CA APM-Installation unterstützen.

■ **Suche** - Führen Sie die folgenden Schritte durch:

- 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 und die optionale Readme-Datei (sofern vorhanden) finden Sie auf der [CA APM-Produktseite](#) auf CA Support Online.

- 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 APM 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.

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

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

- Machen Sie sich mit den verschiedenen Installationstypen für das Produkt vertraut. Berücksichtigen Sie Netzwerkverfügbarkeit, Verwendungsbandbreite und Reaktionsfähigkeit, wenn Sie entscheiden, welchen Installationstyp Sie verwenden möchten.
- Lesen Sie die Informationen über die Produktkomponenten, um die wesentlichen Merkmale kennenzulernen.

■ **Datenbank** - Führen Sie die folgenden Schritte durch:

- Lesen Sie das *Übersichtshandbuch der CA Management-Datenbank*. Machen Sie sich mit der CA MDB vertraut, legen Sie Ihre Bereitstellungsstrategie fest, und werden Sie sich aller SQL Server- oder Oracle-Probleme bewusst, die Sie lösen müssen, um die CA MDB zu verwenden.
- Entscheiden Sie, welche Datenbank (entweder SQL Server oder Oracle) Sie mit CA APM verwenden möchten, und installieren Sie diese.
- Konfigurieren Sie Oracle oder [SQL Server](#) (siehe Seite 18).
- (SQL Server) Stellen Sie sicher, dass SQL Server-Client-Tools auf allen Servern installiert sind, die auf die SQL Server-Datenbank zugreifen.
- (Oracle) Stellen Sie sicher, dass Oracle-Client-Tools, 32-Bit-Version, auf allen Servern installiert ist, die auf die Oracle-Datenbank zugreifen.

Hinweis: Wenn Sie CA SAM mit CA APM implementieren, können einige zusätzliche Schritte gelten. Wenn die CA APM-Datenbank SQL Server ist und die CA SAM-Datenbank Oracle ist, dann installieren Sie den Oracle-Client auf dem CA APM-Installationsserver und auf dem CA APM-Webserver, und [konfigurieren Sie den Net-Servicenamen für die CA SAM-Implementierung](#) (siehe Seite 16).

Hinweis: Wir empfehlen die CA APM-Komponenten nicht zu installieren, mit Ausnahme der CA MDB auf einem 64-Bit-Computer, der einen 64-Bit-Oracle-Datenbankserver hostet.

■ **CA Business Intelligence** - Führen Sie die folgenden Schritte durch:

- Lesen Sie die Informationen über die [CA Business Intelligence-Integration](#) (siehe Seite 133).
- Installieren Sie CA Business Intelligence, und zeichnen Sie die Anmelde- und Verbindungsinformationen auf.

Hinweis: Weitere Informationen über CA Business Intelligence finden Sie im *Installationshandbuch für CA Business Intelligence*.

■ **Internetinformationsdienste (IIS)** - Stellen [Sie sicher, dass die Internetinformationsdienste auf allen Anwendungs- und Webservern installiert sind](#) (siehe Seite 19).

- **CA EEM** - Führen Sie die folgenden Schritte durch:
 - Lesen Sie die Informationen über die [CA EEM-Integration](#) (siehe Seite 136).
 - Installieren von CA EEM.

Hinweis: Bevor Sie CA EEM auf 64-Bit-Computern installieren, stellen Sie sicher, dass CA iTechnology iGateway (32-Bit und 64-Bit) nicht auf dem Computer installiert ist, auf dem Sie CA EEM installieren. Wenn diese Komponente installiert ist, [entfernen Sie zunächst CA Technologies-iTechnology-iGateway](#), (siehe Seite 19) bevor Sie die CA EEM-Installation starten.

Hinweis: CA iTechnology iGateway ist eine gemein genutzte Komponente, die von verschiedenen CA Technologies-Produkten verwendet wird. CA iTechnology iGateway ist ein Webserver, der Anfragen sendet und Antworten über ein http-Protokoll empfängt.

- **Asset Management-System (AMS)** - Bevor Sie CA APM installieren, installieren Sie das Java Development Kit (JDK) auf dem Anwendungsserver, auf dem Sie das AMS installieren werden.
- **CA Software Compliance Manager (CA SCM)** - Wenn Sie CA SCM Version 12.6 mit CA APM Version 12.8 integrieren, installieren Sie CA SCM (und kumulative Versionen), bevor Sie CA APM installieren.

Konfigurieren von Oracle

Bevor Sie mit der CA APM-Installation beginnen, führen Sie die folgenden Aufgaben so aus, dass Sie das Produkt installieren und mit Oracle verwenden können:

- [Konfigurieren Sie die sqlnet.ora-Datei](#), (siehe Seite 14) so dass Sie sich erfolgreich am Produkt anmelden können.
- Wenn die CA APM-Datenbank Oracle ist, [konfigurieren Sie den Oracle-Net-Servicenamen für CA MDB](#) (siehe Seite 14) auf jedem CA APM-Computer. Diese Aufgabe ermöglicht es dem Server, mit der Oracle-Datenbank Verbindung aufzunehmen.
- Wenn Sie CA SAM mit CA APM implementieren und die CA SAM-Datenbank Oracle ist, [konfigurieren Sie den Oracle-Net-Servicenamen für die CA SAM-Implementierung](#) (siehe Seite 16) auf dem CA APM-Installationsserver und auf dem CA APM-Webserver.
- Überprüfen Sie in Oracle, dass der Tablespacepfadordner für CA MDB Schreibberechtigungen besitzt.
- Stellen Sie sicher, dass Oracle-Client-Tools, 32-Bit-Version, auf allen Servern installiert ist, die auf die Oracle-Datenbank zugreifen.

Konfigurieren der sqlnet.ora-Datei

Bevor Sie mit der CA APM-Installation beginnen, konfigurieren Sie die sqlnet.ora-Datei, so dass Sie sich am Produkt anmelden können.

So konfigurieren Sie die sqlnet.ora-Datei:

1. Suchen Sie die sqlnet.ora-Datei in *oracle_installation_path\NETWORK\admin_directory*. Zum Beispiel C:\oracle\product\10,2,0\db_1\NETWORK\ADMIN.
2. Öffnen Sie unter Verwendung eines Texteditors die sqlnet.ora-Datei folgendermaßen.
 - Ändern Sie den Eintrag NAMES.DIRECTORY_PATH= (TNSNAMES) in NAMES.DIRECTORY_PATH= (TNSNAMES, EZCONNECT).
 - Ändern Sie den Eintrag SQLNET.AUTHENTICATION_SERVICES= (NTS) in SQLNET.AUTHENTICATION_SERVICES= (NONE).
3. Speichern Sie die Datei.
Die sqlnet.ora-Datei wird konfiguriert.

Konfigurieren des Net-Servicenamens für CA MDB

Der *Net Service-Name* ist ein einfacher Name für den Oracle-Datenbankdienst, der zur Datenbank-Netzwerkadresse und zum Datenbankdienstnamen zugeordnet wird. Dieser Service ermöglicht es dem Client-Server, mit der Oracle-Datenbank Verbindung aufzunehmen.

Bevor Sie mit der CA APM-Installation beginnen, konfigurieren Sie den Net Service-Namen von Oracle auf jedem CA APM-Server, auf dem eine Komponente einschließlich CCC (Central Configuration Controller), Webserver und Anwendungsserver installiert werden. Berücksichtigen Sie die folgende Informationen bei der Konfiguration des Oracle-Net Service-Namens:

- Alle CA APM-Server müssen den gleichen Net Service-Namen aufweisen, den Sie für die Datenbankkomponente während der CA APM-Installation angeben.
- Der Net Service-Name des CA Business Intelligence-Servers ist unabhängig von CA APM und kann der gleiche oder ein anderer als der CA APM-Net Service-Name sein.

Hinweis: Auf allen Servern, auf denen die CA APM-Komponenten installiert werden sollen, müssen Oracle-Client-Tools installiert sein.

So konfigurieren Sie den Net Service-Namen:

1. Erfragen Sie die folgende Informationen bei Ihrem Oracle-Datenbankadministrator:

- Den *Oracle-Datenbankdienstnamen*, der die logische Darstellung der Oracle-Datenbank ist. Der Dienstname ist normalerweise der globale Datenbankname oder die Datenbankserver-SID.
- Der *Hostname* des Oracle-Datenbankservers, auf dem sich CA MDB für CA APM befindet.
- Die *TCP/IP-Adresse* des Oracle-Datenbankservers, auf dem sich CA MDB für CA APM befindet. Wenn Sie Zugriff auf Oracle haben, können Sie sich beim Oracle-Server anmelden und den Ipconfig-Befehl verwenden, um die TCP/IP-Adresse zu erhalten.

Hinweis: Um zu ermitteln, ob der Hostname oder die TCP/IP-Adresse auf dem Oracle-Datenbankserver aufgelöst wird, verwenden Sie den Ping-Befehl auf dem Datenbankserver. Wenn CA APM nach Namen aufgelöst werden kann, verwenden Sie den Hostnamen des Servers. Wenn eine Auflösung nach Namen nicht möglich ist, geben Sie die TCP/IP-Adresse ein, um den Net Service-Namen in den folgenden Schritten zu konfigurieren.

- Die *Portnummer* des Oracle-Datenbankservers, auf dem sich CA MDB für CA APM befindet. Der Standardwert beträgt 1521.
- Der *Anwendername* und das *Kennwort* für ein zulässiges Oracle-DBMS-Anwenderkonto.

2. Klicken Sie auf "Start", "Programme", *Oracle*, "Konfiguration und Migrations-Tools", "Netzwerkkonfigurationsassistent".

Das Oracle-Fenster "Netzwerkkonfigurationsassistent" wird geöffnet.

3. Wählen Sie "Lokaler Net Service-Name" aus.

4. Wählen Sie "Hinzufügen" aus.

5. Geben Sie den Oracle-Service-Namen ein.

6. Wählen Sie "TCP" aus.

7. Geben Sie den Hostnamen oder die TCP/IP-Adresse des CA APM-Datenbankservers ein, auf dem sich die Oracle-CA MDB befindet.

8. Wählen Sie "Standardportnummer 1521 verwenden", oder geben Sie die Oracle-Datenbankserver-Portnummer ein.

Der Netzwerkkonfigurationsassistent fordert Sie dazu auf, zu überprüfen, ob Sie mit der Oracle-Datenbank eine Verbindung herstellen können.

9. Wählen Sie "Ja" aus, und führen Sie einen Test durch.

Der Netzwerkkonfigurationsassistent testet die Verbindung mit der Oracle-Datenbank vom CA APM-Server, wobei er die von Ihnen angegebenen Verbindungsinformationen verwendet. Der Test schlägt fehl, weil ein zulässiger Oracle-Datenbankmanagement-Systemanwendername und ein Kennwort benötigt werden.

10. Klicken Sie auf "Anwendernamen ändern".

11. Geben Sie den Oracle-Systemanwendernamen und das Kennwort ein, das Ihr Oracle-Datenbank-Administrator angegeben hat.

Der Netzwerkkonfigurationsassistent testet die Verbindung mit der Oracle-Datenbank vom CA APM-Server. Der Test ist erfolgreich.

Hinweis: Wenn der Test fehlschlägt, überprüfen Sie, ob das Oracle-DBMS betriebsbereit ist und die Verbindungsinformationen korrekt sind.

12. Geben Sie den Net Service-Namen für die Oracle-Datenbank ein. Wir empfehlen, *Service Name_Hostname* für den Net Service-Namen zu verwenden.

Der Netzwerkkonfigurationsassistent fordert Sie dazu auf, einen weiteren Net Service-Namen zu konfigurieren.

13. Wählen Sie "Nein" aus.

Der Net Service-Name wird in der tnsnames.ora-Datei auf dem lokalen CA APM-Server gespeichert.

Hinweis: Nachdem Sie CA APM installiert haben, benötigen Sie den Oracle-Systemanwendernamen und das Kennwort nicht, das Sie zum Testen der Verbindung mit dem Datenbankserver verwendet haben. Die Datenbank-Anmeldeinformationen (mdbadmin) werden der CA APM-Installation während der Oracle-Installation zur Verfügung gestellt.

Konfigurieren des Net-Servicenamens für CA SAM-Implementierung

Der *Net Service-Name* ist ein einfacher Name für den Oracle-Datenbankdienst, der zur Datenbank-Netzwerkadresse und zum Datenbankdienstnamen zugeordnet wird. Dieser Service ermöglicht es dem Client-Server, mit der Oracle-Datenbank Verbindung aufzunehmen.

Bevor Sie mit der CA APM-Installation beginnen, konfigurieren Sie den Oracle-Net-Servicenamen auf dem Server der zentralen Konfigurationssteuerung (CCC) von CA APM und auf den Webservern. Der Net-Servicename des CA SAM-Servers ist unabhängig von CA APM und kann der gleiche oder ein anderer als der CA APM-Net-Servicename sein.

Hinweis: Wir empfehlen verschiedene Oracle-Instanzen für CA APM und CA SAM aus Leistungs- und Skalierbarkeitsgründen.

Hinweis: Auf allen Servern, auf denen die Net Service-Namen konfiguriert werden sollen, müssen Oracle-Client-Tools installiert sein.

Gehen Sie wie folgt vor:

1. Erfragen Sie die folgende Informationen bei Ihrem Oracle-Datenbankadministrator:

- Den *Oracle-Datenbankdienstnamen*, der die logische Darstellung der Oracle-Datenbank ist. Der Dienstname ist normalerweise der globale Datenbankname oder die Datenbankserver-SID.
- Der *Hostname* des Oracle-Datenbankservers, auf dem sich die Datenbank für CA SAM befindet.
- Die *TCP/IP-Adresse* des Oracle-Datenbankservers, auf dem sich die Datenbank für CA SAM befindet. Wenn Sie Zugriff auf Oracle haben, können Sie sich beim Oracle-Server anmelden und den Ipconfig-Befehl verwenden, um die TCP/IP-Adresse zu erhalten.

Hinweis: Um zu ermitteln, ob der Hostname oder die TCP/IP-Adresse auf dem Oracle-Datenbankserver aufgelöst wird, verwenden Sie den Ping-Befehl auf dem Datenbankserver. Wenn CA SAM nach Namen aufgelöst werden kann, verwenden Sie den Hostnamen des Servers. Wenn eine Auflösung nach Namen nicht möglich ist, geben Sie die TCP/IP-Adresse ein, um den Net Service-Namen in den folgenden Schritten zu konfigurieren.

- Die *Portnummer* des Oracle-Datenbankservers, auf dem sich die Datenbank für CA SAM befindet. Der Standardwert beträgt 1521.
- Der *Anwendername* und das *Kennwort* für ein zulässiges Oracle-DBMS-Anwenderkonto.

2. Klicken Sie auf "Start", "Programme", *Oracle*, "Konfiguration und Migrations-Tools", "Netzwerkkonfigurationsassistent".

Das Oracle-Fenster "Netzwerkkonfigurationsassistent" wird geöffnet.

3. Wählen Sie "Lokaler Net Service-Name" aus.

4. Wählen Sie "Hinzufügen" aus.

5. Geben Sie den Oracle-Service-Namen ein.

6. Wählen Sie "TCP" aus.

7. Geben Sie den Hostnamen oder die TCP/IP-Adresse des CA SAM-Datenbankservers ein, auf dem sich die Oracle-Datenbank befindet.

8. Wählen Sie "Standardportnummer 1521 verwenden", oder geben Sie die Oracle-Datenbankserver-Portnummer ein.

Der Netzwerkkonfigurationsassistent fordert Sie dazu auf, zu überprüfen, ob Sie mit der Oracle-Datenbank eine Verbindung herstellen können.

9. Wählen Sie "Ja" aus, und führen Sie einen Test durch.

Der Netzwerkkonfigurationsassistent testet die Verbindung mit der Oracle-Datenbank vom CA APM-Server, wobei er die von Ihnen angegebenen Verbindungsinformationen verwendet. Der Test schlägt fehl, weil ein zulässiger Oracle-Datenbankmanagement-Systemanwendername und ein Kennwort benötigt werden.

10. Klicken Sie auf "Anwendernamen ändern".

11. Geben Sie den Oracle-Systemanwendernamen und das Kennwort ein, das Ihr Oracle-Datenbank-Administrator angegeben hat.

Der Netzwerkkonfigurationsassistent testet die Verbindung mit der Oracle-Datenbank vom CA APM-Server. Der Test ist erfolgreich.

Hinweis: Wenn der Test fehlschlägt, überprüfen Sie, ob das Oracle-DBMS betriebsbereit ist und die Verbindungsinformationen korrekt sind.

12. Geben Sie den Net Service-Namen für die Oracle-Datenbank ein. Wir empfehlen, *Service Name_Hostname* für den Net Service-Namen zu verwenden.

Der Netzwerkkonfigurationsassistent fordert Sie dazu auf, einen weiteren Net Service-Namen zu konfigurieren.

13. Wählen Sie "Nein" aus.

Der Net Service-Name wird in der tnsnames.ora-Datei auf dem lokalen CA APM-Server gespeichert.

Konfigurieren von SQL Server

Bevor Sie mit der CA APM-Installation beginnen, konfigurieren Sie SQL Server so, dass Sie das Produkt mit SQL Server installieren und verwenden können.

So konfigurieren Sie SQL Server:

1. Wählen Sie während der SQL Server-Installation die folgenden Einstellungen aus:
 - SQL Server und Windows-Authentifizierungsmodus, was einer Authentifizierung im gemischten Modus entspricht. Wenn SQL Server bereits installiert ist, ändern Sie den Modus, indem Sie die Serversicherheitseinstellungen mit SQL Server Management Studio ändern.

- SQL Server-Sortierreihenfolge:
 - Wörterbuch-Reihenfolge
 - Groß-/Kleinschreibung nicht beachten
 - 1252 Zeichensatz
- 2. Installieren Sie SQL Server-Client-Tools auf allen Servern, auf denen die CA APM-Komponenten installiert werden sollen.
- 3. Während der CA APM-Installation muss der Anwendername, den Sie für die Verbindung mit dem Datenbankserver angeben, Systemadministrator-Rollenberechtigungen haben, die in SQL Server zugewiesen werden.

Überprüfen der Installation der Internetinformationsdienste

Bevor Sie mit der CA APM-Installation beginnen, überprüfen Sie, ob die Internetinformationsdienste (IIS) auf allen Anwendungs- und Webservern installiert sind. Wenn sich der Dienst nicht auf einem Server befindet, fügen Sie den Dienst hinzu, bevor Sie mit der Installation beginnen.

So überprüfen Sie die Installation der Internetinformationsdienste:

1. Melden Sie sich für jede Anwendung und jeden Webserver am Server an.
2. Öffnen Sie die Systemsteuerung (Verwaltung, Dienste).
3. Stellen Sie sicher, dass sich der IIS-Admin-Dienst auf dem Server befindet.

Entfernen von CA iTechnology iGateway

Bevor Sie CA EEM auf 64-Bit-Computern installieren, stellen Sie sicher, dass CA Technologies iTechnology iGateway (32-Bit und 64-Bit) nicht auf dem Computer installiert ist, auf dem Sie CA EEM installieren. Dieser Verifizierungs-Task bezieht sich auf alle Installationsmodi (Standard, Anwenderdefiniert und Demonstration). Wenn CA Technologies iTechnology iGateway bereits installiert ist, entfernen Sie die Komponente, bevor Sie mit der Installation von CA EEM beginnen. CA Technologies iTechnology iGateway (32-Bit) wird installiert, wenn Sie die Installation von CA EEM erfolgreich fertigstellen.

Hinweis: Verschiedene CA Technologies-Produkte oder -Komponenten installieren die 64-Bit-Version von CA Technologies iTechnology iGateway, einschließlich der 64-Bit-Version des CA Technologies eTrustITM-Agenten.

So entfernen Sie CA Technologies iTechnology iGateway vor der 64-Bit-Installation

1. Entfernen Sie CA Technologies iTechnology iGateway auf dem Computer, auf dem Sie CA EEM installieren.

Hinweis: Um CA Technologies iTechnology iGateway erfolgreich zu deinstallieren, sollten Sie zuerst alle Produkte deinstallieren, die von CA Technologies iTechnology iGateway abhängig sind.

- a. Öffnen Sie die Systemsteuerung (klicken Sie zum Beispiel auf "Start", "Einstellungen", "Systemsteuerung").
 - b. Doppelklicken Sie auf "Programme hinzufügen oder entfernen".
Das Dialogfeld "Programme hinzufügen oder entfernen" wird angezeigt.
 - c. Wählen Sie CA Technologies iTechnology iGateway aus, und klicken Sie auf "Entfernen".
2. Entfernen Sie in folgender Lokation den Registrierungsschlüssel-Ordner von iGateway und iTechnology:

HKEY_LocalMachine\SOFTWARE\ComputerAssociates\

3. Löschen Sie die Umgebungsvariable "IGW_LOC".
 - a. Klicken Sie im Startmenü mit der rechten Maustaste auf "Arbeitsplatz", und wählen Sie "Eigenschaften" aus.
 - b. Klicken Sie auf die Registerkarte "Erweitert".
 - c. Klicken Sie auf "Umgebungsvariablen".
 - d. Wählen Sie in der Liste der Systemvariablen "IGW_LOC" aus, klicken Sie auf "Löschen" und anschließend auf "OK".
4. Starten Sie den Computer neu.
5. Installieren Sie CA APM.
6. Wenn die Installation von CA APM abgeschlossen ist, installieren Sie die deinstallierten Komponenten auf dem Computer, auf dem CA EEM installiert ist, erneut.

Hinweis: Wir empfehlen die CA APM-Komponenten nicht zu installieren, mit Ausnahme der CA MDB auf einem 64-Bit-Computer, der einen 64-Bit-Oracle-Datenbankserver hostet.

Installieren des Java Development Kit (JDK)

Bevor Sie mit der Installation von CA APM beginnen, installieren Sie zunächst das Java Development Kit (JDK) 1.6.43 (32-bit) auf dem Anwendungsserver, auf dem Sie das AMS installieren werden. Die Installation von CA APM installiert automatisch das Asset Management-System (AMS) auf dem Anwendungsserver.

Gehen Sie wie folgt vor:

1. Melden Sie sich beim Anwendungsserver an.
2. Laden Sie JDK 1.6.43 (32-bit) von der Oracle-Website (<http://www.oracle.com>) herunter und installieren Sie es.
3. Legen Sie die Umgebungsvariable "JAVA_HOME" fest, um sich auf das Installationsverzeichnis "JDK 1.6.43" (32-bit) zu beziehen.
4. Legen Sie die Umgebungsvariable "JRE_HOME" fest, um sich auf das Unterverzeichnis des Installationsverzeichnisses "JDK 1.6.43" (32-bit) zu beziehen.
5. Aktualisieren Sie die Umgebungsvariable des Pfads, um sich auf das Verzeichnis "\bin" des Installationsverzeichnisses "JDK 1.6.43" (32-bit) zu beziehen.

Installationstypen

Die CA APM-Installation unterstützt die folgenden Optionen:

- [Standard](#) (siehe Seite 22) Wir empfehlen diese Option für die meisten Unternehmen.
- [Demo-Installation](#) (siehe Seite 24)
- [Anwenderdefiniert](#) (siehe Seite 24)

Für alle Optionen wird eine einzelne Installation für die folgenden Produktkomponenten mitgeliefert:

- CA MDB
- Webserver
- Anwendungsserver
- Hardware-Abgleichs-Engine
- Export-Service
- Data Importer-Engine-Dienst
- LDAP Data Import and Sync Service
- Importtreiber

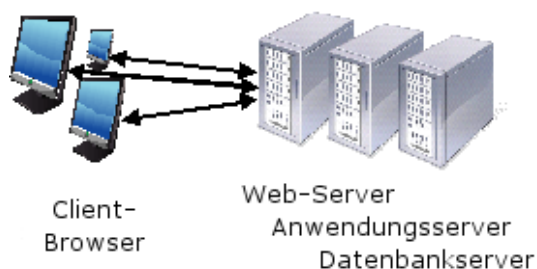
- Storage Manager-Service
- Common Administration for Service Management (CASM)
- Migration Toolkit
- Event-Service
- Registrierungsdienst
- Asset Management-System (AMS)
- WCF-Service
- Software Asset Management

Standardinstallation

Wir empfehlen, dass Sie die Standardinstallation für CA APM verwenden, das eine dreistufige Architektur verwendet. Die Standardinstallationsoption strukturiert Ihre Umgebung so, dass sie mit Ihrem Unternehmen wachsen kann. Wie in der folgenden Abbildung dargestellt, schließt die Standardinstallation Client-Browser ein und benötigt einen separaten physischen oder virtuellen Server für jeden der Hauptdienste: Webserver, Anwendungsserver und Datenbankserver.

Hinweis: Für die standardmäßige Installation verwendet das Produkt (falls CA EEM bereits auf dem Server installiert und konfiguriert ist, den Sie als Anwendungsserver während der CA APM-Installation angegeben haben) Ihr vorhandenes CA EEM für die Authentifizierung.

Wichtig! Das Produkt verwendet zeitgebundene Prozesse. Überprüfen Sie, ob alle Server auf das richtige Datum und die richtige Uhrzeit für die jeweilige Zeitzone eingestellt sind.



Konfiguration der Standardinstallationskomponenten

Die Standardinstallation für CA APM installiert das Produkt und die zugeordneten Komponenten. Wir empfehlen diesen Installationstyp für die meisten Unternehmen. Sie konfigurieren die folgenden Server für die Standardinstallation:

Datenbankserver

Auf diesem Server befindet sich die CA MDB.

Webserver

Auf diesem Server befinden sich die folgenden Komponenten:

- Webkomponente
- CA Business Intelligence. Diese Komponente muss bereits installiert sein. Das Produkt installiert CA Business Intelligence nicht.

Anwendungsserver

Auf diesem Server befinden sich die folgenden Komponenten:

- Hardware-Abgleichs-Engine
- CA EEM. Diese Komponente muss bereits installiert sein. Das Produkt installiert CA EEM nicht.
- Export-Service
- Storage Manager-Service
- LDAP Data Import and Sync Service
- Data Importer-Engine-Dienst
- Gemeinsame Verwaltung des Service Management (CASM). Diese Komponente wird während der Standardinstallation automatisch ohne Anwendereingabe installiert.
- Common Registration API (CORA). Diese Komponente wird automatisch ohne Anwendereingabe installiert.
- Event-Service. Das Produkt installiert diese Komponente mit Anwendereingabe während der Standardinstallation.
- Asset Management-System (AMS). Diese Komponente bietet eine Schnittstelle zum Anzeigen von erkannten und verwalteten Asset-Daten. Das Produkt installiert diese Komponente, die während der standardmäßigen Installation für Apache Tomcat Server und das Java Development Kit (JDK) ohne Anwendereingabe erforderlich ist.
- WCF-Service. Diese Komponente installiert die Funktion der Webdienste.

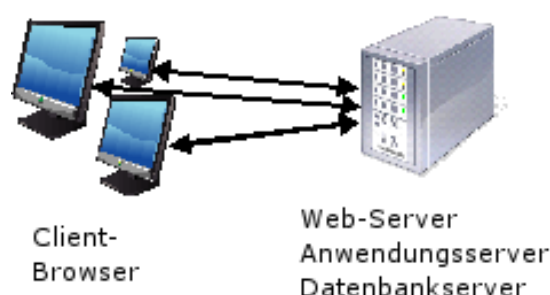
Weitere Informationen:

[CA Business Intelligence-Integration](#) (siehe Seite 133)

Demo-Installation

Die Demo-Installation für CA APM ist zum Kennenlernen und zur Demonstration und nicht für Produktionsumgebungen vorgesehen. Die Demo-Installationsoption verwendet einen einstufigen Architekturansatz. Wie die Demo-Konfiguration in der folgenden Abbildung zeigt, schließt die Demokonfiguration Client-Browser und einen Server ein, auf dem alle drei Hauptdienste (Webserver, Anwendungsserver und Datenbankserver) installiert sind.

Wichtig! Das Produkt verwendet zeitgebundene Prozesse. Überprüfen Sie, ob alle Server auf das richtige Datum und die richtige Uhrzeit für die jeweilige Zeitzone eingestellt sind.



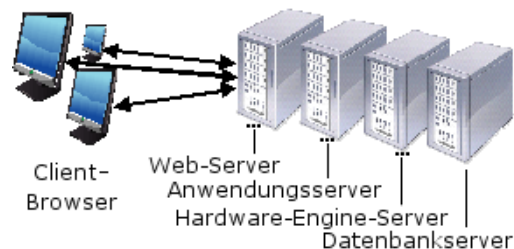
Anwenderdefinierte Installation

Die benutzerdefinierte Installation für CA APM verwendet eine mehrstufige Architektur mit integrierter Skalierbarkeit, mit der Sie die folgenden Aufgaben durchführen können:

- Hinzufügen von mehreren Web- und Anwendungsservern in [Web-Farmen](#) (siehe Seite 26).
- Hinzufügen von Hardware-Abgleichs-Engines.
- Festlegen der Server, auf denen sich die meisten Komponenten befinden.
- Verwenden Sie CA EEM oder CA Business Intelligence auf einem separaten Server.

Bei der benutzerdefinierten Installation kann sich die Hardware-Abgleichs-Engine auf einem separaten Server befinden. Folgende Beispielinstallation verwendet einen separaten physischen oder virtuellen Server für den Webserver, Anwendungsserver, Datenbankserver und die Hardware-Engine und unterstützt Web-Farmen. Die Benutzer greifen auf das Produkt zu, indem Sie ihre Client-Browser auf die Webserver-URL richten.

Wichtig! Das Produkt verwendet zeitgebundene Prozesse. Überprüfen Sie, ob alle Server auf das richtige Datum und die richtige Uhrzeit für die jeweilige Zeitzone eingestellt sind.



Anwenderdefinierte Konfiguration von Installationskomponenten

Die benutzerdefinierte Installation für CA APM installiert das Produkt und die zugeordneten Komponenten. Dieser Installationstyp verwendet eine mehrstufige Architektur und lässt Sie die Server, auf denen sich die meisten Komponenten befinden, wie folgt festlegen:

- Ein Datenbankserver. Auf diesem Server befindet sich nur die CA MDB.
- Einer oder mehrere Webserver
- Einer oder mehrere Anwendungsserver. Auf diesem Server befinden sich die folgenden Komponenten:
 - Export-Service auf einem Server
 - Storage Manager-Service auf einem Server
- Eine oder mehrere Hardware-Abgleichs-Engines
- Ein oder mehrere durch Data Importer installierte Server
- Ein "LDAP-Datenimport und Synchronisation" auf einem der Data Importer-Server
- Ein Data Importer-Engine-Server
- Ein Import-Treiber-Service auf einem der Anwendungsserver
- Ein Registrierungsservice auf einem der Anwendungsserver
- Eine Anwendung des Migrationshilfsprogramms auf dem CCC-Server

- CA Business Intelligence. Diese Komponente befindet sich auf einem Server. CA Business Intelligence muss schon installiert sein. Das Produkt installiert diese Komponente nicht.
- Gemeinsame Verwaltung des Service Management (CASM). Diese Komponente befindet sich auf einem Server. CA APM installiert diese Komponente mit Anwendereingabe während der anwenderdefinierten Installation.
- Event-Service. Diese Komponente befindet sich auf einem Server. Das Produkt installiert diese Komponente mit Anwendereingabe während der anwenderdefinierten Installation.
- Asset Management-System (AMS). Diese Komponente befindet sich auf einem Server. Diese Komponente bietet eine Schnittstelle zum Anzeigen von erkannten und verwalteten Asset-Daten. Das Produkt installiert diese Komponente, die während der anwenderdefinierten Installation für Apache Tomcat Server und das Java Development Kit (JDK) ohne Anwendereingabe erforderlich ist.
- WCF-Service (Windows Communications Foundation). Diese Komponente befindet sich auf einem Server. Das Produkt installiert diese Komponente mit Anwendereingabe während der anwenderdefinierten Installation. Geben Sie den Servernamen an, und ändern Sie optional das WCF-Service-Protokoll für diese Komponente.

Weitere Informationen:

[CA Business Intelligence-Integration](#) (siehe Seite 133)

Web-Farmen

Eine *Web-Farm* ist eine Gruppe oder ein Cluster von Servern, die wie ein allein stehender Webserver fungieren. CA APM unterstützt mehrere Server für die Anwendungs- und Webserverkomponenten. Die Verwendung einer Web-Farm bietet die folgenden Vorteile:

- Leistungssteigerung. Mehr als ein Server ist verfügbar, um Netzwerkanfragen zu verarbeiten.
- Skalierbarkeit. Mehrere Server können hinzugefügt werden, um zusätzliche Anwender und Anfragen zu verarbeiten.

- **Sicherung.** Da jeder Server die Ressourcen der anderen dupliziert, verarbeitet ein Sicherungsserver Netzwerkanfragen, wenn ein Server fehlschlägt oder herunterfährt.

Sie können CA APM in einer Web-Farm verwenden. Allerdings müssen Sie die Software, die die Web-Farm steuert, installieren und konfigurieren, weil CA Technologies diese Software nicht zur Verfügung stellt. Bei der benutzerdefinierten Installation werden die zahlreichen Web- und Anwendungsserver in der Konfiguration eingerichtet, wodurch Sie den ausgewählten Netzwerklastenausgleich konfigurieren können.

Konfigurieren der Server in einer Web-Farm

Sie können eine Web-Farm für die Anwendungsserverkomponente, für die Webserverkomponente und für die WCF-Servicekomponente von CA APM einrichten. Sie konfigurieren jeden Server in der Web-Farm. Um eine Web-Farm zu konfigurieren, führen Sie die folgenden Schritte aus:

1. Konfigurieren Sie eine virtuelle IP-Adresse für die Server. Wenn Sie die Webserver, Anwendungsserver und WCF-Server skalieren möchten, benötigen Sie drei virtuelle IP-Adressen. Verwenden Sie eine Adresse für die Webserverfarm, eine andere Adresse für die Anwendungsserverfarm und eine weitere Adresse für die WCF-Serverfarm.

Hinweis: Weitere Informationen über die Konfiguration einer virtuellen IP-Adresse finden Sie in der *Windows Server 2008 Hilfe*.

Bei der Konfiguration des Netzwerk-Lastenausgleichs für die Anwendungsserver, Webserver und WCF-Server wählen Sie die folgenden Optionen aus:

- (Anwendungsserver) Wählen Sie "Keine" für die Serveraffinität aus.
 - (Webserver) Wählen Sie "Einzeln" oder "Klasse C" für die Serveraffinität aus.
 - (WCF-Server) Wählen Sie "Keine" für die Serveraffinität aus.
2. Verwenden Sie die benutzerdefinierte Installation, um mehrere Server in der Anwendungsserver-Web-Farm zu installieren.
 3. Verwenden Sie die benutzerdefinierte Installation, um mehrere Server in der Web-Farm des WCF-Servers zu installieren.
 4. Verwenden Sie die benutzerdefinierte Installation, um mehrere Server in der Webserver-Web-Farm zu installieren.

Hinweis: Stellen Sie während der Installation sicher, dass sich jeder Webserver auf die virtuelle IP-Adresse des Anwendungsservers und auf die virtuelle IP-Adresse des WCF-Servers bezieht.

5. Geben Sie während der Konfiguration von weiteren Komponenten, wie Data Importer-Engine-Dienst und Hardware-Abstimmungs-Engine, die virtuelle IP-Adresse des Anwendungsservers ein.

Kapitel 3: Aktualisieren

Dieses Kapitel enthält folgende Themen:

[So führen Sie ein Upgrade von Version 11.3.4 durch](#) (siehe Seite 29)

[So führen Sie ein Upgrade von Version 12.6 aus](#) (siehe Seite 31)

[So führen Sie ein Upgrade von Version 12.6.05 aus](#) (siehe Seite 34)

So führen Sie ein Upgrade von Version 11.3.4 durch

Wenn Sie ein Upgrade durchführen, aktualisieren Sie die Anwendung und Datenbank auf eine neuere Version. Um ein Upgrade von Version 11.3.4 auf Version 12.8 durchzuführen, gehen Sie folgendermaßen vor:

1. [Installieren Sie den kumulativen Patch 14 oder höher für die Version 11.3.4](#) (siehe Seite 30).
2. [Halten Sie die Dienste an](#) (siehe Seite 30).
3. [Deinstallieren Sie Version 11.3.4](#) (siehe Seite 30).
4. [Installieren Sie Version 12.8](#) (siehe Seite 31).

Hinweis: Das Durchführen eines Upgrades Ihrer Daten oder die Migration Ihrer Daten sind separate Vorgänge:

- **Upgrade.** Aktualisiert die Anwendung und die Datenbankstrukturen auf eine neuere Version.
- **Migrieren.** Transformiert oder verschiebt die Daten aus früheren Datenbankstrukturen in neue Datenbankstrukturen, die während des Upgrades erstellt wurden.

Am Ende der Version 12.8-Installation wird ein Upgrade der CA MDB-Strukturen durchgeführt, und Sie werden aufgefordert, Ihre Daten in die neuen Datenbankstrukturen zu migrieren. Weitere Informationen zur Migration Ihrer Daten von Version 11.3.4 finden Sie unter [So migrieren Sie CA APM-Daten von Version 11.3.4 auf Version 12.8](#) (siehe Seite 63).

Installieren Sie den kumulativen Patch 14 oder höher für die Version 11.3.4

Stellen Sie sicher, dass Ihre aktuelle Patch-Ebene der Version 11.3.4 der kumulative Patch 14 oder höher ist. Wenn Ihre aktuelle Patch-Ebene unbekannt ist oder nicht dem kumulativen Patch 14 oder höher entspricht, laden Sie den aktuellsten kumulativen Patch von CA APM Version 11.3.4 von der CA Support-Website herunter.

Wichtig! Der kumulative Patch 14 oder höher ist erforderlich, bevor Sie die Version 11.3.4 oder höher deinstallieren. Dieser Patch bringt die CA MDB auf die richtige Ebene, bevor Sie Version 12.8 installieren.

Anhalten der Dienste

Halten Sie die CA APM-Dienste an, bevor Sie mit der Installation beginnen, sodass erforderliche Dateien während der Installation ersetzt und aktualisiert werden können.

Hinweis: Die Dienste der Version 11.3.4 verwenden das Präfix "UAPM" in den Servicenamen.

Gehen Sie wie folgt vor:

1. Öffnen Sie im Startmenü auf dem CA APM-Anwendungsserver die Systemsteuerung, Verwaltung, Dienste.
2. Suchen Sie die CA APM-Dienste und die geplanten Aufgaben, klicken Sie mit der rechten Maustaste auf jeden Dienst, und wählen Sie "Beenden" aus.

Hinweis: Weitere Informationen zu bestimmten CA APM-Diensten und geplanten Aufgaben finden Sie unter den Voraussetzungen im Abschnitt [So migrieren Sie CA APM-Daten von Version 11.3.4 auf Version 12.8](#) (siehe Seite 63).

Der Dienst wird beendet.

Deinstallieren der Version 11.3.4

Deinstallieren Sie alle Komponenten der Version 11.3.4, mit Ausnahme der CA MDB. Die CA MDB kann nicht deinstalliert werden. Wenn Ihre Version 11.3.4 auf mehreren Servern installiert ist, deinstallieren Sie die Version auf allen Servern.

Gehen Sie wie folgt vor:

1. Navigieren Sie im Startmenü auf einem Server der Version 11.3.4 zu "Systemsteuerung", "Programme hinzufügen oder entfernen".
2. Suchen Sie "CA Unicenter Asset Portfolio Management", und wählen Sie den Eintrag aus.

3. Klicken Sie auf "Ändern/Entfernen", und klicken Sie auf "OK", wenn Sie eine Bestätigungsmeldung erhalten.

Hinweis: Starten Sie die Server der Version 11.3.4 neu, wenn Sie dazu aufgefordert werden.

Die Komponenten der Version 11.3.4 werden deinstalliert.

Installieren von Version 12.8

Installieren Sie Version 12.8 mithilfe der Anweisungen unter [Installieren](#) (siehe Seite 37).

Am Ende der Installation wird ein Upgrade der CA MDB-Strukturen durchgeführt, und Sie werden aufgefordert, Ihre Daten in die neuen Datenbankstrukturen zu migrieren. Weitere Informationen zur Migration Ihrer Daten von Version 11.3.4 finden Sie unter [So migrieren Sie CA APM-Daten von Version 11.3.4 auf Version 12.8](#) (siehe Seite 63).

So führen Sie ein Upgrade von Version 12.6 aus

Um ein Upgrade von Version 12.6 auf Version 12.8 durchzuführen, gehen Sie folgendermaßen vor:

1. [Halten Sie die Dienste an](#) (siehe Seite 31).
2. [Deinstallieren Sie Version 12.6](#) (siehe Seite 32).
3. [Installieren Sie Version 12.8](#) (siehe Seite 34).

Anhalten der Dienste

Halten Sie die CA APM-Dienste an, bevor Sie mit der Installation beginnen, sodass erforderliche Dateien während der Installation ersetzt und aktualisiert werden können.

Wenn Sie CA APM Version 12.8 auf CA APM-GA-Version 12.6 installieren (und nicht auf einer kumulativen Version 12.6), löschen Sie auch LDAP-Datenimport und Synchronisation. Nachdem Sie die Installation fertiggestellt haben, installieren Sie LDAP-Datenimport und Synchronisation neu, und Sie starten die Dienste neu, die Sie beendet haben.

Gehen Sie wie folgt vor:

1. Öffnen Sie im Startmenü auf dem CA APM-Anwendungsserver die Systemsteuerung, Verwaltung, Dienste.
2. Suchen Sie die Einträge für jeden der folgenden CA APM-Dienste, und führen Sie folgenden Schritt aus:
 - CA Asset Portfolio Management - Event-Service
 - CA Asset Portfolio Management - Export-Service
 - CA Asset Portfolio Management - HW-Abgleichs-Engine
 - CA Asset Portfolio Management - LDAP Import Service
3. Klicken Sie mit der rechten Maustaste auf jeden Dienst, und wählen Sie "Beenden" aus.

Hinweis: Führen Sie diesen Schritt für die Dienste aus, die derzeit ausgeführt werden und in Ihrer Installation verfügbar sind (z. B. ist der Event-Service optional). Der Dienst wird beendet.

Deinstallieren der Version 12.6

Um das Produkt zu deinstallieren, führen Sie die folgenden Schritte aus. Führen Sie für die standardmäßige und benutzerdefinierte Installation diese Schritte auf jedem Computer (außer dem Datenbankserver) aus, auf dem CA APM installiert ist.

Gehen Sie wie folgt vor:

1. Überprüfen Sie, ob sich alle Anwender vom Produkt abgemeldet haben.

Hinweis: Anwender, die sich vor Beginn der Deinstallation nicht vom Produkt abgemeldet haben, erhalten eine Fehlermeldung (z. B. eine Fehlermeldung, die angibt, dass die Seite nicht angezeigt werden kann), wenn sie versuchen, eine Aufgabe abzuschließen.
2. Melden Sie sich bei dem Computer an, auf dem CA APM installiert ist.
3. Wechseln Sie zum folgenden Ordner:
C:\Programme\CA\ITAM\Uninstall
4. Starten Sie die Deinstallation, indem Sie zweimal auf die Datei "APM_UNINSTALL.bat" klicken.

5. Folgen Sie im Deinstallationsvorgang den Anweisungen auf dem Bildschirm.

Die Deinstallation wird ausgeführt und entfernt alle installierten CA APM-Komponenten, außer CA MDB, der Common Registration API (CORA), dem Asset Management-System (AMS) und CA Business Intelligence.

6. Navigieren Sie zum folgenden Ordner auf dem Version 12.8-Installationsdatenträger:

12.8 DVD\Uninstall\Uninstall\

7. Kopieren Sie die Datei "LDAPUninstallPatch.bat", und fügen Sie sie in den folgenden Ordner ein:

[ITAM-Stammverzeichnis]\ITAM\Uninstall\uninstall

8. Klicken Sie mit der rechten Maustaste auf die Batch-Datei, und wählen Sie "Als Administrator ausführen" aus.

9. Öffnen Sie die Systemsteuerung, und stellen Sie sicher, dass der Eintrag "LDAPImportSyncServiceInstall" nicht mehr gezeigt wird.

10. Greifen Sie auf "services.msc" zu, und stellen Sie sicher, dass der Eintrag für "CA Asset Portfolio Management – LDAP-Import-Service" nicht mehr vorhanden ist.

11. Deinstallieren Sie den Utildev Web Server 2.0, der mit Version 12.6 installiert wurde.

Hinweis: Version 12.8 installiert Utildev Web Server Pro 4.0.

- a. Wählen Sie im Startmenü "Ausführen" aus, geben Sie "appwiz.cpl" in das Dialogfeld ein, und klicken Sie auf "OK".

Das Fenster "Programme und Funktionen" der Systemsteuerung wird geöffnet. Folgende Komponenten werden aufgelistet:

- UtilDev Cassini Web Server Explorer
- UtilDev Cassini Web Server for ASP.NET 2.0

- b. Klicken Sie mit der rechten Maustaste auf "UtilDev Cassini Web Server Explorer", und wählen Sie "Deinstallieren" aus.

- c. Klicken Sie mit der rechten Maustaste auf "UtilDev Cassini Web Server for ASP.NET 2.0", und wählen Sie "Deinstallieren" aus.

- d. Entfernen Sie den Ordner "Utildev" aus den folgenden Speicherorten, sofern vorhanden:

- C:\Programme\
- C:\Programme(x86)\ (für 64-Bit-Server)
- C:\ProgramData\

Installieren von Version 12.8

Installieren Sie Version 12.8 mithilfe der Anweisungen unter [Installieren](#) (siehe Seite 37).

So führen Sie ein Upgrade von Version 12.6.05 aus

Um ein Upgrade von Version 12.6.05 auf Version 12.8 durchzuführen, gehen Sie folgendermaßen vor:

1. [Halten Sie die Dienste an](#) (siehe Seite 34).
2. [Deinstallieren Sie Version 12.6.05](#) (siehe Seite 35).
3. [Installieren Sie Version 12.8](#) (siehe Seite 36).

Anhalten der Dienste

Halten Sie die CA APM-Dienste an, bevor Sie mit der Installation beginnen, sodass erforderliche Dateien während der Installation ersetzt und aktualisiert werden können.

Gehen Sie wie folgt vor:

1. Öffnen Sie im Startmenü auf dem CA APM-Anwendungsserver die Systemsteuerung, Verwaltung, Dienste.
2. Suchen Sie die Einträge für jeden der folgenden CA APM-Dienste, und führen Sie folgenden Schritt aus:
 - CA Asset Portfolio Management - Event-Service
 - CA Asset Portfolio Management - Export-Service
 - CA Asset Portfolio Management - HW-Abgleichs-Engine
 - CA Asset Portfolio Management - LDAP Import Service
3. Klicken Sie mit der rechten Maustaste auf jeden Dienst, und wählen Sie "Beenden" aus.

Hinweis: Führen Sie diesen Schritt für die Dienste aus, die derzeit ausgeführt werden und in Ihrer Installation verfügbar sind (z. B. ist der Event-Service optional).

Der Dienst wird beendet.

Deinstallieren der Version 12.6.05

Um die CA APM-Version 12.6.05 zu deinstallieren, entfernen Sie die Komponenten und Dienste, die Sie installiert haben. Deinstallieren Sie außerdem CA APM Version 12.6.

Hinweis: Um andere kumulative Versionen von Version 12.6 zu deinstallieren, wenden Sie sich an CA Support Online, oder lesen Sie die Readme-Dateien, die in den kumulativen Versionen enthalten sind.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei den Servern an, auf denen Sie CA APM Version 12.6.05 installiert haben.
2. (Windows 2008) Wählen Sie im Startmenü "Systemsteuerung", "Programme und Funktionen" aus, und klicken Sie auf "Installierte Updates anzeigen".
3. Entfernen Sie die folgenden Dienste und Komponenten, die auf den anwendbaren Servern verfügbar sind:

Hinweis: Je nach Ihrer CA APM-Installation haben Sie möglicherweise nicht alle diese Dienste und Komponenten.

- CA ITAM – Event-Service - 12.6.05
- CA ITAM – Export-Service - 12.6.05
- CA Asset Portfolio Management – Hardware-Engine – 12.6.05
- CA ITAM – ITAM Data Importer - 12.6.05
- CA IT Asset Manager – SMServer – 12.6.05
- CA ITAM – Anwendungsserver- 12.6.05
- CA ITAM – Web-Client – 12.6.05
- LDAPImportSyncServiceInstall - 12.6.05
- CA ITAM – WCF-Service – 12.6.05
- CA Asset Portfolio Management – Registrierungsservice – 12.6.945
In Windows 2008 können Sie diesen Dienst im Startmenü über "Systemsteuerung", "Programme und Funktionen" anzeigen.
- CA Asset Portfolio Management – Importtreiber – 12.6.945
In Windows 2008 können Sie diesen Dienst im Startmenü über "Systemsteuerung", "Programme und Funktionen" anzeigen.

Sie haben die Deinstallation von CA APM Version 12.6.05 abgeschlossen.

4. Führen Sie die Schritte aus, um CA APM Version 12.6 zu [deinstallieren](#) (siehe Seite 32).

Installieren von Version 12.8

Installieren Sie Version 12.8 mithilfe der Anweisungen unter [Installieren](#) (siehe Seite 37).

Kapitel 4: Wird installiert

Dieses Kapitel enthält folgende Themen:

- [Implementieren der Software](#) (siehe Seite 37)
- [Installationsphasen](#) (siehe Seite 37)
- [Aktualisieren der Apache Tomcat-Konfigurationsdatei](#) (siehe Seite 54)
- [Konfigurieren von AMS für Sichere Netzwerkkommunikation](#) (siehe Seite 55)
- [Konfigurieren des AMS für den Namen Ihres Domain Name System \(DNS\)](#) (siehe Seite 56)
- [Konfigurieren des AMS mit Teiid](#) (siehe Seite 56)
- [Konfigurieren des Export-Service für Sichere Netzwerkkommunikation](#) (siehe Seite 57)
- [Starten der Dienste](#) (siehe Seite 58)
- [Starten der Web-Schnittstelle](#) (siehe Seite 59)
- [Überprüfen der Installation](#) (siehe Seite 60)
- [Deinstallieren von CA APM](#) (siehe Seite 61)

Implementieren der Software

Der Ausgangspunkt und die Schritte, die Sie vornehmen, um CA APM zu implementieren, basieren auf mehreren Faktoren. Zu diesen Faktoren gehören Betriebssysteme, Datenbanken und die Produkte, die Sie integrieren möchten. Im Allgemeinen befolgen Sie die aufgeführten Schritte, um die Software zu implementieren

1. [Installieren Sie CA APM.](#) (siehe Seite 37)
2. [Starten Sie die Dienste](#) (siehe Seite 58).
3. [Starten Sie die Webschnittstelle.](#) (siehe Seite 59)

Installationsphasen

Die CA APM-Installation besteht aus einer Phase vor der Installation und vier Installationsphasen:

1. [Phase vor der Installation: Installieren Sie den Installations-Manager](#) (siehe Seite 38). Sie installieren die erforderlichen Installationsserververwaltungs-Komponenten und den Installations-Manager auf dem Computer, auf dem Sie die Installation ausführen möchten.
2. [Phase 1: Installieren Sie das CCC, und wählen Sie den Installationstyp aus](#) (siehe Seite 39). Sie installieren den Central Configuration Controller (CCC) und wählen den Installationstyp (Standard, Demo oder benutzerdefiniert) aus.

3. [Phase 2: Geben Sie die erforderlichen Server an](#) (siehe Seite 40). Sie geben die erforderlichen Serverinformationen für alle erforderlichen Server an. Sie geben außerdem die Administratoranmeldeinformationen für den aktuellen lokalen Server und für die zusätzlichen erforderlichen Server an, auf denen Sie die Installation ausführen.
4. [Phase 3: Konfigurieren Sie die Komponenten für alle Server, und installieren Sie das Produkt auf dem lokalen Server](#) (siehe Seite 40). Sie konfigurieren die Komponenten für alle Server und installieren das Produkt auf dem aktuellen lokalen Server, auf dem Sie die Installation ausführen.
5. [Phase 4: Stellen Sie die Installation auf den zusätzlichen erforderlichen Servern fertig](#) (siehe Seite 52) Sie überprüfen die Administrator-Anmeldeinformationen für die zusätzlichen benötigten Server und installieren das Produkt auf den zusätzlichen Servern.

Wenn Sie innerhalb einer Phase die Informationen für eine frühere Seite ändern, verlieren Sie die anderen Daten nicht, die Sie während der Phase eingegeben haben. Wenn Sie in eine frühere Phase zurückkehren möchten, klicken Sie auf "Installation zurücksetzen". Sie können dann den Installationsprozess von Phase 1 neu starten.

Phase vor der Installation: Installieren des Installations-Manager

Installieren Sie in der Phase vor der Installation die erforderlichen Installationsserververwaltungs-Komponenten und den Installations-Manager auf dem lokalen Computer, auf dem CA APM installiert werden soll.

Gehen Sie wie folgt vor:

1. Legen Sie die Installationsdatenträger in das Computerlaufwerk ein.
Wenn "AutoPlay" aktiviert ist, wird die Installation automatisch gestartet. Wenn "AutoPlay" deaktiviert ist, doppelklicken Sie im Stammverzeichnis des Installationsdatenträgers auf die Datei "setup.exe", um die Installation zu starten.
2. Klicken Sie auf "Fortfahren", wenn Windows Ihre Berechtigung zum Fortfahren anfordert. Diese Anfrage wird nur angezeigt, wenn für Ihr Betriebssystem die Anwenderkontosteuerung aktiviert ist.

Das Produkt überprüft, ob die folgenden erforderlichen Installationsserververwaltungs-Komponenten installiert sind:

- .NET Framework 4.0
- UtilDev Web Server Pro

- Web Service Enhancements 3.0

Wenn diese Komponenten nicht gefunden werden, installiert das Produkt die erforderlichen Dateien auf dem Computer, auf dem Sie CA APM installieren möchten.

Hinweis: Wenn Sie eine Aufforderung bekommen, den Computer neu zu starten, nachdem Sie die erforderlichen Komponenten installiert haben, klicken Sie auf "Ja", um neu zu starten. Fahren Sie dann mit der Installation fort, nachdem der Computer neu gestartet wurde.

3. Befolgen Sie weiter die Anweisungen auf dem Bildschirm.

Der Installations-Manager wird in dem von Ihnen angegebenen Ordner installiert, und Sie fahren mit Phase 1 fort.

Phase 1: Installieren von CCC und Auswählen des Installationstyps

Eine typische CA APM-Installation besteht aus mehreren, auf mehreren Servern installierten Komponenten. Das Produkt verwendet eine zentrale Konfigurationssteuerung (CCC), die die Zusammenarbeit dieser Komponenten aktiviert. CCC befindet sich auf einem einzelnen Server und liefert den anderen Servern die Komponenteninstallationen und ihre Konfigurationsdaten.

In Phase 1 der Installation installieren Sie den CCC und wählen den Installationstyp aus (Standard, Demo oder benutzerdefiniert).

So führen Sie Phase 1 der Installation aus:

1. Folgen Sie den Bildschirmanweisungen, um CCC zu installieren, und wählen Sie den Installationstyp aus.
2. Fahren Sie mit Schritt 2 fort.

Phase 2: Festlegen des erforderlichen Servers

In Phase 2 der CA APM-Installation geben Sie die Informationen für die erforderlichen Server an. Geben Sie für die Standardinstallation den Anwendungsserver, den Webserver und den Datenbankserver an. Geben Sie außerdem die Administratoranmeldeinformationen für den aktuellen lokalen Server (Anwendung oder Netz) und für die zusätzlichen erforderlichen Server an, auf denen Sie die Installation ausführen.

Für die Demo-Installation und die benutzerdefinierte Installation zeigt der Installations-Manager den Namen des lokalen Servers an, auf dem Sie die Installation ausführen. Der CCC wird installiert und zeigt die Administratoranmeldeinformationen an, die Sie für die Anmeldung am Server angegeben haben.

Wichtig! Geben Sie für die Standard- und die benutzerdefinierte Installation denselben ITAM-Stammpfad (zum Beispiel, C:\Programme\CA\ITAM) für die Produktkomponenten ein, die Sie in Phase 4 der Installation auf zusätzlichen erforderlichen Servern installieren.

So führen Sie Phase 2 der Installation aus:

1. Folgen Sie den Bildschirmanweisungen, um die erforderlichen Server und die Administratoranmeldeinformationen für den aktuellen lokalen Server und die zusätzlichen Server anzugeben.

Der Installations-Manager überprüft die Konnektivität für den aktuellen lokalen Server (der Server, auf dem Sie die Installation ausführen).

Hinweis: Während Phase 2 können Sie die Komponente und den Server von CA Business Intelligence für Berichterstellungsfunktionen installieren oder überspringen. Außerdem können Sie die Komponenten und Server des Event-Service und von Software Asset Management installieren oder überspringen. Wenn Ihre Implementierung die Konfiguration von Software Asset Management (CA SAM) betrifft, geben Sie die Komponenten und Server des Event-Service und von Software Asset Management an.

2. Fahren Sie mit Schritt 3 fort.

Phase 3: Konfigurieren der Komponenten und Installieren des Produkts

In Phase 3 der CA APM-Installation geben Sie die Konfiguration für alle Komponenten an und installieren das Produkt auf dem aktuellen lokalen Server, auf dem Sie die Installation ausführen. Die Komponenten, die Sie für andere Server festlegen (nicht der aktuelle lokale Server), werden während Phase 4 auf den anderen Servern installiert.

So führen Sie Phase 3 der Installation aus:

1. Folgen Sie den Bildschirmanweisungen, um die Server- und Konfigurationsinformationen für die einzelnen Komponenten anzugeben.

Hinweis: Der Installations-Manager prüft auf dem Datenbankserver und auf den CA Business Intelligence-Seiten, ob Sie alle Voraussetzungen eingegeben haben, bevor Sie mit der Installation fortfahren können.

Der Installations-Manager zeigt eine Konfigurationszusammenfassung an.

2. Wenn Sie mit den Konfigurationseinstellungen zufrieden sind, klicken Sie auf "Fertig stellen".

Der Installations-Manager fängt mit der Produktinstallation auf dem aktuellen lokalen Server an und überprüft, ob alle Komponenten alle Voraussetzungen erfüllen. Die Komponenten, die Sie für den aktuellen lokalen Server festlegen, werden installiert. Eine Konfigurationszusammenfassung wird angezeigt.

Hinweis: In dieser Phase werden nur die Komponenten, die Sie für den aktuellen lokalen Server festlegen, installiert. Die Komponenten, die Sie für andere Server festlegen, werden während Phase 4 auf den anderen Servern installiert.

3. Wenn eine oder mehrere Komponenteninstallationen fehlschlagen, sollten Sie folgende Schritte ausführen:
 - a. Klicken Sie auf "Protokoll anzeigen" und zeigen Sie die Fehlerdetails im Protokoll an.
 - b. Beheben Sie den Fehler. Um die Konfigurationsvoraussetzungen auf einer fehlgeschlagenen Komponente zu korrigieren, verwenden Sie die Navigationsschaltflächen, um zur Komponentenkonfiguration zurückzukehren.
 - c. Klicken Sie auf "Installation wiederholen".

Der Installations-Manager wiederholt nur die Komponenteninstallationen, die zuvor fehlschlagen, und zeigt die Setup-Zusammenfassung an.

4. Korrigieren Sie weiter die fehlgeschlagenen Setups und klicken Sie auf "Installation wiederholen", bis allen Voraussetzungen entsprochen wird und alle Komponenten installiert sind.

Wenn allen Voraussetzungen erfüllt und alle Komponenten installiert sind, ist die Produktinstallation auf dem aktuellen Server abgeschlossen.

Hinweis: Sie können die Komponentenkonfigurationen ändern und zusätzliche Komponenten für Ihr Unternehmen konfigurieren, nachdem Sie das Produkt installiert haben. Weitere Informationen zum Ändern der Konfiguration von Komponenten und Hinzufügen von Servern finden Sie im *Administrationshandbuch*.

Produktkomponenten

Geben Sie während Phase 3 der CA APM-Installation die Informationen über die folgenden Produktkomponenten einschließlich ihrer Serverlokationen und Konfigurationen an:

Wichtig! Die Namen aller Serveranwender erfordern die Domäne als Präfix (z. B. "CAAPM128\administrator").

- [Datenbankserver](#) (siehe Seite 43)
- [Webserver](#) (siehe Seite 43)
- [Anwendungsserver](#) (siehe Seite 44)
- [Hardware-Abgleichs-Engine](#) (siehe Seite 45)
- [CA EEM](#) (siehe Seite 45)
- [CA Business Intelligence](#) (siehe Seite 46)
- [Export-Service](#) (siehe Seite 46)
- [Data Importer-Engine-Dienst](#) (siehe Seite 46)
- [Importtreiber](#) (siehe Seite 47)
- [LDAP Data Import and Sync Service](#) (siehe Seite 47)
- [Storage Manager-Service](#) (siehe Seite 47)
- [CA APM-Registrierungsservice](#) (siehe Seite 48)
- [Common Administration for Service Management \(CASM\)](#) (siehe Seite 48)
- [Event-Service](#) (siehe Seite 48)
- [Migration Toolkit](#) (siehe Seite 50)
- [Asset Management-System \(AMS\)](#) (siehe Seite 50)
- [WCF-Service](#) (siehe Seite 51)
- [Software Asset Management](#) (siehe Seite 52)

Hinweis: Sie können die Komponentenkonfigurationen ändern und zusätzliche Komponenten für Ihr Unternehmen konfigurieren, nachdem Sie das Produkt installiert haben. Weitere Informationen zum Ändern der Konfiguration von Komponenten und Hinzufügen von Servern finden Sie im *Administrationshandbuch*.

Datenbankserver

Der Datenbankserver ist eine Produktkomponente, die das Oracle- oder SQL Server-Datenbankmanagementsystem für CA APM hostet. Die CA MDB wird auf dem Datenbankserver installiert. Der Anwendungsserver, die Hardware-Abgleichs-Engine und andere Produktkomponenten rufen Daten aus der CA MDB ab und speichern Daten darin ab.

Die folgenden Felder bedürfen einer Erklärung:

MS SQL Server-Instanz

Definiert den Namen der MS SQL Server-Instanz, die konfiguriert wird. Geben Sie den Instanznamen nur ein, wenn mehrere benannte SQL Server-Instanzen vorhanden sind. Lassen Sie das Feldformular leer, wenn es nur eine (Standard)-Instanz gibt.

Hinweis: Sie können die Komponentenkonfigurationen ändern und zusätzliche Komponenten für Ihr Unternehmen konfigurieren, nachdem Sie das Produkt installiert haben. Weitere Informationen zum Ändern der Konfiguration von Komponenten und Hinzufügen von Servern finden Sie im *Administrationshandbuch*.

Webserver

Der Webserver ist der Hauptserver, der die Webanwendung hostet und die CA APM-Benutzeroberfläche bereitstellt. Dieser Server kommuniziert mit dem Anwender und dem Anwendungsserver. Die Produkt-Webkomponenten und CA Business Intelligence (Berichterstellung) Webkomponenten sind beide installiert auf dem gleichen Server (Webserver) für eine standardmäßige Installation. Für eine anwenderspezifische Installation können Sie mehr als einen Webserver haben, und die CA Business Intelligence-Komponenten können auf einem anderen Server installiert werden.

Die folgenden Felder bedürfen einer Erklärung:

Webserver oder IP/Host des Lastenausgleichsmoduls

Die Installation von CA APM legt dieses Feld standardmäßig als Hostnamen des Webserver fest.

- In einer Umgebung mit einem einzelnen Webserver können Sie den Hostnamen oder die IP-Adresse des Webserver eingeben.
- In einer Umgebung mit mehreren Webservern können Sie entweder den Hostnamen des Webserver oder die IP-Adresse des Lastenausgleichs eingeben.

Hinweis: Der Webserver kann im Domain Name System (DNS) unter einem anderen Namen registriert werden als der registrierte Hostname des Webserver. Geben Sie in diesem Fall den anderen Namen im Feld an.

Sie können zusätzliche Webserverkomponenten konfigurieren, nachdem Sie das Produkt installiert haben.

Hinweis: Weitere Informationen zum Ändern der Konfiguration von Komponenten und Hinzufügen von Servern finden Sie im *Administrationshandbuch*.

Weitere Informationen:

[Webserver benannt mit Unterstreichungszeichen](#) (siehe Seite 172)

Anwendungsserver

Der Anwendungsserver ist der Server, der den Datenbankserver und den Webserver für CA APM miteinander verbindet. Die Geschäfts- und Datenzugriffslogik befinden sich auf dem Anwendungsserver. Um Skalierbarkeit zu ermöglichen, befinden sich der Anwendungsserver und der Webserver auf zwei unterschiedlichen Servern.

- Für die Standardinstallation werden CA EEM, die Hardware-Abstimmungs-Engine, der Export-Service, die Speicherverwaltungsdienst-Komponente, der LDAP-Datenimport und die Synchronisation auf dem gleichen Server installiert (Anwendungsserver).
- Für eine benutzerdefinierte Installation können Sie über mehr als einen Anwendungsserver verfügen. Die Export-Service-Komponente und die Speicherverwaltungsdienst-Komponente müssen auf einem der Anwendungsserver, aber nicht notwendigerweise auf dem gleichen Server installiert werden.

Die folgenden Felder bedürfen einer Erklärung:

Anwendungsserver oder IP/Host des Lastenausgleichsmoduls

Die Installation von CA APM legt dieses Feld standardmäßig als Hostnamen des Anwendungsservers fest.

- In einer Umgebung mit einem einzelnen Anwendungsserver können Sie den Hostnamen oder die IP-Adresse des Anwendungsservers eingeben.
- In einer Umgebung mit mehreren Anwendungsservern können Sie entweder den Hostnamen des Anwendungsservers oder die IP-Adresse des Lastenausgleichs eingeben.

Hinweis: Der Anwendungsserver kann im Domain Name System (DNS) unter einem anderen Namen registriert werden als der registrierte Hostname des Anwendungsservers. Geben Sie in diesem Fall den anderen Namen im Feld an.

Sie können weitere Anwendungsserverkomponenten konfigurieren, nachdem Sie das Produkt installiert haben.

Hinweis: Weitere Informationen zum Ändern der Konfiguration von Komponenten und Hinzufügen von Servern finden Sie im *Administrationshandbuch*.

Hardware-Abgleichs-Engine

Die Hardware-Abgleichs-Engine ist der Dienst, der mit erkannten Assets mit den entsprechenden verwalteten Assets aus unterschiedlichen logischen Repositories abstimmt, so dass Sie die auf Ihre Geschäftsmethoden basierten Assets verwalten können. Die Hardware-Engine ruft Daten aus der CA MDB ab und speichert die Ergebnisse auch dort.

- Für die Standardinstallation wird die Hardware-Abgleichs-Engine auf dem Anwendungsserver installiert.
- Für die benutzerdefinierte Installation können Sie die Hardware-Abgleichs-Engine auf einem oder mehreren Servern installieren.

Sie können zusätzliche Hardware-Abgleichs-Engine-Komponenten konfigurieren, nachdem Sie das Produkt installiert haben.

Hinweis: Weitere Informationen zum Ändern der Konfiguration von Komponenten und Hinzufügen von Servern finden Sie im *Administrationshandbuch*.

CA EEM

CA APM verwendet CA EEM für die Authentifizierung. Andere Produkte, die CA EEM für die Authentifizierung benötigen, können den gleichen CA EEM-Server verwenden, den CA APM verwendet.

- Um Sicherheit zentral für mehrere CA Technologies-Produkte zu verwalten, geben Sie den Namen, die Lokation und die Anmeldeinformationen für den vorhandenen CA EEM-Server an.
- Um die CA APM-Sicherheit unabhängig von anderen CA Technologies-Produkten zu verwalten, installieren Sie CA EEM auf jedem anderen Anwendungs- oder Webserver als den, auf dem das vorhandene CA EEM installiert ist.

Hinweis: Sie können die Komponentenkonfigurationen ändern und zusätzliche Komponenten für Ihr Unternehmen konfigurieren, nachdem Sie das Produkt installiert haben. Weitere Informationen zum Ändern der Konfiguration von Komponenten und Hinzufügen von Servern finden Sie im *Administrationshandbuch*.

CA Business Intelligence

CA Business Intelligence verwaltet, überwacht und konfiguriert die Berichtsumgebung. CA APM verwendet CA Business Intelligence, um Informationen zu integrieren, zu analysieren und zu präsentieren, die für eine wirksame Unternehmens-IT-Verwaltung erforderlich sind. CA Business Intelligence wird auf dem Webserver für die Standardinstallation und auf einem Server installiert, den Sie für die benutzerdefinierte Installation festlegen.

Weitere Informationen über die Anmelde- und Verbindungsinformationen, die Sie für die CA Business Intelligence-Komponente eingeben, finden Sie unter [Integration von CA APM und CA Business Intelligence](#) (siehe Seite 134).

Diese Komponente ist optional in der Demo-Installation. Sie können diese Komponente während der Installation überspringen und die Komponente zu einem späteren Zeitpunkt von der Produktregisterkarte "Verwaltung", "Systemkonfiguration" hinzufügen.

Export-Service

Der Export-Service exportiert Daten aus CA APM und speichert die Ergebnisse in Formaten, wie z.B. einer kommagetrennten CSV-Datei. Zur Erfüllung dieses Tasks interagiert der Export-Service mit dem Storage Manager Service, so dass Sie einen Speicherort für die exportierten Dateien angeben können.

- Für die Standardinstallation wird die Hardware-Abgleichs-Engine auf dem Anwendungsserver installiert.
- Für die benutzerdefinierte Installation installieren Sie den Export-Service auf einem der Anwendungsserver.

Hinweis: Weitere Informationen über den Export-Service finden Sie im *Benutzerhandbuch*.

Data Importer-Engine-Dienst

Data Importer-Engine-Dienst importiert Massenproduktinformationen über Spalten- und Feldzuordnungen in die CA MDB. Data Importer wird auf dem Anwendungsserver für die standardmäßige Installation und für die anwenderdefinierte Installation installiert.

Hinweis: Sie können die Komponentenkonfigurationen ändern und zusätzliche Komponenten für Ihr Unternehmen konfigurieren, nachdem Sie das Produkt installiert haben. Weitere Informationen zum Ändern der Konfiguration von Komponenten und Hinzufügen von Servern finden Sie im *Administrationshandbuch*.

Importtreiber

Die Prozesse des Importtreibers haben Hardware-Datenexporte von CA SAM erkannt. CA APM verwendet die erkannten Hardware-Daten, um Eigentum und Discovery-Daten zu verknüpfen. CA APM exportiert Eigentumsdaten zurück nach CA SAM.

Der Importtreiber wird auf dem Anwendungsserver für die standardmäßige Installation und für die anwenderdefinierte Installation installiert.

Hinweis: Sie können die Komponentenkonfigurationen ändern und zusätzliche Komponenten für Ihr Unternehmen konfigurieren, nachdem Sie das Produkt installiert haben. Weitere Informationen zum Ändern der Konfiguration von Komponenten und Hinzufügen von Servern finden Sie im *Administrationshandbuch*.

LDAP Data Import and Sync Service

"LDAP-Datenimport und Synchronisation" importiert Daten aus CA EEM oder aus einer externen Datenquelle (LDAP oder CA SiteMinder) in CA APM. Nachdem die Daten vom Dienst importiert wurden, startet der Dienst den Datensynchronisationsvorgang mit der ca_contact-Tabelle.

- Für die Standardinstallation wird der LDAP Data Import and Sync Service auf dem Anwendungsserver installiert.
- Für die benutzerdefinierte Installation installieren Sie den LDAP-Datenimport und Synchronisation auf einem der Data Importer-Server.

Hinweis: Sie können die Komponentenkonfigurationen ändern und zusätzliche Komponenten für Ihr Unternehmen konfigurieren, nachdem Sie das Produkt installiert haben. Weitere Informationen zum Ändern der Konfiguration von Komponenten und Hinzufügen von Servern finden Sie im *Administrationshandbuch*.

Storage Manager-Service

Der Storage Manager-Service speichert exportierten Dateien, Dateianhänge, Datenimportdaten und Zuordnungsdateien und Protokolldateien für Datenimport und Massenänderung.

- Für die Standardinstallation wird der Storage Manager-Service auf dem Anwendungsserver installiert.
- Für die benutzerdefinierte Installation installieren Sie den Storage Manager-Service auf einem der Anwendungsserver.

Hinweis: Sie können die Komponentenkonfigurationen ändern und zusätzliche Komponenten für Ihr Unternehmen konfigurieren, nachdem Sie das Produkt installiert haben. Weitere Informationen zum Ändern der Konfiguration von Komponenten und Hinzufügen von Servern finden Sie im *Administrationshandbuch*.

CA APM-Registrierungsservice

Der CA APM-Registrierungsservice konsolidiert individuelle CA APM-CORA-Dienste in einen Hauptdienst. Sie können Installationen anderer CA Technologies-Produkten haben, die auch die CORA-API verwenden. Die Änderungen, die Sie an der CORA-API in Ihrer CA APM-Umgebung vornehmen, wirken sich nicht auf die Verwendung der CORA-API durch andere CA Technologies-Produkte aus.

Der CA APM-Registrierungsservice wird auf dem Anwendungsserver für die standardmäßige Installation und für die anwenderdefinierte Installation installiert.

Hinweis: Sie können die Komponentenkonfigurationen ändern und zusätzliche Komponenten für Ihr Unternehmen konfigurieren, nachdem Sie das Produkt installiert haben. Weitere Informationen zum Ändern der Konfiguration von Komponenten und Hinzufügen von Servern finden Sie im *Administrationshandbuch*.

Common Administration for Service Management (CASM)

CASM bietet CA APM administrative Funktionen, wie Mandantenfähigkeitsverwaltung. Mit Mandantenfähigkeit können mehrere unabhängige Mandanten (und ihre Anwender) eine einzige Implementierung von CA APM gemeinsam nutzen.

- Für die Standardinstallation wird CASM automatisch auf dem Anwendungsserver ohne Anwendereingabe installiert.
- Für die benutzerdefinierte Installation machen Sie Eingaben für die Installation von CASM auf einem Server (z.B. dem Web- oder Anwendungsserver).

Hinweis: Weitere Informationen über die Implementierung der Mandantenfähigkeit finden Sie unter [Implementieren der Mandantenfähigkeit](#) (siehe Seite 123).

Event-Service

Der Event-Service verwaltet den Ereignis- und Benachrichtigungsprozess in CA APM. Ereignisse sind wichtige Aktivitäts- oder Datenänderungen, die Sie verfolgen wollen und die Sie in CA APM definieren. Nachdem ein angegebenes Ereignis aufgetreten ist, werden Benachrichtigungen gesendet, um entsprechende Anwender und Administratoren über das Ereignis zu warnen.

Um die Benachrichtigungsfunktion durchzuführen, interagiert der Event-Service mit einem Workflow-Provider (z.B. CA Process Automation) unter Verwendung des Webdiensts. Ein Workflow-Provider verwaltet automatische Prozesse. Wenn Ihr Workflow-Provider CA Process Automation ist, können Sie die vorhandene Instanz von CA Process Automation während der Installation angeben, oder Sie können CA Process Automation mit CA Service Desk Manager und CA Service Catalog gemeinsam nutzen.

- Für die Standardinstallation installieren Sie den Event-Service auf dem Anwendungsserver.
- Für die benutzerdefinierte Installation installieren Sie den Event-Service auf einem der Anwendungsserver.

Diese Komponente ist optional in der Installation. Sie können diese Komponente während der Installation überspringen und die Komponente zu einem späteren Zeitpunkt von der Produktregisterkarte "Verwaltung", "Systemkonfiguration" hinzufügen. Diese Komponente ist obligatorisch, wenn SAM-Funktionen (Software Asset Management) aktiviert und konfiguriert sind.

Die folgenden Felder bedürfen einer Erklärung:

Provider-URL

Definiert die URL, mit der auf den Workflow-Provider zugegriffen wird.

Beispiel: Die folgende URL ist ein Beispiel für eine standardmäßige URL der CA Process Automation-Workflow-Webservices:

`http://<wf_hostname>:<wf_tomcat_port>/itpam/soap`

Provider-Anwendername

Definiert die Anwender-ID für das Anmelden beim Workflow-Provider.

Provider-Kennwort

Definiert das Anwenderkennwort für das Anmelden beim Workflow-Provider.

Provider-Prozesspfad

Definiert den Pfad für den Zugriff auf die Startanforderungsformulare für den Workflow-Provider. Diese Formulare müssen für die CA APM-Integration mit dem Workflow-Provider verfügbar sein. Weitere Informationen finden Sie in der Workflow-Provider-Dokumentation.

Standard: /

Hinweis: Weitere Informationen über Ereignisse und Benachrichtigungen finden Sie im *Benutzerhandbuch*.

Hinweis: Sie können die Komponentenkonfigurationen ändern und zusätzliche Komponenten für Ihr Unternehmen konfigurieren, nachdem Sie das Produkt installiert haben. Weitere Informationen zum Ändern der Konfiguration von Komponenten und Hinzufügen von Servern finden Sie im *Administrationshandbuch*.

Migration Toolkit

Mit dem Migration Toolkit können Sie CA APM-Daten von Version 11.3.4 nach Version 12.8 verschieben. Die Datenmigration verschiebt die Daten in Ihrer Datenbank aus den früheren Datenbankstrukturen in die neuen Datenbankstrukturen. Sie verwenden das Migration Toolkit, um die Datenmigration auszuführen. Das Migration Toolkit enthält die folgenden vier Tools:

- Migrationsdokumentation
- Migrationsberichterstellung
- Konfiguration für duplizierte Asset-Namen
- Migrationshilfsprogramm

Das Migration Toolkit wird auf dem Anwendungsserver für die standardmäßige Installation und für die anwenderdefinierte Installation installiert.

Asset Management-System (AMS)

Im Asset Management-System (AMS) können Sie verwaltete und durch Discovery ermittelte Daten für ein Asset anzeigen, das durch Abgleich verknüpft wurde, einschließlich Systemkonfiguration, Betriebssystem, Systemgeräte und Dateisystem. Sie können diese Daten auf der Seite "Asset-Details" anzeigen, indem Sie auf den Link "Verwaltete Informationen" oder "Durch Discovery ermittelte Informationen" klicken.

Das AMS erfordert, dass folgende Komponenten erfolgreich installiert und ausgeführt werden:

- Apache Tomcat-Server, der in der Installation von CA APM enthalten ist. Der Standardwert für den Apache Tomcat-Serverport ist 9080. Sie können diesen Wert nach der Installation ändern. Aktualisieren Sie zuerst den Port in der Konfigurationsdatei von Apache Tomcat. Ändern Sie anschließend den Port im Produkt (Registerkarte "Verwaltung", "Systemkonfiguration", "AMS").
- Java Development Kit (JDK). Bevor Sie mit der Installation von CA APM beginnen, installieren Sie zunächst das JDK auf dem Anwendungsserver, auf dem Sie das AMS installieren werden.

Nach der Konfiguration von AMS wird die Komponente für eine nicht sichere Netzwerkkommunikation konfiguriert (http). Sie können die Komponente für sichere Netzwerkkommunikation (https) konfigurieren, indem Sie zuerst den Apache Tomcat-Server (auf dem AMS installiert ist) konfigurieren, um das SSL-Protokoll zu unterstützen. Dann muss eine Einstellung für die AMS-Komponente in der Netzwerkkonfigurationsdatei geändert werden.

Wichtig! Die Tomcat-Portnummer für CA APM ist in der Standardeinstellung 9080. Wenn ein anderes in CA APM integriertes Produkt diese Portnummer verwendet, ändern Sie die Portnummer in CA APM, um einen Konflikt zu verhindern.

- Für die Standardinstallation installieren Sie AMS auf dem Anwendungsserver.
- Für die benutzerdefinierte Installation installieren Sie AMS auf einem der Anwendungsserver.

WCF-Service

Der Service "Windows Communications Foundation (WCF)" implementiert die Webservice-Funktion in CA APM. Die Webdienst-Funktion ermöglicht es Ihnen eine standardbasierte Schnittstelle zu verwenden, um Client-Anwendungen zu erstellen, die mit CA APM integriert werden.

Mit CA APM-Webservices können Sie CA APM-Objekte über Ihre externe Client-Anwendung erstellen, suchen, aktualisieren, kopieren und löschen. Ihre zugewiesene Anwenderrolle bestimmt, ob Sie über die Berechtigung verfügen, auf die Webdienste in CA APM zuzugreifen und beschränkt auch die Objekte und Daten (Klassen und Attribute), die Sie anzeigen oder ändern können.

- Bei der standardmäßigen Installation wird der WCF-Service auf einem Anwendungsserver mit Anwendereingabe installiert. Sie können die WCF-Service-Protokolleinstellung ändern.
- Bei der anwenderdefinierten Installation wird der WCF-Service auf einem Anwendungsserver mit Anwendereingabe installiert. Sie müssen den Servernamen für die Komponente angeben, und Sie können die Protokolleinstellung von "WCF-Service" ändern.

Die folgenden Felder bedürfen einer Erklärung:

IP/Host des WCF-Serviceservers des Lastenausgleichs

Die Installation von CA APM legt dieses Feld standardmäßig als Hostnamen des WCF-Service-Servers fest.

- In einer Umgebung mit einem einzelnen WCF-Service-Server können Sie den Hostnamen oder die IP-Adresse des WCF-Service-Servers eingeben.
- In einer Umgebung mit mehreren WCF-Service-Servern können Sie entweder den Hostnamen des WCF-Service-Servers oder die IP-Adresse des Lastenausgleichs eingeben.

Hinweis: Der WCF-Service-Server kann im Domain Name System (DNS) unter einem anderen Namen registriert werden als der registrierte Hostname des WCF-Service-Servers. Geben Sie in diesem Fall den anderen Namen im Feld an.

Sie können die Konfiguration der Komponente "WCF-Service" ändern, nachdem Sie das Produkt installiert haben.

Hinweis: Weitere Informationen zum Ändern der Konfiguration von Komponenten und Hinzufügen von Servern finden Sie im *Administrationshandbuch*.

Software Asset Management

Die Software Asset Management-Komponente ermöglicht es Ihnen, Software Asset Management-Funktionen über CA SAM zu aktivieren. Wenn Sie sowohl CA APM als auch CA SAM implementieren, können Sie das Management der Hardware- und Software-Assets in Ihrer Organisation koordinieren. CA APM verwaltet Hardware-Asset-Daten und CA SAM verwaltet Software-Asset und Lizenzdaten. Allgemeine Daten, die beide Produkte benötigen, werden gemeinsam genutzt.

- Bei der standardmäßigen Installation wird Software Asset Management auf einem Anwendungsserver mit Anwendereingabe installiert.
- Bei der anwenderspezifischen Installation wird Software Asset Management auf einem Anwendungsserver mit Anwendereingabe installiert.

Sie können die Konfiguration der Komponente "Software Asset Management" ändern, nachdem Sie das Produkt installiert haben.

Hinweis: Sie können die Komponentenkonfigurationen ändern und zusätzliche Komponenten für Ihr Unternehmen konfigurieren, nachdem Sie das Produkt installiert haben. Weitere Informationen zum Ändern der Konfiguration von Komponenten und Hinzufügen von Servern finden Sie im *Administrationshandbuch*.

Phase 4: Stellen Sie die Installation auf den zusätzlichen erforderlichen Servern fertig.

In Phase 4 der Installation installieren Sie das Produkt auf den zusätzlichen erforderlichen Servern.

Für die Standardinstallation haben Sie den Anwendungsserver, den Webserver und den Datenbankserver in Phase 2 angegeben. In Phase 3 haben Sie das Produkt auf dem ersten Server (Anwendungs- oder Webserver) installiert. In Phase 4 schließen Sie die Produktinstallation auf den zusätzlichen erforderlichen Servern ab, die Sie in Phase 2 identifiziert haben.

Wichtig! Geben Sie für die Standard- und die benutzerdefinierte Installation denselben ITAM-Stammpfad (z.B. C:\Programme\CA\ITAM) für die Produktkomponenten ein, die Sie installieren, wenn Sie die erforderlichen Server in Phase 4 eingeben.

So führen Sie Phase 4 der Installation aus:

1. Legen Sie die Installationsdatenträger in das Computerlaufwerk auf dem nächsten erforderlichen Server ein.
Die Installation startet automatisch.
2. Folgen Sie den Bildschirmanweisungen, um den Installations-Manager zu installieren und die Installation zu konfigurieren (ähnlich den Schritten, die Sie in der Phase vor der Installation und in Phase 1 ausgeführt haben).

3. Wenn die CCC-Seite angezeigt wird, wählen Sie die folgende Option aus:

Ein CA-APM-CCC beauftragte mich, setup.exe auf diesem Computer auszuführen, um die Installation dieser CA-APM-Instanz abzuschließen.

4. Geben Sie den Namen des ersten Servers ein, auf dem Sie die Installation ausgeführt haben (auf dem CCC installiert ist).

5. Überprüfen Sie die Administrator-Anmeldeinformationen für den aktuellen Server.

Der Installations-Manager überprüft die Konnektivität für den Server und startet die Produktinstallation auf dem aktuellen Server. Die Komponenten, die Sie für den aktuellen Server festgelegt haben, werden installiert. Eine Konfigurationszusammenfassung wird angezeigt.

6. Wenn eine oder mehrere Komponenten nicht installiert werden können, führen Sie die folgenden Schritte durch:

- a. Klicken Sie auf "Show Log", um die Fehlerdetails im Protokoll anzuzeigen.
- b. Beheben Sie den Fehler. Um die Voraussetzungen für die Konfiguration einer nicht installierten Komponente zu korrigieren, kehren Sie mithilfe der Navigationsschaltflächen zur Komponentenkonfiguration zurück.
- c. Klicken Sie auf "Retry Install".

Der Installations-Manager versucht, nur die Komponenten zu installieren, bei denen zuvor ein Fehler aufgetreten ist, und zeigt eine Zusammenfassung der Installation an.

7. Fahren Sie fort, die aufgetretenen Installationsfehler zu beheben, und klicken Sie auf "Retry Install", bis alle Voraussetzungen erfüllt und alle Komponenten installiert sind.

8. Wenn mehr erforderliche Server vorhanden sind, wiederholen Sie Phase 4 für die verbleibenden Server.

Wenn alle Voraussetzungen erfüllt und alle Komponenten auf allen erforderlichen Servern installiert sind, ist die Produktinstallation abgeschlossen.

Aktualisieren der Apache Tomcat-Konfigurationsdatei

Im Asset Management-System (AMS) können Sie erkannte und verwaltete Daten für ein Asset anzeigen, das durch Abgleich verknüpft wurde, einschließlich Systemkonfiguration, Betriebssystem, Systemgeräte und Dateisystem. Das AMS erfordert die Installation des Java Development Kit (JDK), bevor Sie die Installation von CA APM starten. Außerdem ist der Apache Tomcat-Server erforderlich, der in der Installation von CA APM eingeschlossen ist. Der Standardwert für den Apache Tomcat-Serverport ist 9080. Sie können diesen Wert nach der Installation ändern. Sie aktualisieren zuerst den Port in der Konfigurationsdatei "Apache Tomcat". Dann ändern Sie den Port im Produkt (Registerkarte "Verwaltung", "Systemkonfiguration", "AMS").

Wichtig! Die Tomcat-Portnummer für CA APM ist in der Standardeinstellung 9080. Wenn ein anderes in CA APM integriertes Produkt diese Portnummer verwendet, ändern Sie die Portnummer in CA APM, um einen Konflikt zu verhindern.

So aktualisieren Sie die Apache Tomcat-Konfigurationsdatei:

1. Navigieren Sie auf dem Anwendungsserver, auf dem AMS installiert ist, zu einem der folgenden Ordner, abhängig von Ihrem Server:

C:\Programme\CA\SharedComponents\AMS\Tomcat\conf (für 32-Bit)

C:\Programme(x86)\CA\SharedComponents\AMS\Tomcat\conf (für 64-Bit)

2. Wählen Sie die server.xml-Datei aus, und öffnen Sie sie.
3. Navigieren Sie zum folgenden Abschnitt der server.xml-Datei:

```
<Connector port="9080" protocol="HTTP/1.1"
  connectionTimeout="20000"
  redirectPort="8443" />
```

4. Aktualisieren Sie die Tomcat-Portnummer mit der gleichen Nummer, die CA APM verwendet (Registerkarte "Administration", "Systemkonfiguration", "AMS").
5. Speichern Sie die server.xml-Datei.

Konfigurieren von AMS für Sichere Netzwerkkommunikation

Mit dem Asset Management-System (AMS) können Sie erkannte und verwaltete Daten für ein Asset anzeigen, das durch Abgleich verbunden wurde. Nachdem Sie das AMS installiert haben, das die [Installation des Java Development Kit \(JDK\)](#) (siehe Seite 21) erfordert, bevor Sie die Installation von CA APM starten, wird die Komponente für nicht sichere Netzwerkkommunikation konfiguriert (http). Sie können die Komponente für sichere Netzwerkkommunikation (https) konfigurieren, indem Sie zuerst den Apache Tomcat-Server (auf dem AMS installiert ist) konfigurieren, um das SSL-Protokoll zu unterstützen. Dann muss eine Einstellung für die AMS-Komponente in der Netzwerkkonfigurationsdatei geändert werden.

Hinweis: Weitere Informationen über die Konfiguration des Apache Tomcat-Servers für das SSL-Protokoll finden Sie in der Apache-Tomcat-Dokumentation.

So konfigurieren Sie AMS für sichere Netzwerkkommunikation:

1. Überprüfen Sie, ob der Apache Tomcat-Server (auf dem AMS installiert ist) für SSL konfiguriert ist.
2. Starten Sie den Tomcat-Server neu.
3. Navigieren Sie auf dem CA APM-Webserver zum folgenden Ordner:
[ITAM-Stammverzeichnis]\Web Server
4. Öffnen Sie die Web.config-Datei mit einem Texteditor.
5. Suchen Sie nach der folgenden Anweisung:

```
<add key="AMS" value="http://server_name:non_ssl_port/AMS/login.do" />
```
6. Ändern Sie die folgende Anweisung, um http in https zu ändern und die nicht sichere Portnummer (*non_ssl_port*) durch eine sichere Portnummer zu ersetzen.

```
<add key="AMS" value="https://server_name:ssl_port/AMS/login.do" />
```
7. Speichern Sie die Änderungen in der Datei "web.config", und schließen Sie die Datei.

AMS verwendet sichere Netzwerkkommunikation.

Hinweis: Folgende Aktualisierungen der Webserverkonfiguration über die Systemkonfiguration im Produkt überschreiben die Änderungen, die Sie in diesem Vorgang vorgenommen haben.

Konfigurieren des AMS für den Namen Ihres Domain Name System (DNS)

Mit dem Asset Management-System (AMS) können Sie erkannte und verwaltete Daten für ein Asset anzeigen, das durch Abgleich verbunden wurde. Nachdem Sie das AMS installiert haben, das die [Installation des Java Development Kit](#) (siehe Seite 21) (JDK) erfordert, bevor Sie die Installation von CA APM starten, wird die Komponente und nicht der öffentliche DNS-Name für den AMS-Servernamen konfiguriert. Um die Komponente für den DNS-Namen zu konfigurieren, ändern Sie in der Netzwerkkonfigurationsdatei die Einstellung für die AMS-Komponente .

So konfigurieren Sie AMS für den DNS-Namen

1. Navigieren Sie auf dem Webserver zum folgenden Ordner:

[ITAM-Stammverzeichnis]\Web Server

2. Öffnen Sie die Web.config-Datei mit einem Texteditor.

3. Suchen Sie nach der folgenden Anweisung:

```
<add key="AMS" value="http://AMS Server Name:9080/AMS/login.do" />
```

4. Ändern Sie die Anweisung, um den AMS-Servernamen mit dem öffentlichen DNS-Namen zu ändern.

```
<add key="AMS" value="http://Public DNS Name where AMS is  
installed:9080/AMS/login.do" />
```

5. Speichern Sie die Änderungen in der Datei "web.config", und schließen Sie die Datei.

AMS verwendet den DNS-Namen statt des AMS-Servernamens.

Hinweis: Folgende Aktualisierungen der Webserverkonfiguration über die Systemkonfiguration im Produkt überschreiben die Änderungen, die Sie in diesem Vorgang vorgenommen haben.

Konfigurieren des AMS mit Teiid

Mit dem Asset Management-System (AMS) können Sie erkannte und verwaltete Daten für ein Asset anzeigen, das durch Abgleich verbunden wurde. Nachdem Sie das AMS installiert haben, das die [Installation des Java Development Kit \(JDK\)](#) (siehe Seite 21) erfordert, bevor Sie die Installation von CA APM starten, konfigurieren Sie die Komponente mit Teiid. Um die Komponente mit Teiid zu konfigurieren, laden Sie Teiid herunter, und extrahieren Sie Teiid auf dem Anwendungsserver, wo AMS installiert ist.

Gehen Sie wie folgt vor:

1. Greifen Sie unter folgender Adresse auf die Teiid-Startseite zu:
<http://www.jboss.org/teiid>
2. Klicken Sie auf der rechten Seite auf "Downloads".
3. Laden Sie "Teiid Embedded", Version 8.3, auf den Anwendungsserver herunter, wo AMS installiert ist.
4. Extrahieren Sie die ZIP-Datei in einen beliebigen Ordner auf dem Server.
5. Wechseln Sie zum folgenden Ordner:
`Teiid_download_folder/lib/`
Ersetzen Sie *Teiid_download_folder* durch den Pfad des Ordners, wo Sie Teiid heruntergeladen haben.
6. Kopieren Sie alle jar-Dateien in den folgenden Ordner:
`<AMS Home>/Tomcat/lib`
7. Wechseln Sie zum folgenden Ordner:
`Teiid_download_folder/optional/`
8. Kopieren Sie alle jar-Dateien in den folgenden Ordner:
`<AMS Home>/Tomcat/lib`
AMS wird mit Teiid konfiguriert.

Konfigurieren des Export-Service für Sichere Netzwerkkommunikation

Der Export-Service exportiert Daten aus CA APM und speichert die Ergebnisse in Formaten, wie z.B. einer kommagetrennten CSV-Datei. Zur Erfüllung dieses Tasks interagiert der Export-Service mit dem Storage Manager Service, so dass Sie einen Speicherort für die exportierten Dateien angeben können. Nachdem Sie das Produkt installiert haben, wird der Export-Service für nicht sichere Netzwerkkommunikation konfiguriert (http). Um den Export-Service für sichere Netzwerkkommunikation zu konfigurieren (https), führen Sie die folgenden Schritte durch.

So konfigurieren Sie den Export-Service für sichere Netzwerkkommunikation:

1. Melden Sie sich an dem Server an, auf dem der Export-Service installiert ist.
2. Wechseln Sie zum folgenden Ordner:
`C:\Programme\CA\ITAM\Export Service`

3. Öffnen Sie die CA.ExportService.exe.config-Datei mit einem Texteditor.
4. Suchen Sie nach der folgenden Anweisung:

```
<add key="SMWebServiceProtocol" value="http" />
```
5. Ändern Sie die folgende Anweisung, um http in https zu ändern.

```
<add key="SMWebServiceProtocol" value="https" />
```
6. Suchen Sie in der Datei nach der Zeichenfolge "SMWebServicePort", und aktualisieren Sie den Wert auf den SSL-Port.
7. Speichern Sie die Änderungen in der Datei "CA.ExportService.exe.config", und schließen Sie die Datei.

Der Export-Service verwendet sichere Netzwerkkommunikation.

Starten der Dienste

Nachdem die Installation abgeschlossen ist, starten Sie alle Dienste.

Hinweis: Unter bestimmten Umständen können Sie nach der Produktinstallation eine Meldung erhalten, dass CA Business Intelligence installiert wurde, Sie jedoch den Webserver neu starten müssen. Starten Sie den Webserver neu, bevor Sie überprüfen, ob die CA Business Intelligence-Dienste gestartet wurden.

Gehen Sie wie folgt vor:

1. Öffnen Sie die Systemsteuerung (klicken Sie zum Beispiel auf "Start", "Einstellungen", "Systemsteuerung").
2. Doppelklicken Sie auf "Verwaltung".
3. Doppelklicken Sie auf "Dienste".
Die verfügbaren Dienste werden angezeigt.
4. Suchen Sie alle folgenden Dienste, und führen Sie folgenden Schritt aus:
 - Apache-Tomcat-AMS
 - CA Asset Portfolio Management - Data Importer-Engine
 - CA Asset Portfolio Management - Event-Service
 - CA Asset Portfolio Management - Export-Service
 - CA Asset Portfolio Management - Registrierungsservice
 - CA Asset Portfolio Management - HW-Abgleichs-Engine

- CA Asset Portfolio Management - LDAP Import Service
- CA-CASM

Wichtig! Zur Leistungsverbesserung empfehlen wir, den CA CASM-Dienst nicht zu starten, wenn Sie keine Mandantenfähigkeit verwenden.

- CA iTechonology iGateway 4.6
- Zentraler Konfigurations-Agent (CCA) von ITAM
- Zentrale Konfigurationssteuerung (CCC) von ITAM
- Utildev Web Server Pro

5. Klicken Sie mit der rechten Maustaste auf jeden Dienst, und wählen Sie "Starten" aus.

Der Dienst wird gestartet.

6. Um CA Business Intelligence-Dienste mit dem Central Configuration Manager zu prüfen, wählen Sie "Start", "Programme", "BusinessObjects XI Release", "BusinessObjects Enterprise", "Central Configuration Manager" aus.

Der Central Configuration Manager wird geöffnet.

7. Wenn ein Dienst nicht gestartet wird, klicken Sie mit der rechten Maustaste auf den Dienst und wählen Sie "Starten".

Der Dienst wird gestartet.

Starten der Web-Schnittstelle

Nachdem die Installation vollständig durchgeführt wurde, können Sie die Webbenutzeroberfläche starten, um zu überprüfen, dass CA APM verwendet werden kann. Nachdem Sie überprüft haben, ob die Webbenutzeroberfläche gestartet wurde, stellen Sie allen Administratoren die URL und Anmeldeinformationen zur Verfügung, damit sie sich anmelden und das Produkt für die Anwender vorbereiten können. Die Administratoren können dann die Sicherheit, die Benutzeroberfläche, den Hardware-Abgleich und ggf. die Produktkomponenten konfigurieren. Nachdem die Administratoren das Produkt vorbereitet haben, können sie den Anwendern die URL und Anmeldeinformationen bereitstellen.

Hinweis: Weitere Informationen über die Verwaltung und Vorbereitung des Produkts für die Anwender erhalten Sie im *Administrationshandbuch*.

Um die Webbenutzeroberfläche zu starten, öffnen Sie einen Web-Browser und geben die folgende URL ein:

`http://servername/itam`

Ersetzen Sie den *Servernamen* durch den Namen des Servers, der die CA APM-Webserver hostet.

Hinweis: Wenn die Sicherheit von Internet Explorer auf "Hoch" gesetzt ist, wird beim Starten der Webbenutzeroberfläche 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.

Auf Ihrem Webserver wird eine Startmenü-Verknüpfung erstellt, die sich auf die URL-Lokation bezieht.

Um sich nach dem Öffnen der URL bei CA APM anzumelden, geben Sie die folgenden Standardanmeldeinformationen ein:

Anwendername

uapadmin

Kennwort

uapadmin

Hinweis: Wenn Sie während der Installation das Kennwort geändert haben, verwenden Sie das von Ihnen erstellte Kennwort.

In einigen Situationen wird ein Browserfehler oder ein [Anwendernamensfehler](#) (siehe Seite 172) angezeigt. Sie können diese Fehler lösen, indem Sie den Fehlersuchanweisungen folgen.

Überprüfen der Installation

Nachdem Sie alle Installationsvorgänge abgeschlossen haben, können Sie überprüfen, ob CA APM Version 12.8 erfolgreich installiert wurde.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei den Servern an, auf denen Sie CA APM Version 12.8 installiert haben.
2. (Windows 2008) Wählen Sie im Startmenü "Systemsteuerung", "Programme und Funktionen" aus.

3. Stellen Sie sicher, dass folgende Komponente auf allen anwendbaren Servern verfügbar sind:

CA Asset Portfolio Management - 12.8

Hinweis: Die individuellen Dienste und Komponente, die in früheren Versionen angezeigt wurden, sind in dieser einen Komponente mit Version 12.8 enthalten.

Sie haben die Installationsüberprüfung abgeschlossen.

Deinstallieren von CA APM

CA APM kann aus verschiedenen Gründen von einem Computer deinstalliert werden. Zum Beispiel kann CA APM deinstalliert werden, weil Sie den Computer für einen anderen Zweck verwenden möchten oder die Komponenten auf einen anderen Computer verschieben möchten. Um das Produkt zu deinstallieren, führen Sie die folgenden Schritte aus:

Hinweis: Führen Sie für die standardmäßige und benutzerdefinierte Installation diese Schritte auf jedem Computer (außer dem Datenbankserver) aus, auf dem CA APM installiert ist.

Gehen Sie wie folgt vor:

1. Überprüfen Sie, ob sich alle Anwender vom Produkt abgemeldet haben.

Hinweis: Anwender, die sich vor Beginn der Deinstallation nicht vom Produkt abgemeldet haben, erhalten eine Fehlermeldung (z. B. eine Fehlermeldung, die angibt, dass die Seite nicht angezeigt werden kann), wenn sie versuchen, eine Aufgabe abzuschließen.

2. Melden Sie sich bei dem Computer an, auf dem CA APM installiert ist.
3. Wechseln Sie zum folgenden Ordner:

[ITAM-Stammverzeichnis]\ITAM\Uninstall

4. Starten Sie die Deinstallation, indem Sie zweimal auf die Datei "APM_UNINSTALL.bat" klicken.
5. Folgen Sie im Deinstallationsvorgang den Anweisungen auf dem Bildschirm.

Die Deinstallation wird ausgeführt und entfernt erfolgreich alle installierten CA APM-Komponenten, außer CA MDB, CA EEM, der Common Registration API (CORA), dem Asset Management-System (AMS), UtilDev, Microsoft .NET 4.0 Framework, WSE 3.0 und CA Business Intelligence.

Kapitel 5: So migrieren Sie CA APM-Daten von Version 11.3.4 auf Version 12.8

Dieses Kapitel enthält folgende Themen:

[So migrieren Sie CA APM-Daten von Version 11.3.4 auf Version 12.8](#) (siehe Seite 63)

So migrieren Sie CA APM-Daten von Version 11.3.4 auf Version 12.8

Als Systemadministrator führen Sie die Datenmigration aus, wenn Sie CA APM-Daten von Version 11.3.4 auf Version 12.8 verschieben möchten. Nachdem Sie Version 12.8 installiert haben, wird ein Upgrade der Strukturen der CA Management-Datenbank (CA MDB) ausgeführt, und Sie werden aufgefordert, Ihre Daten zu migrieren.

Die Installation des Upgrades und der Migrationsvorgang Ihrer Daten sind separate Prozesse:

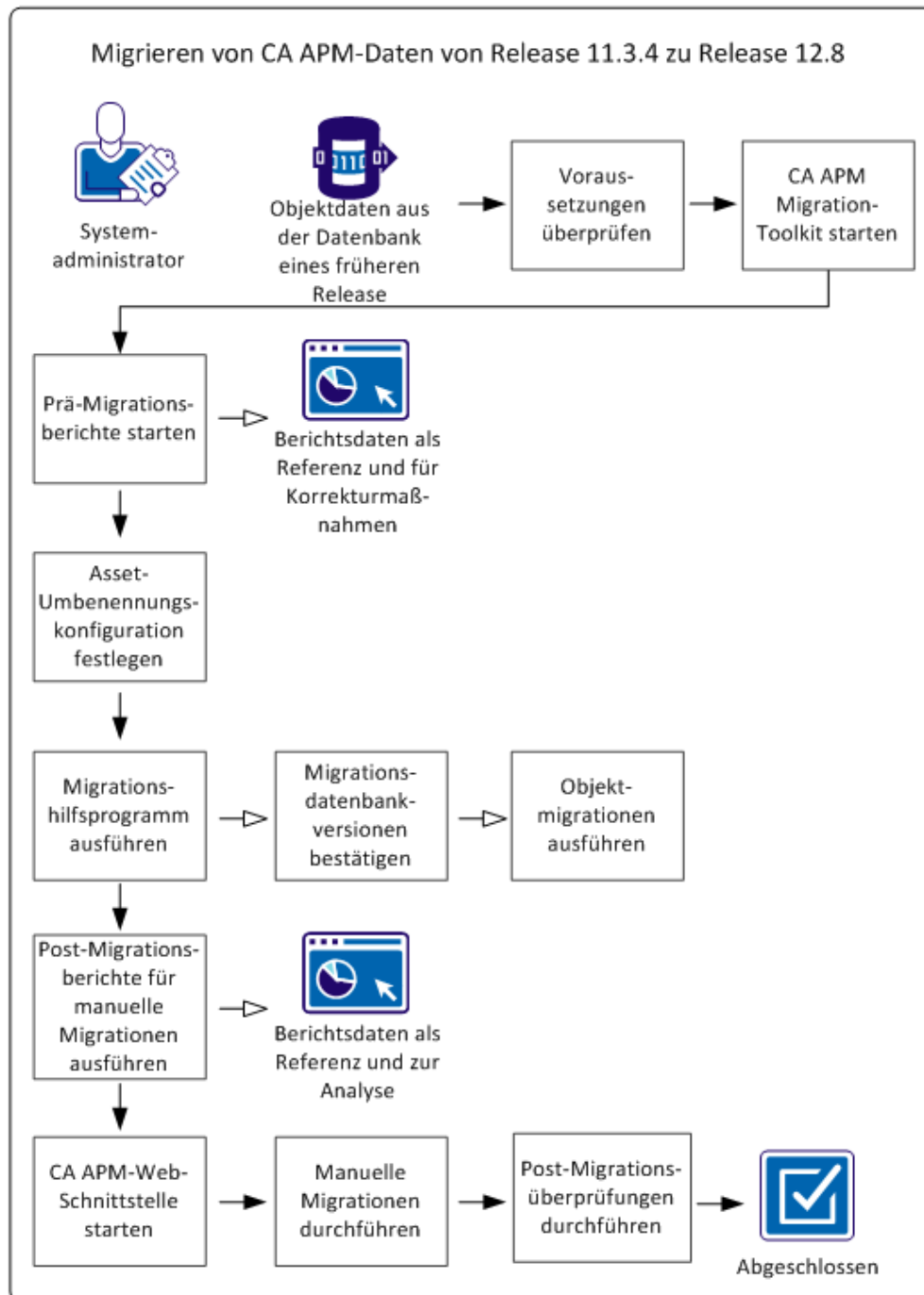
- **Upgrade.** Aktualisiert die Anwendung und die Datenbankstrukturen auf eine neuere Version.
- **Migrieren.** Transformiert oder verschiebt die Daten aus früheren Datenbankstrukturen in neue Datenbankstrukturen, die während des Upgrades erstellt wurden.

Das Migrations-Toolkit von CA APM enthält folgende Tools, die Ihnen helfen, Ihre Daten von Datenbankstrukturen der Version 11.3.4 in neue Datenbankstrukturen der Version 12.8 zu migrieren:

- **Migrationsdokumentation.** Stellt die Anweisungen bereit, um Migrationsberichte zu generieren, das Migrationshilfsprogramm auszuführen und um Objekte manuell zu migrieren.
- **Migrationsberichterstellung.** Generiert Berichte, die Ihnen während des Migrationsvorgangs helfen. Sie generieren [Prä-Migrationsberichte](#), (siehe Seite 73) *bevor* Sie das [Migrationshilfsprogramm](#) (siehe Seite 83) ausführen, um potenzielle Probleme während der Migration zu vermeiden. Sie generieren [Post-Migrationsberichte](#) (siehe Seite 89), *nachdem* Sie das Migrationshilfsprogramm ausgeführt haben. Mit diesen Post-Migrationsberichten können Sie Legacy-Datenbankstrukturen manuell migrieren, die nicht mithilfe des Migrationshilfsprogramms migriert werden können.

- **Konfiguration für duplizierte Asset-Namen.** Gibt die Umbenennungskonfiguration an, die auf duplizierte Asset-Namen angewendet werden soll.
- **Migrationshilfsprogramm.** Gibt die automatisierten Schritte an, um die ausgewählten Objekte in Ihren Legacy-Datenbankstrukturen in neue Datenbankstrukturen zu verschieben.

Folgendes Diagramm veranschaulicht, wie ein Systemadministrator Daten migriert.



Um CA APM-Daten zu migrieren, führen Sie diese Schritte aus:

1. [Überprüfen Sie die Voraussetzungen](#) (siehe Seite 67).
2. [Starten Sie das CA APM-Migrations-Toolkit](#) (siehe Seite 73).
3. [Führen Sie die Prä-Migrationsberichte aus](#) (siehe Seite 73).

Verwenden Sie die [Berichtsdaten der Prä-Migrationsberichte zur Referenz und für Korrekturmaßnahmen](#) (siehe Seite 75).

4. [Geben Sie die Umbenennungskonfiguration des Asset an](#) (siehe Seite 82).
5. [Führen Sie das Migrationshilfsprogramm aus](#) (siehe Seite 83).
 - a. [Bestätigen Sie die Versionen der Migrationsdatenbank](#) (siehe Seite 85).
 - b. [Führen Sie die Objektmigrationen aus](#) (siehe Seite 87).
6. [Führen Sie die Post-Migrationsberichte für manuelle Migrationen aus](#) (siehe Seite 89).

Verwenden Sie die [Berichtsdaten der Post-Migrationsberichte zur Referenz und zur Analyse](#) (siehe Seite 91).

7. [Starten Sie die CA APM-Webschnittstelle](#) (siehe Seite 96).
8. [Führen Sie manuelle Migrationen aus](#) (siehe Seite 97).
9. [Führen Sie eine Verifizierung der Post-Migration aus](#) (siehe Seite 115).

Beispiel: Migrieren von CA APM-Daten von Version 11.3.4 auf Version 12.8

Miriam ist CA APM-Systemadministrator beim Unternehmen "Document Management Company". Sie möchte ein Upgrade der CA APM-Version 11.3.4 auf Version 12.8 durchführen, und sie möchte die Daten aus den Legacy-Datenstrukturen in die aktualisierten Datenstrukturen migrieren. Miriam überprüft die Voraussetzungen für den Start der Migration und der Upgrades auf die neue Version.

Miriam startet das Migration Toolkit von CA APM. Zuerst generiert und überprüft sie die Prä-Migrationsberichte. Die Berichte helfen dabei, Objekte zu identifizieren, die sie in den Legacy-Datenstrukturen korrigieren muss, bevor das Migrationshilfsprogramm erfolgreich ausgeführt wird. Sie legt einige Berichte beiseite, die später verwendet werden, um neue Namen für Assets zu konfigurieren, die den gleichen Namen haben, und um manuelle Migrationen auszuführen.

Nachdem Miriam die Korrekturen in den Legacy-Datenstrukturen vorgenommen hat, überprüft sie die duplizierten Berichte für Asset-Namen, um nicht eindeutige Asset-Namen zu identifizieren. Miriam öffnet die Konfiguration für duplizierte Asset-Namen und wählt eine Umbenennungskonfiguration für duplizierte Asset-Namen aus. Diese Assets werden umbenannt, wenn Miriam das Migrationshilfsprogramm ausführt.

Miriam öffnet das Migrationshilfsprogramm. Sie testet die Datenbankverbindungen, wodurch bestätigt wird, dass die richtige CA APM-Legacy-Datenbankversion zur richtigen neuen Versionsdatenbankversion migriert wird.

Miriam wählt die zu migrierenden Objekte aus, und sie führt das Migrationshilfsprogramm aus. Sie überwacht den Migrationsvorgang, indem Sie die Fortschritts- und Statusmeldungen liest. Wenn alle Objekte migriert sind, wird das Objekt des Audit-Verlaufs für die Migration verfügbar. Sie wählt das Objekt des Audit-Verlaufs aus und führt das Migrationshilfsprogramm erneut aus.

Wenn der Prozess des Migrationshilfsprogramms abgeschlossen ist, generiert Miriam die Post-Migrationsberichte. Die Berichte geben die erfolgreich migrierten Daten und die nicht migrierten Daten an. Miriam muss die Daten, die nicht migriert wurden, manuell migrieren.

Manuelle Migrationen werden mithilfe der aktualisierten CA APM Version 12.8-Webschnittstelle ausgeführt. Miriam startet die Webschnittstelle. Sie führt die manuellen Migrationen mithilfe der Informationen der Post-Migrationsberichte aus. Sie bestätigt die migrierten Daten, um den Migrationsvorgang abzuschließen.

Überprüfen der Voraussetzungen

Stellen Sie sicher, dass Sie diese Voraussetzungen in folgender Reihenfolge abgeschlossen haben, um sicherzustellen, dass Sie Daten erfolgreich migrieren können:

Hinweis: Viele Migrationsvoraussetzungen werden während der Version 12.8-Installation abgeschlossen. Das *Implementierungshandbuch* stellt Informationen zur Installation bereit.

1. Lesen Sie folgende Informationen:
 - [CA IT Asset Manager-Produkt-Roadmap](#).
 - [Unterschiede zwischen CA IT Asset Manager 12.8 und früheren Versionen \(CA IT Asset Manager 12 und CA Asset Portfolio Management 11.3.4\)](#).
 - Bekannte Probleme sind auf der [CA APM-Produktseite](#) verfügbar.
 - [Beziehungsunterschiede zwischen Version 11.3.4 und Version 12.8](#) (siehe Seite 70).
2. Stellen Sie sicher, dass die aktuelle Patch-Ebene der Version 11.3.4 der kumulative Patch 14 oder höher ist. Wenn die aktuelle Patch-Ebene unbekannt ist oder nicht dem kumulativen Patch 14 oder höher entspricht, laden Sie den aktuellsten kumulativen Patch von CA APM Version 11.3.4 von der CA Support-Website herunter.

3. Laden Sie Kettle von der CA Support-Website herunter, und installieren Sie Kettle auf dem Server, auf dem CA APM Version 12.8 installiert ist. Gehen Sie folgendermaßen vor, um Kettle herunterzuladen:
 - a. Navigieren Sie zu <http://ca.com/support>, und melden Sie sich bei CA Support an.
 - b. Klicken Sie auf "Download Center".
 - c. Wählen Sie in der Drop-down-Liste der Produktsuche "CA Asset Portfolio Management" aus.
 - d. Wählen Sie "12.8" in der Drop-down-Liste zur Versionsauswahl aus.
 - e. Wählen Sie "pentaho-kettle-4.4.0.zip" in der Liste der Komponentenauswahl aus, und klicken Sie auf "Start".
 - f. Speichern Sie "pentaho-kettle-4.4.0.zip" in das gewünschte Verzeichnis.
Beispiel: C:\Programme(x86)\CA\ITAM
 - g. Extrahieren Sie die Inhalte von "pentaho-kettle-4.4.0.zip".
Ein neuer Ordner mit dem Namen "Kettle" wird erstellt. Notieren Sie den Pfad des Ordners.
4. Erstellen Sie eine Umgebungsvariable für Kettle, indem Sie diese Schritte ausführen.
 - a. Klicken Sie auf "Start", "Ausführen", und geben Sie "sysdm.cpl" ein, um auf die Systemeigenschaften zuzugreifen.
 - b. Klicken Sie auf die Registerkarte "Erweitert".
 - c. Klicken Sie auf "Umgebungsvariablen".
 - d. Klicken Sie im Abschnitt der Systemvariablen auf die Schaltfläche "New..." (Neu...), und geben Sie folgende Details ein:

Variablenname	
	KETTLE_HOME
Variablenwert	
	Pfad des Kettle-Ordners.

Hinweis: Stellen Sie sicher, dass der Pfad auf den übergeordneten Ordner festgelegt ist, der den Ordner "data-integration" enthält. Beispiel:
C:\Programme(x86)\CA\ITAM\Kettle.
 - e. Klicken Sie auf "OK", und beenden Sie die Systemeigenschaften.

5. Halten Sie folgende Services und die geplanten Tasks für CA APM und andere integrierte Service Management-Produkte an:
 - CA Unicenter Asset Portfolio Management (CA APM)
 - CA APM-Zwischenspeicherdienst
 - CA APM-Benachrichtigungsdienst
 - Automatisierte Abgleichstasks
 - CA Service Catalog Version 12.8
 - CA Service Catalog
 - CA Service Accounting
 - CA Service Catalog Version 12.7
 - CA Service Accounting
 - CA Service Fulfillment
 - CA Service Repository Agent
 - CA Service View
 - CA Service Desk Manager
 - CA Service Desk Manager Server
 - CA Client Automation
 - Für CA Client Automation-Enterprise-Manager und Domänen-Manager, die die CA MDB, die migriert wird, direkt freigeben, halten Sie den CA Client Automation-Service mithilfe von *caf stop* an.
 - Für andere Server, die ergänzende Engine-Prozesse anhand der CA MDB, die migriert wird, ausführen, halten Sie den CA Client Automation-Service mithilfe von *caf stop* an.
 - Für Engine-Prozesse, die die Tasks der Datenbanksynchronisierung für die CA MDB ausführen, die migriert wird, halten Sie die Jobs der Datenbanksynchronisierung mithilfe des DSM-Explorers an.
 - Halten Sie die Tasks der Engine-Replikation für die Enterprise mithilfe des DSM-Explorers für jeden CA Client Automation-Domänen-Manager an, der Berichte an die Enterprise sendet.

6. Sichern Sie die Datenbank von CA APM Version 11.3.4.
7. Suchen Sie das Hilfsprogramm für die Migrations-Zustandsprüfung im Ordner "Health Check Utility" (Hilfsprogramm für die Zustandsprüfung) auf den CA APM Version 12.8-Installationsdatenträgern. Führen Sie das Hilfsprogramm auf der Datenbank von CA APM Version 11.3.4 aus.
Wichtig! Weitere Informationen zur Ausführung des Hilfsprogramms finden Sie im Benutzerhandbuch des *Hilfsprogramms für die Zustandsprüfung von CA Migration*, das sich auf dem Installationsdatenträger befindet.
8. Laden Sie die "JRE 1.6.43" von der Oracle-Website (<http://www.oracle.com>) herunter, und installieren Sie die JRE auf dem Server, wo Sie CA APM Version 12.8 installieren.
9. Überprüfen Sie die Einstellungen der Transaktionsprotokollreihenfolge von Microsoft SQL Server für die CA MDB, und stellen Sie sicher, dass die Einstellungen für den Massenimport von Daten positioniert sind. Führen Sie die folgenden Schritte aus, um diese Informationen zu finden:
 - a. Öffnen Sie in einem Web-Browser die Microsoft-Website (<http://www.microsoft.com>) und suchen Sie nach "Transaktionsprotokollverwaltung".
 - b. Folgen Sie den Anweisungen im Artikel.
10. Installieren Sie Version 12.8 für die Datenbank der Version 11.3.4.
Hinweis: Das Implementierungshandbuch stellt Informationen zur Version 12.8-Installation bereit.
11. Stellen Sie sicher, dass keine Version 12.8-Services ausgeführt werden. Diese Services können weiterhin ausgeführt werden, wenn Sie das CA APM-Migrations-Toolkit beendet haben, bevor Sie das Datenmigrationshilfsprogramm ausgeführt oder die Berichte für die manuelle Migrationen generiert haben.

Beziehungsunterschiede zwischen Version 11.3.4 und Version 12.8

CA APM Version 11.3.4 enthält Beziehungen, die im Produkt angegeben sind, und ermöglicht es Ihnen, neue anwenderspezifische Beziehungen hinzuzufügen. Die Unterstützung von Beziehungen wurde in Version 12.8 geändert.

Beziehungen, die nicht in Version 12.8 unterstützt werden

Folgende Beziehungen und zugeordnete Links, die in Version 11.3.4 angegeben sind, werden in Version 12.8 nicht unterstützt:

- Aktivitätsübersicht
- Kontakte (Budget-Manager, Unterstützt von, Benutzer)
- Abhängigkeiten (Ist abhängig von)
- Produktentwicklung (Entwickelt in)
- Produkt-Upgrade (Aktualisiert auf)
- Benutzerzuordnung (Reserviert für)
- SW-Zuordnung (Reserviert auf)

Beziehungen, die in Version 12.8 unterstützt werden

Folgende Beziehungen der Version 11.3.4 werden in Version 12.8 unterstützt:

- Asset-Berechtigung (Lizenziert für)
- Unternehmenserwerb (Erworben von)
- Firmenberechtigung (Lizenziert für)
- Kontaktberechtigung (Lizenziert für)
- Übergeordnetes Dokument (Unterliegt)
- Bildpartitionen (Partitionierte CPU)
- Rechtliche Ergänzungsvereinbarung (Ergänzung)
- Lokationsberechtigung (Lizenziert für)
- HW-Asset-Konfiguration (Generische Komponente, Spezifische Komponente)
- HW-Modellkonfiguration (Generische Komponente)

Die Datenstrukturen, um die Beziehungsinformationen zu speichern, wurden geändert. Um die Beziehungsinformationen von Version 11.3.4 in Version 12.8 zu verschieben, muss das Migrationshilfsprogramm die Beziehungen nach dem Namen der Beziehungsvorlage und nach dem Linknamen der Beziehungsvorlage identifizieren.

Was Sie vornehmen müssen: Bevor Sie das Migrationshilfsprogramm ausführen, ändern Sie die geänderten Namen in der Beziehungsvorlage oder im Link der Beziehungsvorlage in die Werte der ursprünglichen Version 11.3.4.

Änderungen der Benutzeroberfläche

In CA APM Version 11.3.4 werden Beziehungen und Links angezeigt und in separaten Abschnitten der Benutzeroberfläche geändert. In Version 12.8 werden Beziehungen und Links in eine einzelne Entität verbunden, die angezeigt und im gleichen Abschnitt der Benutzeroberfläche geändert wird.

Einige Menüpunkte für Beziehungsnamen in Version 12.8 sind anders als Version 11.3.4. Folgendes Diagramm listet alle unterstützten Beziehungen von Version 11.3.4 und den entsprechenden zugeordneten Beziehungsmenüpunkt von Version 12.8 auf. Einige Beziehungsmenüpunkte haben eine andere Bezeichnung, wenn die Beziehung in umgekehrter Richtung angezeigt wird. Zum Beispiel wird die Beziehung "Unternehmensberechtigung" als "Unternehmenszuordnung" dargestellt, wenn vom Software-Asset angezeigt, und sie wird als "Software-Zuweisung" dargestellt, wenn vom Unternehmen angezeigt.

Beziehung der 11.3.4-Beziehung	Version 12.8-Entität	Version 12.8-Beziehung
Asset-Berechtigung	Asset (Software)	Asset-Zuordnung
Asset-Berechtigung	Asset (Hardware)	Software-Zuordnung
Unternehmenserwerb	Unternehmen	Unternehmenserwerb
Firmenberechtigung	Asset (Software)	Unternehmenszuordnung
Firmenberechtigung	Unternehmen	Software-Zuordnung
Kontaktberechtigung	Asset (Software)	Kontaktzuordnung
Kontaktberechtigung	Kontakt	Software-Zuordnung
Übergeordnetes Dokument	Rechtsdokument	Übergeordnetes Rechtsdokument
Bildpartitionen	Asset	Image-Partitionen
Rechtliche Ergänzungsvereinbarung	Rechtsdokument	Rechtliche Änderung
Lokationsberechtigung	Asset (Software)	Lokationszuordnung
Lokationsberechtigung	Lokation	Software-Zuordnung
HW-Asset-Konfiguration (Generische Komponente)	Asset	Modellkonfiguration
HW-Asset-Konfiguration (Spezifische Komponente)	Asset	Asset-Konfiguration
HW-Modellkonfiguration	Modell	Modellkonfiguration

Anwenderspezifische Beziehungen, die nicht in Version 12.8 unterstützt werden

Anwenderspezifische Beziehungen, die mit Version 11.3.4 erstellt werden, werden in Version 12.8 nicht unterstützt und werden während des Migrationsvorgangs nicht migriert. Weitere Informationen zur Unterstützung von anwenderspezifischen Beziehungen finden Sie in der [CA IT Asset Manager-Produkt-Roadmap](#).

Die Daten der anwenderspezifischen Beziehung von Version 11.3.4 gehen während der Migration auf Version 12.8 nicht verloren. Die Informationen werden in den Legacy-Datenstrukturen in der CA MDB gespeichert.

Starten des CA APM-Migrations-Toolkit

Während des Upgrades von Version 11.3.4 auf Version 12.8 wird das Migration Toolkit von CA APM auf dem gleichen Computer installiert, der das Upgrade durchführt. Wir empfehlen, dass Sie Ihre CA MDB-Daten sofort nach dem Upgrade in die neuen Versionsdatenstrukturen migrieren.

Starten Sie das Migration Toolkit von CA APM auf dem gleichen Computer, auf dem Sie das Upgrade durchgeführt haben.

Gehen Sie wie folgt vor:

- Klicken Sie "Start", "Alle Programme", "CA", "Asset Portfolio Management", "CA APM-Migrations-Toolkit".

Ausführen der Prä-Migrationsberichte

Bevor Sie die CA MDB migrieren, führen Sie die Prä-Migrationsberichte aus. Die Prä-Migrationsberichte identifizieren folgende Datentypen:

- Daten, die während der Datenmigration Probleme verursachen können. Sie korrigieren die Daten in der CA MDB, *bevor* Sie das [Migrationshilfsprogramm](#) (siehe Seite 83) ausführen. Wenn Sie zum Beispiel eine Beziehungsvorlage umbenannt haben, die in der Version 11.3.4 bereitgestellt wurde, könnte diese Änderung bei der Migration von Beziehungen ein Problem verursachen. Der Beziehungsbericht identifiziert die umbenannten Vorlagen, die Sie vor Migration wieder auf die ursprünglichen Vorlagennamen, die im Produkt vorgegeben sind, ändern.

- Daten, die eine Analyse für die Entscheidungen bei der Migrationskonfiguration benötigen.
- Daten, die nicht mit dem Migrationshilfsprogramm migriert werden, die jedoch mithilfe von aktualisierten Produktfunktionen manuell migriert werden können. Während der [manuellen Migration](#) (siehe Seite 97), *nachdem* Sie das Migrationshilfsprogramm ausgeführt haben, beziehen Sie sich auf diese Daten. Sie müssen die Daten in diesen Berichten erfassen, bevor Sie Ihre Legacy-Daten migrieren, da die Daten nicht in die Version 12.8-Datenbankstrukturen migriert werden. Sie speichern diese Berichte, und während der [manuellen Migration](#) (siehe Seite 97) für Version 12.8 beziehen sich auf ihre Informationen.
- Daten, die in Version 11.3.4 unterstützt werden, die jedoch nicht in Version 12.8 unterstützt werden. Sie können diese Daten nicht mit dem Migrationshilfsprogramm migrieren oder mithilfe von Version 12.8 hinzufügen. Diese Berichte identifizieren nicht unterstützte Daten und stellen Legacy-Referenzinformationen bereit.

Hinweis: Weitere Informationen zu den in Version 12.8 unterstützten Funktionen finden Sie in der [CA IT Asset Manager Produkt-Roadmap](#) und in den Dokumenten [Unterschiede zwischen CA IT Asset Manager 12.8 und früheren Versionen \(CA IT Asset Manager 12. und CA Asset Portfolio Management 11.3.4\)](#) auf der CA Support-Website.

Gehen Sie wie folgt vor:

1. Klicken Sie im Hauptfenster des CA APM-Migrations-Toolkit auf "Berichterstellung zur Migration".

Folgende Kontrollkästchen im Bereich "Prä-Migrationsberichte" sind ausgewählt:

- Custom Index (Anwenderspezifischer Index)
- Duplicate Asset Name (Duplizierter Asset-Name)
- Abstimmung
- Beziehungen

Hinweis: Wenn Sie nicht alle Berichte generieren möchten, wählen Sie nur die gewünschten Berichtstypen aus.

2. Klicken Sie im Bereich "Report Output Folder" (Berichtsausgabeordner) auf "Durchsuchen", und wählen Sie den Ausgabeordner aus, in dem Sie die Berichte speichern möchten.
3. Klicken Sie auf "Generate Reports" (Berichte generieren).

Statusmeldungen werden im Meldungsbereich angezeigt, wo Sie den Berichterstellungsprozess überwachen können.

Sie werden aufgefordert, den Berichtsausgabeordner zu öffnen, um die Berichte anzuzeigen.

4. Klicken Sie auf "Ja".

Windows Explorer wird geöffnet. Das Berichterstellungs-Tool erstellt einen Ordner für jedes Kontrollkästchen, das Sie zuvor aktiviert haben.

5. Navigieren Sie zu einem Berichtsordner, und öffnen Sie ihn.

Die Berichte werden im CSV-Format (durch Kommas getrennte Werte) angezeigt.

6. Klicken Sie mit der rechten Maustaste auf einen Bericht, und wählen Sie "Öffnen mit", "Excel" aus, um den Bericht zu öffnen und in einem Tabellenformat anzuzeigen.

Die [Berichtsdaten](#) (siehe Seite 75) werden in einem Tabellenformat dargestellt. Die Tabellenüberschriften sind in der ersten Zeile.

Hinweis: Sie können auf den Bericht klicken, um ihn zu öffnen und in einem Texteditor im CSV-Format anzuzeigen.

Berichtsdaten der Prä-Migration zur Referenz und für Korrekturmaßnahmen

Das Berichterstellungs-Tool generiert Berichte in CSV-Format, die Sie mit einem Texteditor öffnen können. Die Berichtsfeldnamen und Feldwerte werden durch Kommas getrennt. Sie können auch einen Bericht mit Excel öffnen, wo die Daten in einem Tabellenformat dargestellt werden. Wenn Sie einen Bericht mit Excel öffnen, sind die Feldnamen die Spaltenüberschriften, und die Feldwerte werden in den Zeilen unter den Überschriften angezeigt.

Folgende Prä-Migrationsberichte stellen Ihnen Informationen zu Daten bereit, die Sie vor der Migration in der CA MDB ändern müssen. Die zugehörigen Objekte können dann erfolgreich in die Version 12.8 CA MDB-Datenstrukturen migriert werden.

- [Anwenderspezifischer Indexbericht](#) (siehe Seite 76)
- [Beziehungsbericht](#) (siehe Seite 77)

Folgende Berichte identifizieren Daten, die Sie für Entscheidungen bei der Migrationskonfiguration analysieren:

- [Bericht für duplizierte Asset-Namen](#) (siehe Seite 80)
- Abgleichsbericht:
 - [Abfragebericht der Hauptübersetzungsliste](#) (siehe Seite 80)

Folgende Prä-Migrationsberichte identifizieren Daten, die Sie verwenden, *nachdem* Sie das [Migrationshilfsprogramm](#) (siehe Seite 83) ausgeführt haben, wenn Sie manuelle Migrationen [ausführen](#) (siehe Seite 97). Speichern Sie diese Berichte, und verweisen Sie während der manuellen Migration auf sie.

- Abgleichsberichte:
 - [Bericht "Abfrage des Haupt-Task"](#) (siehe Seite 81)
 - [Bericht "Task zum Hinzufügen eines Asset"](#) (siehe Seite 81)
 - [Bericht "Anwenderspezifische Suche"](#) (siehe Seite 81)

Folgende Berichte identifizieren Daten, die nicht in Version 12.8 unterstützt werden und die Legacy-Referenzinformationen bereitstellen:

- Abgleichsberichte:
 - [Berichte über veraltete Übersetzungslisten](#) (siehe Seite 81)
 - [Berichte über unkonvertierte Übersetzungslisten](#) (siehe Seite 81)

Anwenderspezifischer Indexbericht

Der anwenderspezifische Indexbericht identifiziert Indizes, die zu Feldern in Version 11.3.4 (oder in früheren Versionen) zur Anwenderanpassung hinzugefügt wurden. Diese Indizes können zu Leistungsproblemen in Version 12.8 führen. Wir empfehlen, dass Sie [anwenderspezifische Indizes aus Ihrer Datenbank entfernen](#) (siehe Seite 76). Der Bericht gibt SQL-Anweisungen an, die Sie ausführen, um die anwenderspezifischen Indizes zu entfernen.

Entfernen von anwenderspezifischen Indizes aus der Datenbank

Wir empfehlen, dass Sie anwenderspezifische Indizes aus Ihrer Datenbank entfernen, um Leistungsprobleme zu vermeiden. Entfernen Sie die Indizes, *bevor* Sie das Migrationshilfsprogramm ausführen. Der [anwenderspezifische Indexbericht](#) (siehe Seite 76) stellt Informationen bereit, die Sie verwenden, um anwenderspezifische Indizes zu entfernen.

Gehen Sie wie folgt vor:

1. Suchen Sie den anwenderspezifischen Indexbericht.
2. Kopieren Sie die SQL-Anweisungen aus der Drop-Spalte "SQL" auf dem Bericht.
Hinweis: Löschen Sie die Anführungszeichen am Anfang und am Ende der Anweisungen.
3. Fügen Sie die SQL-Anweisungen in Ihr bevorzugtes Tool ein, zum Beispiel Microsoft SQL Server Management Studio und Oracle SQL Developer, und führen Sie die Anweisungen aus.

Folgende Elemente werden entfernt:

- Anwenderspezifische Indizes
- Indexdefinitionen aus der Tabelle "arg_index_member"
- Indexinformationen aus der Tabelle "arg_index_def"

Beziehungsbericht

Der Beziehungsbericht identifiziert die Beziehungsvorlagen, die von den ursprünglichen Namen, die in der Produktversion 11.3.4 vorgegeben sind, umbenannt wurden. Ändern Sie diese Daten in der CA MDB *vor* der Migration.

Das Tool generiert den Beziehungsbericht in verschiedenen Sprachen. Verwenden Sie den entsprechenden Bericht für die Sprache, die für die Version 11.3.4 konfiguriert wurde.

Der Bericht zeigt folgenden Status für die Beziehungsvorlage oder für den Link der Beziehungsvorlage an:

Benutzerdefiniert

Gibt an, dass der Anwender in Version 11.3.4 die Beziehungsvorlagen oder die Links der Beziehungsvorlagen hinzugefügt oder umbenannt hat.

- Wenn die Beziehung in Version 11.3.4 hinzugefügt wurde, wird sie in Version 12.8 nicht unterstützt, und sie wird nicht migriert.
- Wenn die Beziehung in Version 11.3.4 im Produkt angegeben ist und in Version 12.8 unterstützt wird, benennen Sie die Beziehungsvorlagen oder die Links der Beziehungsvorlage in ihre ursprünglichen Werte um, um die Beziehung auf Version 12.8 zu migrieren.

Migriert durch das Migrationshilfsprogramm

Gibt an, dass die Beziehungsvorlagen oder die Links der Beziehungsvorlage in Version 12.8 unterstützt und über das Hilfsprogramm migriert werden.

Nicht mehr unterstützt

Zeigt die Beziehungsvorlagen oder die Links der Beziehungsvorlage an, die veraltet sind. Das Migrationshilfsprogramm wird diese Beziehungen nicht migrieren.

Nicht gefunden

Zeigt die im Produkt angegebenen Beziehungsvorlagen oder Links der Beziehungsvorlage in Version 11.3.4 an, die nicht in der Datenbank des Anwenders gefunden wurden. Wenn die Beziehungsvorlagen oder die Links der Beziehungsvorlage umbenannt wurden und in Version 12.8 unterstützt werden, benennen Sie die Beziehungsvorlagen oder die Links der Beziehungsvorlage in ihre ursprünglichen Werte, um die Beziehung auf Version 12.8 zu migrieren.

Vor Migration in Migrieren umbenennen

Gibt die umbenannten Beziehungsvorlagen oder Links der Beziehungsvorlage in Version 11.3.4 an, die vor der Migration in die ursprünglichen Namen geändert werden müssen.

Führen Sie folgende Aktionen durch, wenn Sie die umbenannten Beziehungsvorlagen, die im Produkt vorgegeben sind, in die Migration aufnehmen möchten:

- [Ändern Sie die umbenannte Beziehungsvorlage in den ursprünglichen Namen, der im Produkt vorgegeben ist](#) (siehe Seite 78).
- [Ändern Sie den umbenannten Link der Beziehungsvorlage in den ursprünglichen Namen, der im Produkt vorgegeben ist](#) (siehe Seite 79).

Ändern der umbenannten Beziehungsvorlage in den ursprünglichen Namen, der im Produkt vorgegeben ist

Bevor Sie das [Migrationshilfsprogramm ausführen](#) (siehe Seite 83), ändern Sie die umbenannten Beziehungsvorlagenamen in die ursprünglichen Beziehungsvorlagenamen von Version 11.3.4, die im Produkt vorgegeben sind.

Sie führen eine SQL-Anweisung aus, um den Beziehungsvorlagenamen zu ändern. Führen Sie diese Schritte für jeden Eintrag im Bericht mit dem Status "Vor Migration in Migrieren umbenennen" und einem Wert, der unter "Neuer Name der Beziehungsvorlage" angegeben ist, aus.

Gehen Sie wie folgt vor:

1. Führen Sie folgende SQL-Anweisung in Ihrem bevorzugten Tool aus (zum Beispiel "Microsoft SQL Server Management Studio" oder "Oracle SQL Developer"):

Hinweis: Die Klammern und der Text innerhalb der Klammern sind Platzhalter. Die Platzhalternamen stellen die Spaltennamen im Beziehungsbericht dar.

```
UPDATE arg_actiondf
SET adtext = '{Relationship Template Rename}'
WHERE adtext = '{Relationship Template Name}'
      AND adlobty IN (SELECT slentry
                      FROM arg_strlst
                      WHERE slid = 9
                      AND slvalue1 = '{Relationship Object Type}')
```

2. Ersetzen Sie die Platzhalter durch die Werte in den gleichnamigen Spalten im Beziehungsbericht. Zum Beispiel identifiziert die Spalte des Berichts "Relationship Template Rename" den Namen "Aktivitätsübersicht", der im Produkt vorgegeben ist. Sie ersetzen {Relationship Template Rename} durch "Aktivitätsübersicht".

Ändern des umbenannten Links der Beziehungsvorlage in den ursprünglichen Namen, der im Produkt vorgegeben ist

Bevor Sie das [Migrationshilfsprogramm ausführen](#) (siehe Seite 83), ändern Sie die umbenannten Link-Namen der Beziehungsvorlage in die ursprünglichen Link-Namen der Beziehungsvorlagen von Version 11.3.4, die im Produkt vorgegeben sind.

Sie führen eine SQL-Anweisung aus, um den Link-Namen der Beziehungsvorlage zu ändern. Führen Sie diese Schritte für jeden Eintrag im Bericht mit dem Status "Vor Migration in Migrieren umbenennen" und einem Wert, der unter "Linkumbenennung" angegeben ist, aus.

Gehen Sie wie folgt vor:

1. Führen Sie folgende SQL-Anweisung in Ihrem bevorzugten Tool aus (zum Beispiel "Microsoft SQL Server Management Studio" oder "Oracle SQL Developer"):

Hinweis: Die Klammern und der Text innerhalb der Klammern sind Platzhalter. Die Platzhalternamen stellen die Spaltennamen im Beziehungsbericht dar.

```
UPDATE arg_linkdef
SET ndtext = '{Link Rename}'
WHERE ndtext = '{Link Name}'
      AND nd2obty IN (SELECT slentry
                      FROM arg_strlst
                      WHERE slid = 9
                      AND slvalue1 = '{Link Object Type}')
```

2. Ersetzen Sie die Platzhalter durch die Werte in den gleichnamigen Spalten im Beziehungsbericht. Zum Beispiel identifiziert die Spalte des Berichts "Link Rename" (Linkumbenennung) den Namen "Approved by" (Vom Anwender genehmigt), der im Produkt vorgegeben ist. Sie ersetzen {Link Rename} durch "Approved by".

Bericht für duplizierte Asset-Umbenennung

Der Bericht für duplizierte Asset-Namen identifiziert nicht eindeutige Asset-Namen.

Hinweis: Es sind nur Assets betroffen, die den gleichen Asset-Namen und keine Werte für folgende Registrierungsfelder haben:

- Seriennummer
- Alt. Asset-ID
- Hostname
- DNS Name
- MAC-Adresse
- Seriennummer

Während der Migration kann das Migration Toolkit von CA APM automatisch einen eindeutigen Asset-Namen für jeden duplizierten Asset-Namen in Ihrer CA MDB konfigurieren. Verwenden Sie den Bericht für duplizierte Asset-Namen, um zu entscheiden, wie die [Konfiguration der Asset-Umbenennung angegeben werden soll](#) (siehe Seite 82).

Abgleichsberichte

Das Berichterstellungs-Tool generiert folgende Abgleichsberichte:

- [Abfragebericht der Hauptübersetzungsliste](#) (siehe Seite 80)
- [Berichte über veraltete Übersetzungslisten](#) (siehe Seite 81)
- [Berichte über unkonvertierte Übersetzungslisten](#) (siehe Seite 81)
- [Bericht "Abfrage des Haupt-Task"](#) (siehe Seite 81)
- [Bericht "Task zum Hinzufügen eines Asset"](#) (siehe Seite 81)
- [Bericht "Anwenderspezifische Suche"](#) (siehe Seite 81)

Abfragebericht der Hauptübersetzungsliste

Der Abfragebericht der Hauptübersetzungsliste identifiziert Daten der Legacy-Übersetzungslisten für Unternehmen, Betriebssysteme und Modelle. Sie analysieren die Daten auf diesem Bericht, um festzulegen, ob das Migrationshilfsprogramm verwendet werden soll, um Legacy-Übersetzungslisten zu den entsprechenden Version 12.8-Normalisierungsregeln zu migrieren oder ob die Listen manuell migriert werden sollen.

Wenn Sie [die Übersetzungslisten manuell migrieren](#) (siehe Seite 112), verwenden Sie die Daten im Abfragebericht der Hauptübersetzungsliste.

Bericht "Abfrage des Haupt-Task"

Der Bericht "Abfrage des Haupt-Task" der Prä-Migration identifiziert Daten, die Sie verwenden, *nachdem* Sie das [Migrationshilfsprogramm](#) (siehe Seite 83) ausgeführt haben. Der Bericht enthält Informationen zu Legacy-Abgleichstasks von Version 11.3.4. Speichern Sie den Bericht, und verweisen Sie ihn während der [manuellen Migration von Hardware-Abgleichstasks](#) (siehe Seite 112), um Abgleichsregeln in Version 12.8 zu erstellen.

Bericht "Task zum Hinzufügen eines Asset"

Der Bericht "Task zum Hinzufügen eines Asset" identifiziert Daten, die Sie verwenden, *nachdem* Sie das [Migrationshilfsprogramm](#) (siehe Seite 83) ausgeführt haben, wenn Sie manuelle Migrationen ausführen. Der Bericht identifiziert die Legacy-Abgleichstasks, die verwaltete Assets von Version 11.3.4 hinzufügen. Speichern Sie den Bericht, und verweisen Sie ihn während der [manuellen Migration von Hardware-Abgleichstasks](#) (siehe Seite 112).

Bericht "Anwenderspezifische Suche"

Der Bericht "Anwenderspezifische Suche" gibt Daten an, die Sie verwenden, *nachdem* Sie das [Migrationshilfsprogramm](#) (siehe Seite 83) ausgeführt haben, wenn Sie manuelle Migrationen ausführen. Der Bericht identifiziert die anwenderspezifische Suche des Legacy-Hardware-Abgleichs von Version 11.3.4. Version 12.8 stellt vordefinierte Berichte für den Hardware-Abgleich bereit. Sie können diese Berichte mithilfe von CA Business Intelligence anpassen, die auch in Version 12.8 bereitgestellt wird. Speichern Sie den Bericht, und verweisen Sie ihn während der [manuellen Migration von Hardware-Abgleichssuchen](#) (siehe Seite 113).

Berichte über veraltete Übersetzungslisten

Die Berichte über veraltete Übersetzungslisten identifizieren die Legacy-Übersetzungslisten des Hardware-Abgleichs von Version 11.3.4, die veraltet sind und in Version 12.8 nicht mehr unterstützt werden. Dieser Bericht dient zur Referenz. Keine Aktion erforderlich.

Berichte über unkonvertierte Übersetzungslisten

Die Berichte über unkonvertierte Übersetzungslisten identifizieren die Legacy-Übersetzungslisten des Hardware-Abgleichs von Version 11.3.4, die fehlende oder ungültige Einträge enthalten, die nicht in Version 12.8 migriert werden. Die Übersetzungsliste wird migriert, jedoch werden einige Einträge in der Liste nicht migriert, da in der Legacy-Datenbank keine unterstützenden Daten vorhanden sind.

Verwenden Sie die Daten der Berichte über unkonvertierte Übersetzungslisten und die Daten des [Abfrageberichts der Hauptübersetzungslisten](#) (siehe Seite 80), um nach der Migration die [fehlenden Einträge zu den Normalisierungslisten hinzuzufügen](#) (siehe Seite 113).

Angeben der Umbenennungskonfiguration des Asset

In Version 12.8 enthält die Registrierung den Asset-Namen, die Seriennummer, die Alt.Asset-ID, den Hostnamen, den DNS-Namen und die Mac-Adresse. Ein *eindeutiger* Asset-Name ist für jedes Asset-Objekt erforderlich. Diese Anforderung war nicht in Version 11.3.4 vorhanden. Somit könnte Ihre CA MDB über Asset-Namen verfügen, die für die Asset-Registrierung nicht eindeutig sind. Während der Migration kann das Migration Toolkit von CA APM automatisch einen eindeutigen Asset-Namen für jeden duplizierten Asset-Namen in Ihrer CA MDB konfigurieren.

Das Migration Toolkit von CA APM verwendet eine Konfiguration, um die duplizierten Asset-Namen umzubenennen. Sie wählen die Konfiguration im Dialogfeld der Konfiguration für duplizierte Asset-Namen im CA APM-Migrationshilfsprogramm aus. Wenn Sie das Migrationshilfsprogramm ausführen, werden die duplizierten Assets in Ihrer Version 12.8-Datenbank umbenannt.

Hinweis: Ein eindeutiger Asset-Name ist eine Anforderung für die Asset-Registrierung durch die Common Registration API (CORA) in Version 12.8. Wenn CORA nicht aktiviert ist, dann wird die Asset-Registrierung nicht durchgeführt. Daher müssen Sie die Asset-Umbenennungskonfiguration nicht angeben.

Gehen Sie wie folgt vor:

1. Überprüfen Sie den [Bericht für duplizierte Asset-Namen](#) (siehe Seite 80).
2. Klicken Sie im Hauptfenster des Migration Toolkit von CA Asset Portfolio Management auf "Konfiguration für duplizierte Asset-Namen".
3. Wählen Sie eine der folgenden Umbenennungskonfigurationen aus:

Replacement (Ersatz)

Ersetzt die duplizierten Asset-Namen durch den Wert in einem anderen Feld. Sie wählen dieses Feld in der Drop-down-Liste aus.

Hinweis: Die Felder in der Drop-down-Liste sind die gleichen Felder, die die Überschriften im [Bericht für duplizierte Asset-Namen](#) (siehe Seite 80) sind.

Die Inkrementierungskonfiguration ist automatisch ausgewählt und gesperrt. Wenn die Ersatzkonfiguration zu einem duplizierten Asset-Namen fügt, dann wird durch das Hinzufügen der Inkrementierung zur Konfiguration sichergestellt, dass die Umbenennung eindeutig ist.

Concatenation (Verkettung)

Hängt die Werte von einem oder mehreren Feldern ans Ende der duplizierten Asset-Namen an. Sie wählen bis zu vier Felder in den Drop-down-Listen aus.

Hinweis: Die Felder in den Drop-down-Listen sind die gleichen Felder, die die Überschriften im [Bericht für duplizierte Asset-Namen](#) (siehe Seite 80) sind.

Die Inkrementierungskonfiguration ist automatisch ausgewählt und gesperrt. Wenn die Verkettungskonfiguration zu einem duplizierten Asset-Namen fügt, dann wird durch das Hinzufügen der Inkrementierung zur Konfiguration sichergestellt, dass die Umbenennung eindeutig ist.

Incrementation (Inkrementierung)

Hängt einen eindeutigen Ganzzahlwert ans Ende des duplizierten Asset-Namens an, und erhöht die Ganzzahl um eins für jeden nachfolgenden duplizierten Asset-Namen. Sie geben die Startganzzahl in den Basislinienwert der Ganzzahl ein.

KEINE

Duplizierte Asset-Namen werden nicht umbenannt. Sie können diese Option auswählen, wenn CORA nicht aktiviert ist oder wenn Sie die Assets nach Migration manuell korrigieren möchten.

4. (Optional) Geben Sie einen Feldbegrenzer mit einem Zeichen an, das zwischen allen Feldern und zwischen einem Feld und einer Inkrementierungsganzzahl in den Inkrementierungs- und Verkettungskonfigurationen angezeigt wird.
5. Klicken Sie auf "Speichern".

Hinweis: Abhängig von der Anzahl der Datensätze nimmt das Speichern der Konfiguration etwas Zeit in Anspruch. Die Fortschrittsleiste zeigt den Status der Fertigstellung an.

6. Klicken Sie auf "Beenden".

Ausführen des Migrationshilfsprogramms

Das Migrationshilfsprogramm migriert Audits, Objekte und Events von einer CA APM-Version zur aktualisierten Datenbankstruktur einer anderen Version.

Die hierarchische Struktur der Objekte im Auswahlbereich des CA APM-Migrationshilfsprogramms ermöglicht es Ihnen, alle Objekte innerhalb einer Hierarchieebene auszuwählen oder individuelle Objekte innerhalb einer Ebene auszuwählen. Ein Statussymbol zeigt den Migrationsstatus für jedes Objekt oder für jede Objektebene an.

Das Schlüsselsymbol im oberen Bereich des Fensters zeigt die Status an. Wenn ein Objektstatus abgeschlossen ist, können Sie das Objekt nicht auswählen.

Die Registerkarten "Messages" (Meldungen) und "Zusammenfassung" ermöglichen es Ihnen, den [Migrationsvorgang zu überwachen](#) (siehe Seite 89) und den Migrationsablauf zu überprüfen.

Wichtig: Zusätzlich zu den Services und den geplanten Tasks, die unter [Voraussetzungen](#) (siehe Seite 67) angegeben sind, sollten Sie sicherstellen, dass die Version 12.8-Services nicht ausgeführt werden, bevor Sie das Migrationshilfsprogramm ausführen.

Wenn Sie das Fenster das erste Mal öffnen, werden Sie aufgefordert, die [Versionen der Migrationsdatenbank zu bestätigen](#) (siehe Seite 85). Nachdem Sie diese Aufgabe abgeschlossen haben, können Sie die [Objektmigrationen ausführen](#) (siehe Seite 87).

Mit dem Migrationshilfsprogramm können Sie folgende Objekte und zugeordnete Events migrieren:

- Assets
 - Eindeutiger Asset-Namen für CORA
 - Aktueller Statusverlauf des Asset
- Kosten und Zahlungen
 - Abrechnungscodes
 - Preiserhebungstypen
 - Kostentypen
 - Währungstyp
- Rechtsdokumente
 - Rechtsdefinition
 - Dokumentlokationen
 - Rechtsstellung
 - Statusverläufe der Rechtsdokumente

- Hinweise
 - Typen der Anmerkung
- OOTB-Beziehungen (Ursprüngliche Beziehungen, die im Produkt vorgegeben sind).
- Erweiterungen
 - Einfache Erweiterungen
 - Listenerweiterungen
 - Lokationshierarchien
- Anhänge
- Rollen
- Abgleichsübersetzungslisten (nur für unterstützte Typen)
 - Übersetzungsliste des Betriebssystems
 - Übersetzungsliste des Systemmodells
 - Übersetzungsliste des Herstellers
- Legacy-Audits, um Archivtabellen zu überwachen. Das Objekt "Audit-Verlauf" wird aktiviert, nachdem Sie andere Objekte migrieren und die Audit-Generierung für Events den Status "Abgeschlossen" anzeigt.

Hinweis: Um sicherzustellen, dass Events im Produkt ordnungsgemäß funktionieren, wählen Sie Audit-Generierung für Events aus der Liste der Migrationsobjekte aus. Audit-Generierung für Events erstellt Baseline-Audit-Datensätze.

Bestätigen der Versionen der Migrationsdatenbank

Sie bestätigen die Versionen der Migrationsdatenbank, indem Sie die Datenbankverbindung testen. Wenn Sie das Migrationshilfsprogramm das erste Mal ausführen, wird das Dialogfeld für die Konfiguration des CA APM-Migrationshilfsprogramms automatisch geöffnet. Die Dialogfelder werden mit den Einstellungen der Datenbankkonfiguration aufgefüllt, die Sie während der Version 12.8-Installation angegeben haben.

Hinweis: Nachdem Sie die Versionen der Migrationsdatenbank bestätigt haben, klicken Sie im Fenster des Migrationshilfsprogramms auf "Konfigurieren".

Wenn Sie die Datenbankverbindungen testen, entdeckt das Migrationshilfsprogramm die Produkt-Release-Version, *aus* der Sie Daten migrieren, und die Release-Version, *in* die Sie die Daten migrieren. Das Hilfsprogramm füllt die Felder "From Version" (Aus Version) und "To Version" (In Version) im Dialogfeld mit den erkannten Produkt-Release-Versionen auf. Sie können die Release-Versionen nicht im Dialogfeld ändern.

Der erkannte Wert in "Quellversion" muss Version 11.3.4 sein, und "Zielversion" muss Version 12.8 sein. Wenn das Migrationshilfsprogramm eine andere Release-Version entdeckt, können Sie nicht mit der Migration fortfahren.

Gehen Sie wie folgt vor:

1. Geben Sie das Datenbankkennwort ein.
2. Klicken Sie auf "Test Connection" (Verbindung testen).
Eine Bestätigungsmeldung zeigt an, dass der Verbindungstest entweder erfolgreich war oder fehlgeschlagen ist.
3. Klicken Sie im Konfigurationsdialogfeld des CA APM-Migrationshilfsprogramms auf "Speichern", wenn die Bestätigungsmeldung anzeigt, dass der Verbindungstest erfolgreich war.
Das Dialogfeld wird geschlossen.
4. Wenn die Bestätigungsmeldung anzeigt, dass der Datenbankverbindungstest fehlgeschlagen ist, ermitteln Sie, warum das Migrationshilfsprogramm nicht an die Datenbankkonfiguration angeschlossen werden konnte. Nachdem Sie das Problem gelöst haben, wiederholen Sie den Verbindungstest.

Hinweis: Wenn die Produkt-Release-Versionen im Konfigurationsdialogfeld des CA APM- Migrationshilfsprogramms nicht mit den Release-Versionen übereinstimmen, mit denen Sie das Migrationshilfsprogramm verbinden möchten, dann schlägt der Datenbankverbindungstest fehl. Sie können nicht mit der Migration fortfahren.

Wenn Sie die Konfigurationseinstellungen der Datenbank zu einem späteren Zeitpunkt ändern möchten, lesen Sie den Abschnitt [Konfigurieren der Überwachungsdatenbank](#) (siehe Seite 86).

Konfigurieren der Überwachungsdatenbank

Sie müssen die Migrationsdatenbank während der Migration nicht konfigurieren. Die Datenbank wird für die Einstellungen konfiguriert, die während der Version 12.8-Installation angegeben wurden.

Wenn Sie den Speicherort der CA MDB ändern, müssen Sie die Migrationsdatenbank auf den neuen Speicherort konfigurieren, bevor Sie das Migrationshilfsprogramm ausführen.

Gehen Sie wie folgt vor:

1. Klicken Sie im Fenster des Migrationshilfsprogramms auf "Konfigurieren".
2. Geben Sie die Konfigurationseinstellungen ein.
3. Klicken Sie auf "Test Connection" (Verbindung testen).
Eine Bestätigungsmeldung zeigt an, dass der Verbindungstest entweder erfolgreich war oder fehlgeschlagen ist.

4. Klicken Sie im Konfigurationsdialogfeld des CA APM-Migrationshilfsprogramms auf "Speichern", wenn die Bestätigungsmeldung anzeigt, dass der Verbindungstest erfolgreich war.

Das Konfigurationsdialogfeld des CA APM- Migrationshilfsprogramms wird geschlossen.

5. Wenn die Bestätigungsmeldung anzeigt, dass der Datenbankverbindungstest fehlgeschlagen ist, ermitteln Sie, warum das Migrationshilfsprogramm nicht an die Datenbankkonfiguration angeschlossen werden konnte. Nachdem Sie das Problem gelöst haben, wiederholen Sie den Verbindungstest.

Ausführen der Objektmigrationen

Wichtig: Zusätzlich zu den Services und den geplanten Tasks, die unter [Voraussetzungen](#) (siehe Seite 67) angegeben sind, sollten Sie sicherstellen, dass die Version 12.8-Services nicht ausgeführt werden, bevor Sie das Migrationshilfsprogramm ausführen.

Das Fenster des CA APM-Migrationshilfsprogramms listet die Migrationsobjekte in einer hierarchischen Struktur im CA APM-Objektbereich auf. Sie wählen die Objekte aus, die Sie migrieren möchten. Sie können die Daten in Phasen migrieren. Die hierarchische Struktur ermöglicht es Ihnen, alle Objekte innerhalb einer Hierarchieebene auszuwählen oder individuelle Objekte innerhalb einer Ebene auszuwählen.

Wenn Sie ein Objekt auswählen, das migriert werden soll, werden auch alle Objekte innerhalb der Hierarchie dieses Objekts ausgewählt. Diese Objekte werden sekundäre Objekte genannt. Die sekundären Objekte innerhalb der Hierarchie werden zuerst migrieren, und das oberste Objekt, das Sie ausgewählt haben, wird als letztes migriert. Wenn Sie zum Beispiel "Cost and Payments" (Kosten und Zahlungen) als oberstes Objekt auswählen, werden auch die sekundären Objekte "Abrechnungscode", "Preiserhebungstyp" und "Kostentyp" innerhalb der Objekthierarchie "Kosten" und "Zahlung" ausgewählt. Erweitern Sie das oberste Objekt, um die entsprechenden sekundären Objekte anzuzeigen. Während der Migration werden "Abrechnungscode", "Preiserhebungstyp" und "Kostentyp" zuerst migriert. Das Objekt auf oberster Ebene, "Cost and Payments" (Kosten und Zahlungen), wird nach seinen sekundären Objekten migriert.

Sie können die Kontrollkästchen neben den Objekten, die Sie nicht migrieren möchten, deaktivieren. Sie können ein Objekt, eine Gruppe von Objekten oder alle Objekte zur Migration auswählen.

Objekte, die bereits migriert wurden, haben den Status "Abgeschlossen", und ihre Kontrollkästchen sind deaktiviert. Auf diese Weise verhindert das Migrationshilfsprogramm, dass Sie versuchen, ein Objekt zu migrieren, das bereits migriert wurde.

Klicken Sie mit der rechten Maustaste auf ein Objekt, um ausführbare Optionen anzuzeigen. Die Optionen, die verfügbar sind, hängen vom aktuellen Status des Objekts ab. Folgende Beispieloptionen stehen Ihnen zur Verfügung, wenn Sie mit der rechten Maustaste auf ein Objekt klicken:

- Deaktivieren Sie die Kontrollkästchen für die sekundären Objekte
- Move to Completed (In "Abgeschlossen" verschieben)
- Moved to Not Started (In "Nicht gestartet" verschieben)

Das Objekt "Audit-Verlauf" ist anfangs deaktiviert. Sie starten mit der Migration der Nicht-Audit-Objekte. Das Objekt "Audit-Verlauf" ist aktiviert, wenn die Migration erfolgreich ist, und die Audit-Generierung von Events zeigt den Status "Abgeschlossen" an. Sie können die Objekte "Audit-Verlauf" jederzeit migrieren, sobald die Option aktiviert ist und alle Anwendungen und Services wieder online sind.

Wichtig! Abhängig von der Datengröße kann die Migration der Objekte "Audit-Verlauf" viel Zeit in Anspruch nehmen. Wenn der Audit-Verlauf ca. 1 Million Datensätze hat, ist es empfehlenswert, die Migration außerhalb der Hauptgeschäftszeiten durchzuführen.

Gehen Sie wie folgt vor:

1. Aktivieren Sie im Fenster des CA APM-Migrationshilfsprogramms die Kontrollkästchen neben den Objekten, die Sie migrieren möchten.

Hinweis: Um sicherzustellen, dass die Events im Produkt ordnungsgemäß funktionieren, wählen Sie Audit-Generierung für Events aus der Liste der Migrationsobjekte aus. Audit-Generierung für Events erstellt Baseline-Audit-Datensätze.

2. Klicken Sie auf „Starten“

Prüfen Sie die Informationen auf der Registerkarte "Messages" (Meldungen), um den [Migrationsfortschritt zu überwachen](#) (siehe Seite 89).

Wenn die Migration abgeschlossen ist, haben die Objekte im Auswahlbereich des Fensters den Status "Abgeschlossen".

Hinweis: Wenn die Migration fehlschlägt, zeigen Sie die Details in den Protokolldateien der Objektmigration im folgenden Speicherort an:

[ITAM-Stammverzeichnis]\Migration Toolkit\migration-utility\logs

3. (Optional) Wenn die Migration erfolgreich ist, wählen Sie das Objekt "Audit-Verlauf" aus, und wiederholen Sie Schritt 2.
4. Klicken Sie auf "Beenden".

Das Fenster des CA APM- Migrationshilfsprogramms wird geschlossen.

Wenn die Migration abgeschlossen ist, starten Sie die Services für folgende Service Management-Produkte neu:

- CA Service Catalog
- CA Service Desk Manager
- CA Client Automation
- CA APM Version 12.8

Überwachen des Migrationsvorgangs

Die Registerkarte "Messages" (Meldungen) im Fenster des CA APM-Migrationshilfsprogramms zeigt den Fortschritt des aktuellen Migrationsvorgangs an. Sie überwachen den Migrationsvorgang, indem Sie die Meldungen prüfen. Die Meldungen zeigen den sich ändernden Status von allen Objekten, die migriert werden.

Wenn die Migration abgeschlossen ist, können Sie eine Zusammenfassung der erfolgreichen, ausstehenden und fehlgeschlagenen Migrationen auf der Registerkarte "Zusammenfassung" anzeigen. Die Registerkarte "Zusammenfassung" zeigt den Migrationsstatus für alle Migrationen an, die während Ihrer Sitzung ausgeführt wurden.

Sie können die Protokolldateien der Objektmigration im folgenden Speicherort anzeigen:

`[ITAM-Stammverzeichnis]\Migration Toolkit\migration-utility\logs`

Bei Fehlermeldungen, die in den Protokolldateien angezeigt werden, wenden Sie sich an den CA Support.

Ausführen der Post-Migrationsberichte für manuelle Migrationen

Nachdem Sie das Migrationshilfsprogramm ausgeführt haben, führen Sie die Post-Migrationsberichte aus, die Sie während der manuellen Migrationen verwendet haben. Die Post-Migrationsberichte identifizieren Objektdaten, die Sie in Version 12.8 eingeben müssen. Das Hilfsprogramm konnte einige Daten nicht migrieren, da die Funktion, die den Daten zugeordnet ist, geändert wurde.

Gehen Sie wie folgt vor:

1. Klicken Sie im Hauptfenster des CA APM-Migrations-Toolkit auf "Berichterstellung zur Migration".

2. Deaktivieren Sie alle Kontrollkästchen im Bereich der Prä-Migrationsberichte, und wählen Sie folgende Berichte im Bereich der Post-Migrationsberichte aus:

- Fortgeschrittene Suche
- Anhänge
- Basic Search Return Fields (Rückgabefelder der Basissuche)
- Events
- Filter
- Role Security (Rollensicherheit - Feld- und Funktionsberechtigungen)

Hinweis: Wenn Sie nicht alle Typen der Post-Migrationsberichte generieren möchten, wählen Sie nur die gewünschten Berichtstypen aus.

3. Klicken Sie im Bereich des Berichtsausgabeordners auf "Durchsuchen", und wählen Sie den Ausgabeordner aus, in dem Sie die Berichte speichern möchten.

4. Klicken Sie auf "Generate Reports" (Berichte generieren).

Statusmeldungen werden im Meldungsbereich angezeigt, wo Sie den Berichterstellungsprozess überwachen können.

Sie werden aufgefordert, den Berichtsausgabeordner zu öffnen, um die Berichte anzuzeigen.

5. Klicken Sie auf "Ja".

Windows Explorer wird geöffnet. Das Berichterstellungs-Tool erstellt einen Ordner für jedes Kontrollkästchen für Post-Migrationsberichte, das Sie zuvor aktiviert haben.

6. Navigieren Sie zu einem Berichtsordner, und öffnen Sie ihn.

Die Berichte werden im CSV-Format (durch Kommas getrennte Werte) angezeigt.

7. Klicken Sie mit der rechten Maustaste auf einen Bericht, und wählen Sie "Öffnen mit", "Excel" aus, um den Bericht zu öffnen und in einem Tabellenformat anzuzeigen.

Die [Berichtsdaten](#) (siehe Seite 91) werden in einem Tabellenformat dargestellt. Die Tabellenüberschriften sind in der ersten Zeile.

Hinweis: Sie können einen Bericht öffnen und in einem Texteditor im CSV-Format anzeigen.

Migrationsberichtsdaten zur Referenz und Analyse

Das Berichterstellungs-Tool generiert Berichte in CSV-Format, die Sie mit einem Texteditor öffnen können. Die Berichtsfeldnamen und Feldwerte werden durch Kommas getrennt. Sie können auch einen Bericht mit Excel öffnen, wo die Daten in einem Tabellenformat dargestellt werden. Wenn Sie einen Bericht mit Excel öffnen, sind die Feldnamen die Spaltenüberschriften, und die Feldwerte werden in den Zeilen unter den Überschriften angezeigt.

Die Post-Migrationsberichte stellen Informationen zu Daten bereit, die Sie *nach* der Migration in Version 12.8 eingeben. Diese Daten konnten nicht mithilfe des Migrationshilfsprogramms migriert werden.

Folgende Post-Migrationsberichte stellen Informationen bereit, die Sie verwenden, um [manuelle Migrationen auszuführen](#) (siehe Seite 97):

- [Advanced Search Report \(Fortgeschrittener Suchbericht\)](#) (siehe Seite 91)
- [Attachments Report \(Anhangsbericht\)](#) (siehe Seite 92)
- [Basic Search Report \(Basissuchbericht\)](#) (siehe Seite 93)
- [Event Reports \(Event-Berichte\)](#) (siehe Seite 93)
- [Filtering Reports \(Filterberichte\)](#) (siehe Seite 95)
- [Role Security Reports \(Berichte für Rollensicherheit - Feld- und Funktionsberechtigungen\)](#) (siehe Seite 95)

Advanced Search Report (Fortgeschrittener Suchbericht)

Der erweiterte Suchbericht gibt eine Zusammenfassung aller erweiterten Suchen an, und es werden Speicherortinformationen für die [Detailberichte für jede erweiterte Suche](#) (siehe Seite 92) angegeben. Die Detailspalte des Berichts gibt den Speicherort und den Namen von jedem Detailbericht der fortgeschrittenen Suche an.

Folgende Datumsfelder erfordern weitere Erläuterung:

Typ exportieren

Zeigt das Exportformat für die Suchergebnisse an.

Aktualisierungsintervall

Identifiziert die Startzeit und Häufigkeit für einen Exportablaufplan.

Objekttyp

Zeigt den Rollenzugriff an, wenn die Einstellung der Sicherheitssuche eine oder mehrere Rollen hat.

Zuweisung

Identifiziert den Rollennamen oder Kontakt, der Berechtigungen für den Zugriff auf die Suche hat.

Creator (Ersteller)

Identifiziert den Namen des letzten Anwenders, um die Suche zu aktualisieren. Verwenden Sie diese Informationen, um die manuelle Migration (Wiedererstellung) der erweiterten Suche zu delegieren. Sie weisen dieses Feld zu keiner Einstellung in der erweiterten Suche zu.

Creator ID (Ersteller-ID)

Identifiziert den Namen des letzten Anwenders, um die Suche zu aktualisieren. Verwenden Sie diese Informationen, um die manuelle Migration (Wiedererstellung) der erweiterten Suche zu delegieren. Sie weisen dieses Feld zu keiner Einstellung in der erweiterten Suche zu.

Verwenden Sie den erweiterten Suchbericht, um [die erweiterten Suchen manuell auf Version 12.8 zu migrieren](#) (siehe Seite 100).

Detailberichte der fortgeschrittenen Suche

Jeder Detailbericht der fortgeschrittenen Suche identifiziert die Daten für eine erweiterte Suche. Überprüfen Sie die Informationen zu den erweiterten Suchen, die in Version 11.3.4 erstellt wurden.

Verwenden Sie die Detailberichte der fortgeschrittenen Suche, um [diese fortgeschrittenen Suchen manuell auf Version 12.8 zu migrieren](#) (siehe Seite 100).

Attachments Report (Anhangsbericht)

Der Anhangsbericht identifiziert Informationen, die Sie verwenden, um [Dateianhänge manuell zu migrieren](#) (siehe Seite 105). Das Migrationshilfsprogramm migriert die vollständigen Link-Anhänge der Web-URL und die Metadaten für Remote-Server und lokale Dateianhänge. Nach der Migration verschieben Sie die physischen Dateianhänge in den Storage Manager-Service.

Der Anhangsbericht enthält den Dateispeicherort, die Beschreibung und folgende Informationen für jeden Anhang:

UUID

Universell eindeutiger Identifikator identifiziert ein Objekt und unterscheidet zwischen zwei Objekten, die denselben Namen haben.

Objekttyp

Identifiziert den Typ des Objekts, zu dem die Datei angehängt ist.

Zuweisung

Identifiziert den Namen des Objekts, zu dem die Datei angehängt ist.

Basic Search Report (Basissuchbericht)

Verwenden Sie den Basissuchbericht, um folgende Informationen zu Suchen anzuzeigen, die in Version 11.3.4 erstellt wurden, und um [diese Basissuchen manuell auf Version 12.8 zu migrieren](#) (siehe Seite 98):

- Objekttyp, den die Suche zurückgibt.
- Rolle, sofern vorhanden, die die Rückgabefelder der Suche anzeigen darf.
- Rückgabefelder der Suche, die in Version 11.3.4 "Anzeigefelder" genannt wurden.

Event Reports (Event-Berichte)

Der [Bericht des Benachrichtigungsverlaufs-Event](#) (siehe Seite 93) stellt Verlaufsinformationen aus der Version 11.3.4 bereit, die Sie überprüfen können. Folgende Event-Berichte identifizieren Daten, die Sie verwenden, *nachdem* Sie das [Migrationshilfsprogramm](#) (siehe Seite 83) ausgeführt haben, wenn Sie manuelle Migrationen ausführen. Beziehen Sie sich während der [manuellen Migration von Events](#) (siehe Seite 106) auf diese Berichte:

- [Bericht für Event-Datum](#) (siehe Seite 94)
- [Bericht für Überwachungs- und Änderungs-Events](#) (siehe Seite 94)

Bericht für Benachrichtigungsverlaufs-Events

Der Bericht des Benachrichtigungsverlaufs-Events stellt Verlaufsinformationen aus der Version 11.3.4 bereit, die Sie überprüfen können. Keine Aktion erforderlich.

Dieser Bericht identifiziert Events, die im letzten Jahr verarbeitet wurden. Die folgenden Felder bedürfen einer Erklärung:

Event Enabled (Event aktiviert)

Zeigt an, dass das Event aktiviert und nicht inaktiv ist, wenn der Wert "WAHR" ist.
Zeigt an, dass das Event inaktiv ist, wenn der Wert "FALSCH" ist.

Event Field Name (Event-Feldname)

Das Event basiert auf dem Wert dieses Objektfelds.

Event Recipient (Event-Empfänger)

Die E-Mail-Adresse der aktuellen Event-Benachrichtigung.

Event Notification Definition Text (Text der Event-Benachrichtigungsdefinition)

Der E-Mail-Nachrichtentext der aktuellen Event-Benachrichtigung.

Benachrichtigungstyp

Zeigt den Typ der Benachrichtigung an, den der Empfänger erhält. "Initial Event" (Anfangs-Event) zeigt den Empfänger der ersten Benachrichtigung an. "Escalation" (Eskalation) zeigt den Empfänger von nicht bestätigten Benachrichtigungen an.

Benachrichtigungstext

Der E-Mail-Nachrichtentext der letzten Event-Benachrichtigung.

Notification Recipient (Benachrichtigungsempfänger)

Die E-Mail-Adresse der letzten Event-Benachrichtigung.

Das *Implementierungshandbuch* stellt Informationen über Workflow-Provider-Prozessparameter bereit, die in CA Process Automation angegeben sind. Informationen über Benachrichtigungsprozessparameter finden Sie in Ihrer Workflow-Provider-Dokumentation.

Bericht für Event-Datum

Der Bericht für Event-Datum gibt Daten an, die Sie verwenden, *nachdem* Sie das [Migrationshilfsprogramm](#) (siehe Seite 83) ausgeführt haben, wenn Sie manuelle Migrationen ausführen. Dieser Bericht identifiziert Event-Datum und Benachrichtigungen. Beziehen Sie sich während der [manuellen Migration von Events](#) (siehe Seite 106) auf die Berichte.

Das Implementierungshandbuch stellt Informationen über Workflow-Provider-Prozessparameter bereit, die in CA Process Automation angegeben sind. Informationen über Benachrichtigungsprozessparameter finden Sie in Ihrer Workflow-Provider-Dokumentation.

Bericht für Überwachungs- und Änderungs-Events

Der Bericht für Überwachungs- und Änderungs-Events gibt Daten an, die Sie verwenden, *nachdem* Sie das [Migrationshilfsprogramm](#) (siehe Seite 83) ausgeführt haben, wenn Sie manuelle Migrationen ausführen. Dieser Bericht enthält Informationen zu Überwachungs-Events und Benachrichtigungen sowie zu Änderungs-Events und Benachrichtigungen aus Version 11.3.4. Beziehen Sie sich während der [manuellen Migration](#) (siehe Seite 97) auf die Berichte.

Hinweis: Manuelle Events waren in Version 11.3.4 verfügbar, werden jedoch nicht in Version 12.8 unterstützt. Manuelle Events werden nicht im Bericht für Überwachungs- und Änderungs-Events eingeschlossen.

Das Implementierungshandbuch stellt Informationen über Workflow-Provider-Prozessparameter bereit, die in CA Process Automation angegeben sind. Informationen über Benachrichtigungsprozessparameter finden Sie in Ihrer Workflow-Provider-Dokumentation.

Filtering Reports (Filterberichte)

Der Filterbericht gibt eine Zusammenfassung von jedem Filter an, und es werden Speicherortinformationen für die [Detailberichte für jeden Filter](#) (siehe Seite 95) angegeben. Die Detailspalte des Berichts gibt den Speicherort und den Namen von jedem Detailbericht des Filters an.

Detailbericht für Kontaktfiler

Jeder Detailbericht für Filter identifiziert die Daten für einen Filter. Verwenden Sie die Detailberichte für Filter, um die Informationen der Filter anzuzeigen, die in Version 11.3.4 erstellt wurden, und [um Filter manuell zu migrieren](#) (siehe Seite 107).

Role Security Reports (Berichte für Rollensicherheit - Feld- und Funktionsberechtigungen)

Jeder Bericht für Rollensicherheit identifiziert die Daten für eine Sicherheitseinstellung, die mit einem Feld, einer Funktion oder sichtbar mit einem Objekt verbunden ist. Das Migration Toolkit generiert folgende Typen von Berichten für Rollensicherheit:

- **Feldsicherheitsberichte.** Generiert einen Feldsicherheitsbericht für jedes Objekt, das Einstellungen der Rollensicherheit hat. Der Bericht identifiziert die Rolle, das Objekt, das Objektfeld und die Berechtigung für das Feld, die der Rolle zugewiesen ist. Die Berichtsspaltenbezeichnung "Update Permission" (Aktualisierungsberechtigung) und die Berichtsspaltenbezeichnung "Add New Permission" (Neue Berechtigung hinzufügen) beziehen sich auf die Funktion von Version 11.3.4. Version 12.8 unterscheidet nicht zwischen den Berechtigungen für das Aktualisieren und Erstellen von Objekten.
- **Funktionelle Sicherheitsberichte.** Generiert einen funktionellen Sicherheitsbericht für jedes Objekt, das Einstellungen der Rollensicherheit hat. Der Bericht identifiziert die Rolle, das Objekt, die zum Objekt zugehörige Funktion und die Berechtigung für die Funktion, die der Rolle zugewiesen ist.
- **Sichtbare Berichte für Feldsicherheit, die mit einem Objekt verbunden sind.** Generiert einen sichtbaren Bericht für Feldsicherheit, die mit einem Objekt verbunden sind, für jedes Objekt, das Einstellungen der Rollensicherheit hat. Der Bericht identifiziert die Rolle, die Objekte und die zugewiesenen Felder für das Objekt.

Verwenden Sie die Berichte für Rollensicherheit, um die Informationen für die Einstellungen der Rollensicherheit anzuzeigen, die in CA APM Version 11.3.4 erstellt wurden, und um die Einstellungen der Rollensicherheit manuell zu migrieren.

Folgende Objekte, Felder und Funktionen werden nicht in Version 12.8 unterstützt. Sie werden in den Datenbankberichten der Version 11.3.4 nur zur Referenz angezeigt:

- Asset-Version
- Statusverlauf der Asset-Version
- Modellversion

- Schlüsselwörter
- Budget-Manager (Beziehung)
- Kontaktbenutzer (Beziehung)
- Abhängigkeiten (Beziehung)
- Produktentwicklung (Beziehung)
- Produktupdate (Beziehung)
- Supportkontakte (Beziehung)
- Benutzerzuordnung (Beziehung)
- Alle angepassten und anwenderspezifischen Beziehungen
- Kosten (Erweiterte Felder)
- Zahlungen (Erweiterte Felder)
- Beziehungen (Erweiterte Felder)

Starten der CA APM-Webschnittstelle

Sie starten die CA APM-Webschnittstelle, um das auf Version 12.8 aktualisierte Produkt auszuführen und um Daten manuell auf die Version 12.8-Datenbank zu migrieren. Sie müssen die automatischen Migrationen des [Migrationshilfsprogramms](#) (siehe Seite 83) abschließen und die [Post-Migrationsberichte ausführen](#) (siehe Seite 89), *bevor* Sie [manuelle Migrationen ausführen](#) (siehe Seite 97).

Um die Webbenutzeroberfläche zu starten, öffnen Sie einen Web-Browser und geben die folgende URL ein:

`http://servername/itam`

Ersetzen Sie den *Servernamen* durch den Namen des Servers, der die CA APM-Webserver hostet.

Hinweis: Wenn die Sicherheit von Internet Explorer auf "Hoch" gesetzt ist, wird beim Starten der Webbenutzeroberfläche 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.

Auf Ihrem Webserver wird eine Startmenü-Verknüpfung erstellt, die sich auf die URL-Lokation bezieht.

Um sich nach dem Öffnen der URL bei CA APM anzumelden, geben Sie die folgenden Standardanmeldeinformationen ein:

Anwendername

uapmadmin

Kennwort

uapmadmin

Hinweis: In einigen Situationen wird ein Browserfehler oder ein Anwendernamensfehler angezeigt. Sie können diese Fehler lösen, indem Sie den [Fehlersuchanweisungen](#) (siehe Seite 115) folgen.

Ausführen von manuellen Migrationen

Sie können die manuelle Migration von Daten auf Version 12.8 ausführen, nachdem Sie folgende Aufgaben abgeschlossen haben:

- Sie migrieren Daten mithilfe des Migrationshilfsprogramms.
- Sie generieren die Post-Migrationsberichte.

Wenn Sie Daten manuell migrieren, verwenden Sie Version 12.8, um die Daten in die Datenstrukturen der neuen Version einzugeben. Die Migrationsberichte geben die Felder und Werte an, die Sie eingeben.

Wichtig: Beenden Sie das Migrations-Toolkit, und [starten Sie die Webschnittstelle](#) (siehe Seite 96), bevor Sie die manuellen Datenmigrationen ausführen können.

Führen Sie die folgenden manuellen Migrationen aus:

- [Migrieren der Basissuchen](#) (siehe Seite 98)
- [Migrieren der erweiterten Suchen](#) (siehe Seite 100)
- [Migrieren der Dateianhänge](#) (siehe Seite 105)
- [Migrieren der Events](#) (siehe Seite 106)
- [Migrieren der Filter](#) (siehe Seite 107)
- [Migrieren der Rollensicherheit \(Feld- und Funktionsberechtigungen\)](#) (siehe Seite 109)
- [Migrieren der Tasks und Regeln des Hardware-Abgleichs](#) (siehe Seite 112)
- [Migrieren der Übersetzungslisten des Hardware-Abgleichs](#) (siehe Seite 112)
- [Migrieren der Suchen des Hardware-Abgleichs](#) (siehe Seite 113)

Migrieren der Basissuchen

In Version 11.3.4 werden die Rückgabefelder der Suche, die einem Anwender angezeigt werden, in der Sicherheitsfunktion nach der Rolle festgelegt. Version 12.8 erweitert die grundlegende Suchfunktion, sodass sie mehr als erweiterte Suche ausgerichtet ist. Alle Felder sind in der grundlegenden Suche verfügbar. In Version 12.8 legen Sie die Rückgabefelder der Suche fest, die dem Anwender in der Suchfunktion angezeigt werden können. Wenn Sie eine neue Suche erstellen und die konfigurierte Suche speichern, können Sie die Sicherheit auf die Suche anwenden, indem Sie bestimmte Anwenderrollen und Konfigurationen auswählen.

Standardmäßig ist die Sicherheit so festgelegt, dass die von Ihnen erstellten Suchen nur für den Ersteller verfügbar sind. Sie weisen Rollen und Konfigurationen zu Ihren Suchen zu, um den Anwendern, die diesen Rollen und Konfigurationen zugewiesen sind, Zugriff zu gewähren.

Hinweis: Weitere Informationen zur Suche finden Sie im *Benutzerhandbuch*.

Diese Änderungen können nicht mit dem Migrationshilfsprogramm migriert werden. Verwenden Sie während der manuellen Migration die Daten des Basissuchberichts.

Gehen Sie wie folgt vor:

1. Identifizieren Sie den Objekttyp für die Suche auf dem Basissuchbericht.
2. Klicken Sie in CA APM auf die Registerkarte und auf die optionale Unterregisterkarte für das Objekt, das Sie finden möchten.
3. Klicken Sie links auf "Neue Suche".
Das Dialogfeld "Felder hinzufügen" wird angezeigt.
Hinweis: Für einige Objekttypen werden Sie aufgefordert, Vorlagen, Familien oder andere Attribute auszuwählen, um die Suche einzuschränken.
4. Wählen Sie mithilfe der Rückgabefelder der Berichtssuche die Felder aus, die der Suche hinzugefügt werden sollen. In Version 11.3.4 wurden diese Felder als "Display Fields" (Anzeigefelder) bezeichnet.
5. Wählen Sie im Bereich "Feld(er) hinzufügen zu" am unteren Rand des Dialogfelds die Option "Suchkriterien und Suchergebnisse" aus.
6. Klicken Sie auf "OK".
Die Felder werden sowohl zu den Suchkriterien als auch zu den Suchergebnissen hinzugefügt. Das Dialogfeld "Felder hinzufügen" wird geschlossen.
7. Klicken Sie im oberen Bereich der Seite auf SUCHE KONFIGURIEREN: AUS.
Die Konfiguration der Suche ist abgeschlossen.
8. Geben Sie im Bereich "Suchinformationen" den Suchtitel und andere beschreibende Informationen ein, wie z. B. "Kategorie" und "Beschreibung".
9. (Optional) Öffnen Sie den Bereich "Sicherheit suchen".

10. (Optional) Wählen Sie im Bereich "Sicherheit suchen" die Anwenderrollen aus, für die die Suche verfügbar ist.

Hinweis: Wir empfehlen, dass Sie die Anwenderrolle auswählen, die auf dem [Basissuchbericht](#) (siehe Seite 93) identifiziert ist.

11. (Optional) Wählen Sie im Bereich "Sicherheit suchen" die Konfiguration aus, für die die Suche verfügbar ist.

Hinweis: Wenn Sie nicht entweder eine Rolle oder eine Konfiguration auswählen, ist die Suche nur für den Ersteller der Suche verfügbar.

12. Suchen Sie den Bereich "Suchkriterien" und die Kriterienfelder, die Sie eingegeben haben.

13. Geben Sie für jedes Suchkriterienfeld den Feldwert ein. Sie können auf das Suchsymbol klicken, um nach einem Wert zu suchen.

14. (Optional) Öffnen Sie den Bereich "Weitere Einstellungen", und fügen Sie andere Einstellungen hinzu, wie z. B. Sortierungseinstellungen.

15. Klicken Sie auf "Speichern".

Die Suche wird gespeichert.

16. Wenn Sie Anwenderrollen im Bereich "Sicherheit suchen" ausgewählt haben, führen Sie folgende Schritte für jede Rolle aus:

- a. Klicken Sie auf "Verwaltung", "Anwender-/Rollenverwaltung".
- b. Erweitern Sie das Menü "Rollenverwaltung" links.
- c. Klicken Sie auf "Rollensuche".
- d. Suchen Sie eine Rolle, und wählen Sie die Rolle aus.
Die Rollendetails werden angezeigt.
- e. Klicken Sie im Bereich "Standardsuchen" auf "Neue Auswahl".
- f. Suchen Sie nach der Suche, die Sie gerade erstellt haben.
- g. Weisen Sie die Suche als Standardsuche für die Rolle zu.
- h. Klicken Sie auf "Speichern".

Die aktualisierte Rolle ist gespeichert.

Migrieren der erweiterten Suchen

In CA APM Version 11.3.4 werden die Rückgabefelder der Suche, die einem Anwender angezeigt werden, in der Sicherheitsfunktion nach der Rolle festgelegt. In Version 12.8 unterstützen Suchen eine hinzugefügte Sicherheitsebene. Sie legen die Rückgabefelder der Suche fest, die dem Anwender in der Suchfunktion angezeigt werden können. Wenn Sie die konfigurierte Suche speichern, können Sie Sicherheit auf die Suche anwenden, indem Sie bestimmte Anwenderrollen und Konfigurationen auswählen.

Standardmäßig ist die Sicherheit so festgelegt, dass die von Ihnen erstellten Suchen nur für den Ersteller verfügbar sind. Sie weisen Rollen und Konfigurationen zu Ihren Suchen zu, um den Anwendern, die diesen Rollen und Konfigurationen zugewiesen sind, Zugriff zu gewähren.

Hinweis: Weitere Informationen zur Suche finden Sie im *Benutzerhandbuch*.

Diese Änderungen können nicht mit dem Migrationshilfsprogramm migriert werden.

Wenn Sie "Fortgeschrittene Suche" migrieren, führen Sie folgende Schritte aus:

- [Erstellen Sie die fortgeschrittene Suche](#) (siehe Seite 100)
- [Planen Sie eine Suche und exportieren die Ergebnisse](#) (siehe Seite 103)

Erstellen einer fortgeschrittenen Suche

Verwenden Sie während der manuellen Migration Daten aus dem [fortgeschrittenen Suchbericht](#) (siehe Seite 91) und aus dem [Detailbericht der fortgeschrittenen Suche](#) (siehe Seite 92).

Gehen Sie wie folgt vor:

1. Identifizieren Sie den Objekttyp für die Suche nach dem Detailbericht der fortgeschrittenen Suche.
2. Klicken Sie in CA APM auf die Registerkarte und auf die optionale Unterregisterkarte für das Objekt, das Sie finden möchten.
3. Klicken Sie links auf "Neue Suche".

Das Dialogfeld "Felder hinzufügen" wird angezeigt.

Hinweis: Für einige Objekttypen werden Sie aufgefordert, Vorlagen, Familien oder andere Attribute auszuwählen, um die Suche einzuschränken.

4. Identifizieren Sie im Detailbericht die Felder, die *sowohl* in den Rückgabefeldern als auch in den Felder der ausgewählten Kriterien sind.
5. Wählen Sie im Dialogfeld "Felder hinzufügen" die gemeinsamen Felder aus, die Sie im Bericht identifiziert haben.

6. Wählen Sie im Bereich "Feld(er) hinzufügen zu" am unteren Rand des Dialogfelds die Option "Suchkriterien und Suchergebnisse" aus.
7. Klicken Sie auf "OK".

Die Felder, die sowohl "Suchkriterien" als auch "Suchergebnisse" sind, werden der Suche hinzugefügt, und das Dialogfeld "Felder hinzufügen" wird geschlossen.
8. Klicken Sie auf "Felder hinzufügen".

Das Dialogfeld "Felder hinzufügen" wird angezeigt.
9. Wählen Sie die Rückgabefelder aus, die im Detailbericht nicht von den Rückgabefeldern und den Feldern der ausgewählten Kriterien gemeinsam verwendet werden.
10. Wählen Sie im Bereich "Feld(er) hinzufügen zu" am unteren Rand des Dialogfelds die Option "Nur Suchergebnisse" aus.
11. Klicken Sie auf "OK".

Die Felder "Nur Suchergebnisse" werden zur Suche hinzugefügt, und das Dialogfeld "Felder hinzufügen" wird geschlossen.
12. Klicken Sie auf "Felder hinzufügen".

Das Dialogfeld "Felder hinzufügen" wird angezeigt.
13. Wählen Sie die Felder der ausgewählten Kriterien aus, die im Detailbericht nicht von den Rückgabefeldern und den Feldern der ausgewählten Kriterien gemeinsam verwendet werden.
14. Wählen Sie im Bereich "Feld(er) hinzufügen zu" am unteren Rand des Dialogfelds die Option "Nur Suchkriterien" aus.
15. Klicken Sie auf "OK".

Die Felder "Nur Suchkriterien" werden zur Suche hinzugefügt, und das Dialogfeld "Felder hinzufügen" wird geschlossen.
16. Klicken Sie im oberen Bereich der Seite auf SUCHE KONFIGURIEREN: AUS.

Die Konfiguration der Suche ist abgeschlossen.
17. Geben Sie im Bereich "Suchinformationen" den Suchtitel und andere beschreibende Informationen aus dem Bericht ein. Zum Beispiel: "Kategorie" und "Beschreibung".

18. (Optional) Erweitern Sie den Bereich "Sicherheit suchen".
19. (Optional) Wählen Sie im Bereich "Sicherheit suchen" die folgenden Schritte aus, um die Anwenderrollen auszuwählen, für die die Suche verfügbar ist:
 - a. Klicken Sie im Bereich "Rollenzugriff" auf "Neue Auswahl".
Das Dialogfeld "Rollensuche" wird geöffnet.
 - b. Geben Sie den Rollennamen ein, der im Zuweisungsfeld im fortgeschrittenen Suchbericht identifiziert ist. "Rollenname" kann der Name einer Rolle oder ein Kontaktname sein.
 - c. Wenn Sie möchten, können Sie eine Beschreibung eingeben.
 - d. Wählen Sie aus, ob inaktive Datensätze in der Suche nach der neuen Rolle aufgenommen werden sollen.
 - e. Klicken Sie auf "Los".
Das Fenster "Suchergebnisse" wird angezeigt.
 - f. Wählen Sie die Rollen oder Kontakte aus, für die die Suche verfügbar ist.
 - g. Klicken Sie auf "OK".
Das Dialogfeld "Rollensuche" wird geschlossen.
20. (Optional) Wählen Sie im Bereich "Sicherheit suchen" die Konfiguration aus, für die die Suche verfügbar ist.
Hinweis: Wenn Sie nicht entweder eine Rolle oder eine Konfiguration auswählen, ist die Suche für alle Anwender und Konfigurationen verfügbar.
21. Suchen Sie den Bereich "Suchkriterien" und die Kriterienfelder, die Sie ausgewählt haben.
22. Klicken Sie auf "Erweitert".
Der erweiterte Bereich "Suchkriterien" wird geöffnet.
23. Führen Sie für jedes Suchkriterien die folgenden Schritte aus:
 - a. Klicken Sie neben einem Suchkriterium auf das Symbol "Datensatz bearbeiten".
 - b. Suchen Sie die Kriterieninformationen zum Bericht.
 - c. Geben Sie den Operator, den Wert, den Connector und die Klammern, wie im Detailbericht angezeigt, ein.

d. Klicken Sie auf das Symbol "Datensatzbearbeitung abschließen".

24. (Optional) Öffnen Sie den Bereich "Weitere Einstellungen", und fügen Sie andere Sucheinstellungen hinzu, wie z. B. Sortieren.

Hinweis: Wählen Sie im Bereich "Suchergebnisse sortieren" die Werte "Ausgewähltes Feld" und "Sortierrichtung" aus, wie im Sortierrichtungsbereich des Detailberichts identifiziert.

25. Klicken Sie auf "Speichern".

Die fortgeschrittene Suche wird gespeichert.

Planen Sie eine Suche und exportieren die Ergebnisse

Sie können eine Suche planen, um die Suchergebnisse periodisch zu bearbeiten und in eine CSV-Datei oder eine Datenbankansicht zu exportieren.

Gehen Sie wie folgt vor:

1. Klicken Sie in CA APM auf die Registerkarte und auf die optionale Unterregisterkarte für das Objekt, das Sie finden möchten.
2. Klicken Sie im linken Bereich auf "Suchen verwalten".
3. Suchen Sie nach der Suche, und wählen Sie die Suche aus, die Sie gespeichert haben.
4. Klicken Sie links auf "Neuer Export".
5. Geben Sie die grundlegenden Exportinformationen ein, die auf den Exportinformationen des Detailberichts basieren.
6. Die folgenden Felder bedürfen einer Erklärung:

Exportname

Gibt den Exportnamen an.

Exportformat

Gibt das Format für die exportierten Suchergebnisse an.

Name anzeigen

Gibt den Anzeigenamen der Datenbank an.

Hinweis: Der Anzeigename ist erforderlich, wenn Sie die Datenbankansicht als das Export-Format auswählen. Der Name muss ein gültiger Datenbankansichtsname sein.

Beschreibung

Gibt eine Beschreibung für die exportierten Suchergebnisse an.

Aufbewahrungsdauer in Tagen

Gibt an, wie lange die exportierten Suchergebnisse beibehalten werden, bevor die Ergebnisse verworfen werden.

Ordnername

Gibt den Ordner für die exportierten CSV-Datei-Suchergebnisse an.

Läuft nie ab

Gibt an, dass die CSV-Datei oder die Datenbankansicht niemals bereinigt wird.

7. Planen Sie die Suche im Bereich "Exportplan". Verwenden Sie den Wert "Aktualisierungsintervall" des Detailberichts, um die Suche zu planen.

Die folgenden Felder bedürfen einer Erklärung:

RunTime

Gibt die Tageszeit an, um die Suche in der lokalen Zeitzone auf dem CA APM-Anwendungsserver durchzuführen.

Intervalltyp

Gibt den Intervalltyp für die Suche an, zum Beispiel "Tag", "Monat", "Quartal", "Woche" oder "Jahr".

Intervalltag

Gibt den Tag während des Intervalls an, um die Suche durchzuführen. Wenn der Intervalltyp zum Beispiel "Monat" und der Intervalltyp "1" ist, wird der Suchvorgang am ersten Tag des Monats durchgeführt.

Erstes Ausführungsdatum

Gibt das Datum an, an dem die erste Suche durchgeführt wird.

Intervall

Gibt an, wie oft die Suche basierend auf dem ausgewählten Intervalltyp durchgeführt wird. Wenn der Intervalltyp zum Beispiel wöchentlich ist und das Intervall 2 beträgt, erfolgt der Suchvorgang alle zwei Wochen.

Letzter Tag des Intervalls

Gibt an, dass der Suchvorgang am letzten Tag des Intervalltyps durchgeführt wird.

8. Geben Sie an, ob alle der Suche zugewiesenen Rollen und Konfigurationen die exportierten Suchergebnisse bekommen.
9. Klicken Sie auf "Speichern".

Die Suche wird gespeichert. Die Suchvorgänge zur geplanten Zeit und die Suchergebnisse werden exportiert.

Migrieren von Anhängen

In Version 12.8 verarbeitet der Storage Manager-Service alle Dateianhänge. Sie können zwei Typen von Anhängen angeben:

- **Web-URL-Verknüpfung.** Bietet direkten Zugriff auf die in der URL angegebene Seite. Wenn Sie diesen Typ von Anhang hinzufügen, müssen Sie das Präfix "*http://*" einschließen, damit die Verknüpfung richtig funktioniert.
- **Dateipfad.** Gibt direkten Zugriff auf eine Datei an. Die Datei wird mithilfe des Standardprogramms für den Dateityp geöffnet. Zum Zeitpunkt, an dem Sie diesen Anhangstyp erstellen, wird die Datei von Ihrem Dateisystem in das Dateisystem auf einem CA APM-Server kopiert.

Hinweis: Wenn Sie mehrere Anhänge hinzufügen (zu einem Objekt oder zu verschiedenen Objekten), müssen der Name und der Dateipfad oder die URL für jeden Anhang für alle Objekte eindeutig sein.

In Version 11.3.4 wurden Dateianhänge in einem gemeinsamen Freigabeordner gespeichert.

Das Migrationshilfsprogramm migriert die vollständigen Link-Anhänge der Web-URL und die Metadaten für Remote-Server und lokale Dateianhänge. Die Metadaten enthalten die Beschreibungsinformationen des Anhangs und die Speicherortinformationen des Dateipfads. Das Migrationshilfsprogramm ändert den Speicherort des Dateipfads zum Storage Manager-Service. Nach der Migration verschieben Sie die physischen Dateianhänge in den Storage Manager-Service.

Nachdem Sie das Migrationshilfsprogramm ausgeführt haben, kopieren Sie die Dateianhänge der Version 11.3.4 aus dem Freigabeordner und Ihrem lokalen Server in den Version 12.8 Storage Manager-Service. Link-Anhänge der Web-URL werden vom Migrationshilfsprogramm migriert.

Hinweis: Weitere Informationen zu Dateianhängen finden Sie im *Benutzerhandbuch*.

Verwenden Sie während der manuellen Migration die Daten des [Anhangsberichts](#). (siehe Seite 92)

Gehen Sie wie folgt vor:

1. Navigieren Sie zum Speicherort der Dateianhänge, die im Bericht identifiziert ist.
2. Kopieren Sie den Dateianhang, und fügen Sie ihn in den folgenden Speicherort im Storage Manager-Service auf dem Anwendungsserver ein:
 - `[ITAM-Stammverzeichnis]\Storage\Common Store\Attachment\attachment.extn`

Ersetzen Sie *attachment.extn* durch den Anhangsdateinamen und die Erweiterung.

Geben Sie den vollständigen Pfad zum Dateianhang ein, zum Beispiel:

C:\Programme(x86)\ITAM\Storage\Common Store\Attachment\legaldoc1.docx

3. Wiederholen Sie diese Schritte für jeden Remote-Server oder für jeden lokalen Dateianhang im Bericht.

Hinweis: Dateien, die nicht in den Speicherort des Storage Manager-Computers verschoben werden, sind im Produkt nicht verfügbar.

4. Wenn Sie einen Anhang aus dem Remote-Server oder von Ihrem lokalen Rechner jedoch nicht von CA APM gelöscht haben, migriert das Migrationshilfsprogramm die Metadaten für den Anhang. Wenn der Bericht Anhänge identifiziert, die physisch nicht mehr vorhanden sind, verwenden Sie Version 12.8, um die Metadaten des Anhangs zu löschen.

Migrieren der Events

Sie können die Benutzeroberfläche verwenden, um Datum, Änderung und Überwachungs-Events zu definieren. Sie können Benachrichtigungen mithilfe eines hartcodierten Textes und mithilfe der CA APM-Objektwerte einrichten. Zum Beispiel können Sie angeben, dass der Betreff einer Benachrichtigung die Wörter "Bestätigung benötigt für", gefolgt vom Wert des ID-Objekts des CA APM-Rechtsdokuments beinhaltet. Wenn ein Ereignis auftritt, können E-Mail-Benachrichtigungen an bestimmte Empfänger gesendet werden. Benachrichtigungen, die nicht bestätigt werden, können eskaliert werden.

Verwenden Sie während der manuellen Migration von Events und Benachrichtigungen die Daten des [Berichts für Event-Datum](#) (siehe Seite 94) und die Daten des [Berichts für Überwachungs- und Änderungs-Events](#) (siehe Seite 94).

Gehen Sie wie folgt vor:

1. Befolgen Sie die Anweisungen für das Erstellen von Events und Benachrichtigungen im *Benutzerhandbuch*.
2. Verwenden Sie die Informationen im Bericht für Datumsevent und im Bericht für Überwachungs- und Änderungs-Events, um die Events und Benachrichtigungen zu erstellen.

Hinweis: Das *Implementierungshandbuch* stellt Informationen über Workflow-Provider-Prozessparameter bereit, die Sie in CA Process Automation angeben. Informationen über Benachrichtigungsprozessparameter finden Sie in Ihrer Workflow-Provider-Dokumentation.

Migrieren der Filter

In CA APM Version 11.3.4 werden die Filter, die einem Anwender angezeigt werden, in der Sicherheitsfunktion nach der Rolle festgelegt. In dieser Version unterstützen Filter eine hinzugefügte Sicherheitsebene. Sie legen die Filter fest, die dem Anwender in der Filterfunktion angezeigt werden können. Wenn Sie einen Filter konfigurieren, können Sie Sicherheit auf den Filter anwenden, indem Sie bestimmte Anwenderrollen und Anwender auswählen, die Anzeigeberechtigung für den Filter haben.

Standardmäßig ist die Sicherheit so festgelegt, dass die Filter, die Sie erstellen, für alle Rollen und Anwender verfügbar sind. Wenn Sie eine einzigartige Sicherheit auf Ihre Filter anwenden, können Sie sicherzustellen, dass bestimmte Anwender vertrauliche Informationen in einem Filter nicht anzeigen können.

Diese Änderungen können nicht mit dem Migrationshilfsprogramm migriert werden. Verwenden Sie während der manuellen Migration die Daten des [Detailbericht des Filters](#). (siehe Seite 95)

Gehen Sie wie folgt vor:

1. Identifizieren Sie das Objekt für den Filter im Detailbericht für Filter.
2. Klicken Sie in CA APM auf die Registerkarte "Verwaltung" und auf die Unterregisterkarte "Filterverwaltung".
3. Klicken Sie auf "Neue Filter".
Die Seite "Filterdetails" wird geöffnet.
4. Führen Sie im Bereich "Filterinformationen" die folgenden Schritte aus, indem Sie die Informationen im Detailbericht des Filters verwenden:
 - a. Geben Sie den Filternamen und das Objekt ein, das Sie filtern möchten.
 - b. (Optional) Geben Sie eine Beschreibung ein.
 - c. (Optional) Wählen Sie "Filter allen Anwendern zuweisen" aus, wenn Sie möchten, dass alle Anwender die Filterdaten anzeigen können. Wenn Sie Sicherheit auf den Filter anwenden möchten, schließen Sie den Bereich "Filtersicherheit", wie in den folgenden Schritten beschrieben, ab.

5. Führen Sie im Bereich "Filtersicherheit" eine oder mehrere der folgenden Aktionen aus:
 - Um Rollen einzugeben, die den Filter sehen können:
 - Klicken im Bereich "Rollen" auf "Neue Auswahl".
Das Dialogfeld "Rollensuche" wird geöffnet.
 - Suchen Sie nach Rollen, und wählen Sie die Rollen aus, die den Filter sehen dürfen.
 - Klicken Sie auf "OK".
 - Um Anwender einzugeben, die den Filter sehen können:
 - Klicken im Bereich "Anwender" auf "Neue Auswahl".
Das Suchdialogfeld wird geöffnet.
 - Suchen Sie nach Anwendern, und wählen Sie die Anwender aus, die den Filter sehen dürfen.
 - Klicken Sie auf "OK".
6. Klicken Sie auf "Felder hinzufügen".
Das Dialogfeld "Feld(er) hinzufügen" wird geöffnet.
7. Wählen Sie die Felder aus, die im Bericht unter Abschnitt der Felder der ausgewählten Kriterien angezeigt werden.
8. Klicken Sie auf "OK".
Das Dialogfeld "Feld(er) hinzufügen" wird geschlossen, und die Felder, die Sie ausgewählt haben, werden im Bereich "Filterkriterien" angezeigt.
9. Führen Sie mithilfe der Informationen im Bereich "Kriterien" des Detailberichts die folgenden Schritte für alle Filterkriterien aus:
 - a. Klicken Sie neben einem Suchkriterium auf das Symbol "Filterkriterien".
 - b. Geben Sie den Operator, den Wert, den Connector und die Klammern, wie im Bericht angezeigt, ein.
 - c. Klicken Sie auf das Symbol "Datensatzbearbeitung abschließen".
10. Klicken Sie auf "Speichern".
Der Filter wird gespeichert.

Migrieren der Rollensicherheit

Das Migrationshilfsprogramm migriert Anwenderrollen jedoch nicht die Rollensicherheitseinstellungen. Sie migrieren die Rollensicherheit (Feld, Funktion und sichtbar mit Objektberechtigungen verbunden) manuell.

Eine Anwenderrolle ist der primäre Datensatz für die Überwachung der Sicherheit und Benutzeroberflächennavigation. Jede Rolle definiert eine Detailansicht des Produkts, indem nur die Funktionen angezeigt werden, die die Anwender zum Ausführen der Aufgaben benötigen, die gewöhnlich ihrer Rolle in der Geschäftsorganisation zugewiesen sind. Die Standardrolle für einen Anwender bestimmt zusammen mit der Konfiguration der Benutzeroberfläche, was der Anwender nach der Anmeldung sieht. Ein Anwender kann nur einer einzelnen Rolle angehören.

Sie konfigurieren Anwenderrollen, um Berechtigungen für den Zugriff auf das Repository auf funktioneller Ebene und auf Feldebene zuzuweisen. Sie können die erforderliche Zugriffsebene für jede Rolle festlegen und zuweisen. Durch die Rollenzuweisung wird verhindert, dass Anwender nicht autorisierte Aufgaben durchführen, z. B. Daten hinzufügen oder löschen.

Feldsicherheit definiert die Rollenberechtigungen für ein Objektfeld, zum Beispiel volle Kontrolle. Funktionssicherheit definiert die Rollenberechtigungen für Funktionen auf einem Objekt, zum Beispiel Kopieren eines Asset. Sichtbar verbundene Objektsicherheit definiert die Felder für das Objekt.

Sie erstellen die Einstellungen der Sicherheitsberechtigung für ein Objekt in den lokalen Konfigurationen des Objekts. Anschließend ordnen Sie eine der Objektkonfigurationen zu einer Rolle zu. Die Feld- und Funktionssicherheitsberechtigungen für eine Rolle werden von den Objektkonfigurationen bestimmt, die dieser Rolle zugewiesen sind. Die Objektkonfiguration für jede Rolle wird auf die [Berichte für Rollensicherheit](#) (siehe Seite 95) für das Objekt identifiziert.

Sie führen folgende manuelle Migrationen aus, um Rollensicherheit zu migrieren:

- [Migrieren der Rollenfeldsicherheit](#) (siehe Seite 109)
- [Migrieren der Rollenfunktionssicherheit](#) (siehe Seite 110)
- [Migrieren der Rolle, die sichtbar mit Objektsicherheit verbunden ist](#) (siehe Seite 111)

Verwenden Sie die Informationen in den [Berichten für Rollensicherheit](#) (siehe Seite 95), um Rollenfeldsicherheit, Rollenfunktionssicherheit und Rollen, die sichtbar mit Feldsicherheit verbunden sind, manuell zu migrieren.

Migrieren der Rollenfeldsicherheit

Verwenden Sie die Informationen in den [Berichten für Rollensicherheit](#), (siehe Seite 95) um Rollenfeldsicherheit manuell zu migrieren.

Gehen Sie wie folgt vor:

1. Für Berechtigungen der Rollenfeldsicherheit, suchen Sie im Feldsicherheitsbericht für das Objekt ein Feld und die Rollenberechtigung für das Feld.

Erstellen Sie eine lokale Konfiguration, und benennen Sie sie für das Objektfeld. Folgende Konfigurationen der Feldsicherheit sind verfügbar:

- **Vollständige Steuerung.** Das Feld kann von der Rolle bearbeitet werden.
- **Verborgen.** In der Anwenderoberfläche ausgeblendet und für die Rolle entfernt.
- **Schreibgeschützt.** Das Feld ist für die Rolle schreibgeschützt.

Hinweis: Weitere Informationen über die Konfiguration der Benutzeroberfläche finden Sie im *Administrationshandbuch*.

Migrieren der Rollenfunktionssicherheit

Verwenden Sie die Informationen in den [Berichten für Rollensicherheit](#), (siehe Seite 95) um Rollenfunktionssicherheit manuell zu migrieren.

Gehen Sie wie folgt vor:

1. Für Berechtigungen der Rollenfunktionssicherheit, suchen Sie im Funktionssicherheitsbericht für das Objekt eine Funktion und die Rollenberechtigung für die Funktion.

Erstellen Sie eine lokale Konfiguration, und benennen Sie sie für die Objektfunktion. Konfigurationen der Funktionssicherheit können eine von vielen Funktionen sein, zum Beispiel die Anwenderberechtigung zur Änderung des Asset-Modells. Konfigurationen der Funktionssicherheit haben die Berechtigung "Gewährte Berechtigungen" oder "Abgelehnte Berechtigungen".

Hinweis: Weitere Informationen über die Konfiguration der Benutzeroberfläche finden Sie im *Administrationshandbuch*.

2. Speichern Sie die Objektkonfiguration.
3. Klicken Sie auf "Verwaltung", "Anwender-/Rollenverwaltung".
4. Erweitern Sie auf der linken Seite den Bereich "Rollenverwaltung".
5. Klicken Sie auf "Rollensuche".
6. Suchen Sie nach der Rolle, die im Sicherheitsbericht angegeben ist.
7. Klicken Sie auf den Link des Rollennamens im Rückgabebereich der Suche.

Das Bereich "Standardinformationen" wird geöffnet.

8. Klicken Sie links auf "Rollenkonfiguration".
Der Bereich "Rollenkonfiguration" wird angezeigt.
9. Klicken Sie auf "Neue Auswahl".
Die Liste der gespeicherten Konfigurationen wird angezeigt.
10. Wählen Sie die Objektkonfiguration aus, die Sie der Rolle zuweisen möchten.
11. Klicken Sie auf "OK".
Die Objektkonfiguration wird der Rolle zugewiesen.

Migrieren der Rolle, die sichtbar mit Objektsicherheit verbunden ist

Verwenden Sie die Informationen in den [Berichten für Rollensicherheit](#) (siehe Seite 95), um die Rolle, die sichtbar mit der Objektsicherheit verbunden ist, manuell zu migrieren.

Gehen Sie wie folgt vor:

1. Für die Rolle, die sichtbar mit Objektsicherheitsberechtigungen verbunden ist, suchen Sie in den sichtbaren Berichten für Feldsicherheit, die mit einem Objekt verbunden sind, ein verbundenes Objekt und die Rolle für das Objekt.
2. Erstellen Sie eine lokale Konfiguration, und benennen Sie sie für das Objekt. Verknüpfen Sie die Felder, die als "Zugeordnete Felder" für das Objekt im Bericht definiert sind.
3. Speichern Sie die Objektkonfiguration.
4. Klicken Sie auf "Verwaltung", "Anwender-/Rollenverwaltung".
5. Erweitern Sie auf der linken Seite den Bereich "Rollenverwaltung".
6. Klicken Sie auf "Rollensuche".
7. Suchen Sie nach der Rolle, die im Sicherheitsbericht angegeben ist.
8. Klicken Sie auf den Link des Rollennamens im Rückgabebereich der Suche.
Das Bereich "Standardinformationen" wird geöffnet.
9. Klicken Sie links auf "Rollenkonfiguration".
10. Klicken Sie auf "Neue Auswahl".
11. Wählen Sie die Objektkonfiguration aus, die Sie der Rolle zuweisen möchten, und klicken Sie auf "OK".

Die Objektkonfiguration wird der Rolle zugewiesen. Wiederholen Sie die Schritte für jede Rolle im Bericht.

Migrieren der Tasks und Regeln des Hardware-Abgleichs

Der Hardware-Abgleichsvorgang umfasst folgende Schritte:

1. Richten Sie Datennormalisierungsregeln ein, um Datenwerte zwischen Discovery-Repositorys und dem Produkt zuzuordnen.
2. Definieren Sie eine Abgleichsregel, um die Verarbeitung von Daten einzuschränken und um anzugeben, wie gefundene Datensätze verarbeitet werden sollen.

Hinweis: Die Abgleichsregeln in diesem Schritt ersetzen die Abgleichstasks in Version 11.3.4. Während der manuellen Migration erstellen Sie Abgleichsregeln, die auf Tasks in Version 11.3.4 vom [Bericht "Abfrage des Haupt-Task"](#) (siehe Seite 81) und vom [Bericht "Task zum Hinzufügen eines Asset"](#) (siehe Seite 81) basieren.

3. (Optional) Definieren Sie Optionen für die Abgleichsaktualisierung, um die verwalteten Asset-Felder anzugeben, die die Hardware-Abgleichs-Engine automatisch mit den Änderungen aktualisieren soll, die in den durch Discovery ermittelten Assets festgestellt wurden.
4. Definieren Sie Asset-Zuordnungskriterien, um verwaltete und durch Discovery ermittelte Assets für eine Abgleichsregel zuzuordnen.
5. Zeigen Sie die Ergebnisse des Abgleichs in der Nachrichtenwarteschlange an.

Verwenden Sie den [Bericht "Abfrage des Haupt-Task"](#) (siehe Seite 81) und den [Bericht "Task zum Hinzufügen eines Asset"](#) (siehe Seite 81) während der manuellen Migration von Aufgaben in Abgleichsregeln.

Gehen Sie wie folgt vor:

1. Befolgen Sie die Anweisungen zum Definieren von Abgleichsregeln im Abschnitt "Definieren einer Abgleichsregel" des *Administrationshandbuchs*.
2. Verwenden Sie die Informationen im Bericht "Abfrage des Haupt-Task" und im Bericht "Task zum Hinzufügen eines Asset", um Abgleichsregeln zu erstellen.

Migrieren der Übersetzungslisten des Hardware-Abgleichs

Wenn Sie es vorziehen, Übersetzungslisten des Hardware-Abgleichs *nicht* mithilfe des Migrationshilfsprogramms zu migrieren, dann migrieren Sie die Listen manuell. Sie analysieren den [Abfragebericht der Hauptübersetzungslisten](#) (siehe Seite 80), um diese Entscheidung zu treffen.

Version 12.8 ersetzt mehrere Übersetzungslisten des gleichen Typs mit Normalisierungsregeln für Modell, Hersteller und Betriebssystem.

Verwenden Sie die Daten des [Abfrageberichts der Hauptübersetzungslisten](#) (siehe Seite 80) während der manuellen Migration von Übersetzungslisten in Normalisierungsregeln.

Gehen Sie wie folgt vor:

1. Befolgen Sie die Anweisungen für das Erstellen von Normalisierungsregeln im Abschnitt "Datennormalisierung" des *Administrationshandbuchs*.
2. Verwenden Sie die Informationen im Abfragebericht der Hauptübersetzungslisten, um die Normalisierungsregeln zu erstellen.

Hinweis: Führen Sie alle Listen des gleichen Typs zusammen, entfernen Sie duplizierte Einträge, und migrieren Sie die kombinierte Liste in die entsprechenden Normalisierungsregeln.

Migrieren von fehlenden Einträgen aus den Übersetzungslisten des Hardware-Abgleichs

Die Berichte über unkonvertierte Übersetzungslisten identifizieren die Legacy-Übersetzungslisten des Hardware-Abgleichs von CA APM Version 11.3.4, die fehlende oder ungültige Einträge enthalten, die nicht in Version 12.8 migriert sind. Die Übersetzungsliste sind migriert, jedoch sind einige Einträge in der Liste nicht migriert, da in der Legacy-Datenbank keine unterstützenden Daten vorhanden sind.

Das Produkt ersetzt mehrere Übersetzungslisten des gleichen Typs mit Normalisierungsregeln für Modell, Hersteller und Betriebssystem.

Verwenden Sie Daten aus dem [Bericht über unkonvertierte Übersetzungslisten](#) (siehe Seite 81) und aus dem [Abfragebericht der Hauptübersetzungsliste](#) (siehe Seite 80), um fehlende Einträge in den Legacy-Übersetzungslisten zu Version 12.8-Normalisierungsregeln hinzuzufügen.

Gehen Sie wie folgt vor:

1. Befolgen Sie die Anweisungen für das Aktualisieren von Normalisierungsregeln im Abschnitt "Datennormalisierung" des *Administrationshandbuchs*.
2. Verwenden Sie die Informationen im [Bericht über unkonvertierte Übersetzungslisten](#) (siehe Seite 81), um die Normalisierungsregeln in Version 12.8 mit den fehlenden Einträgen, die im Bericht identifiziert sind, zu aktualisieren.

Hinweis: Führen Sie alle Listen des gleichen Typs zusammen, entfernen Sie duplizierte Einträge, und migrieren Sie die kombinierte Liste in die entsprechenden Normalisierungsregeln.

Migrieren der Suchen des Hardware-Abgleichs

Sie migrieren die anwenderspezifischen Suchen des Hardware-Abgleichs von CA APM Version 11.3.4 in Version 12.8-Berichte für den Hardware-Abgleich. Das Produkt gibt vordefinierte Berichte für den Hardware-Abgleich an, die von der CA Business Intelligence-Software generiert wurden. Sie können diese Berichte mithilfe der bereitgestellten CA Business Intelligence anpassen.

Berichte für den Hardware-Abgleich geben folgende Informationen an:

- Verwaltete Assets, die auf ein durch Discovery ermitteltes Asset abgestimmt worden sind, einschließlich durch Discovery ermittelter Inventar- und Netzwerk-Discovery-Datensätze.
- Abgerechnete Assets (ein aktives oder empfangenes Asset, das einen zulässigen Rechnungscode hat), die mit keinem Discovery-Datensatz übereinstimmen.
- Durch Discovery ermittelte Assets, die auf kein verwaltetes Asset abgestimmt sind.
- Durch Discovery ermittelte Assets, die auf Grund fehlender oder ungültiger Daten nicht bearbeitet wurden.
- Anzahl des aktuellen Discovery-Datenvolumens.
- Verwaltete Assets, die mit Discovery-Datensätzen übereinstimmen.
- Verwaltete Assets, die nicht mit Discovery-Datensätzen übereinstimmen.
- Übereinstimmungen zwischen Netzwerk-Discovery-Daten und Agent-Discovery-Daten.
- Potenzielle entgangene Umsätze, einschließlich Assets, die ermittelt, aber nicht in Rechnung gestellt wurden. Dieser Bericht stellt Umsatzchancen dar, basierend auf der Anzahl von Assets, die in Rechnung gestellt werden. Verwenden Sie die Informationen in diesem Bericht, um Beweise zu erhalten, dass ein Asset aktiviert und ermittelt ist.
- Netzwerk-Discovery-Datensätze, die mit keinem entsprechenden durch Discovery ermittelten Inventar übereinstimmen. Netzwerk-Discovery stellt beschränkte Daten zur Identifikation eines Assets im Netzwerk bereit. Discovery gibt detaillierte Hardware- und Softwareinformationen über ein Asset an.

Verwenden Sie die Suchinformationen der Version 11.3.4 im [Bericht "Anwenderspezifische Suche"](#) (siehe Seite 81), um festzustellen, welche Berichte für den Hardware-Abgleich generiert und möglicherweise angepasst werden sollen.

Gehen Sie wie folgt vor:

1. Befolgen Sie die Anweisungen für das Generieren der Berichte für den Hardware-Abgleich im Abschnitt "Berichterstellung" des *Benutzerhandbuchs*.
2. Verwenden Sie die Informationen im Bericht "Anwenderspezifische Suche", um den zugehörigen Bericht für den Hardware-Abgleich zu finden, und geben Sie die Suchkriterien ein.

Hinweis: Um nicht abgestimmte Assets hinzuzufügen, indem Sie die Ergebnisse eines Berichts generieren und exportieren und anschließend die Berichtsergebnisse über Data Importer importieren, befolgen Sie die Anweisungen im Abschnitt "Hinzufügen von Assets aus nicht abgestimmten, durch Discovery ermittelten Datensätzen" des *Administrationshandbuchs*.

Ausführen einer Verifizierung der Post-Migration

Wenn Sie über Integrationen mit CA Service Desk Manager und CA Service Catalog vor der Datenmigration verfügt haben, führen Sie die Verifizierung der Post-Migration dieser Integrationen aus. Sie führen diese Verifizierung aus, nachdem Sie alle Daten auf Version 12.8 migriert haben.

Gehen Sie wie folgt vor:

1. Klicken Sie auf "Ausführen", und führen Sie "services.msc" aus.
2. Wenn der Service "CA Service Desk Manager" nicht ausgeführt wird, wählen Sie den Service aus, und starten Sie den Service.
3. Gehen Sie in das Verzeichnis "CA Service Desk Manager".
4. Wenn der Service "CA Service Desk Manager PDM Tomcat" nicht ausgeführt wird, wählen Sie den Service aus, und starten Sie den Service.
5. Melden Sie sich bei CA Service Catalog an.
6. Gehen Sie auf "Verwaltung", und klicken Sie auf "Konfiguration".
7. Klicken Sie auf den Hyperlink "CA APM-Services".
8. Klicken Sie auf das Bearbeitungssymbol (Bleistift) für den Namen des CA APM-Webservers.
9. Geben Sie den Namen des CA APM-Webservers ein.
10. Klicken Sie auf das Bearbeitungssymbol für die CA APM-Portnummer.
11. Geben Sie folgende Portnummer ein, und klicken Sie auf "Speichern".
12. Melden Sie sich ab, und starten Sie den Service "CA Service View" in "services.msc".

Stellen Sie sicher, dass die CA APM-Integrationen mit CA Service Desk Manager und CA Service Catalog funktionieren.

Fehlerbehebung

Dieser Abschnitt enthält die folgenden Themen:

- [Webserver benannt mit Unterstreichungszeichen](#) (siehe Seite 116)
- [Fehlschlagen der Migration des Audit-Verlaufs](#) (siehe Seite 116)
- [Klassenfehler des Migrationshilfsprogramms](#) (siehe Seite 116)
- [Link des Konfigurators duplizierter Asset-Namen kann nicht gestartet werden](#) (siehe Seite 117)

Webserver benannt mit Unterstreichungszeichen

Symptom:

Die Verwendung von Unterstreichungszeichen in Webserver-Hostnamen führt zu Problemen, wenn Sie sich im Produkt anmelden oder wenn Sie CA EEM für die Anwenderkonfiguration verwenden.

Lösung:

Wenn Sie ein virtuelles oder gehostetes System verwenden, konfigurieren Sie einen neuen Hostnamen, indem Sie ein anderes Image ohne Unterstreichungszeichen erstellen. Fügen Sie für ein Produktionssystem Ihrem internen Domain Name System (DNS) einen Hostnamen hinzu, sodass auf das Produkt mit einer anderen URL zugegriffen werden kann.

Fehlschlagen der Migration des Audit-Verlaufs

Symptom:

Nachdem Sie das Migrationshilfsprogramm ausgeführt haben, zeigt das Statussymbol für Audit-Verlauf "Fehler" an und weist daraufhin, dass die Migration fehlgeschlagen ist, und die Protokolle des Migrationshilfsprogramms zeigen folgende Meldung an:
Die Migration des Audit-Verlaufs wurde aufgrund eines Verlaufsdatenkonflikts mit dem Gruppentrennzeichen abgebrochen. Wenden Sie sich an den CA Support, um ein eindeutiges Gruppentrennzeichen festzulegen.

Lösung:

Wenden Sie sich an den CA Support.

Klassenfehler des Migrationshilfsprogramms

Symptom:

Wenn Sie versuchen, das Migrationshilfsprogramm vom Toolkit oder von der Eingabeaufforderung aus zu starten, erhalten Sie folgende Fehlermeldung:
Die Hauptklasse konnte nicht gefunden werden: com.ca.core.gui.Application

Lösung:

Der Fehler tritt auf, wenn ein falscher Pfad für "KETTLE_HOME" konfiguriert ist. Stellen Sie sicher, dass die Umgebungsvariable "KETTLE_HOME" auf den Pfad von Kettle festgelegt ist, der den Ordner "data-integration" enthält. Zum Beispiel:
C:\Programme\Pentaho\Kettle\.

Link des Konfigurators duplizierter Asset-Namen kann nicht gestartet werden

Gültig unter dem Betriebssystem "Windows 2008" und "Windows 7"

Symptom:

Sie können den Konfigurator duplizierter Asset-Namen mit eingeschalteter UAC (User Access Control) nicht ausführen.

Lösung:

Um den Konfigurator duplizierter Asset-Namen mit eingeschalteter UAC auszuführen, starten Sie die Benutzeroberfläche als Administrator.

- Klicken Sie mit der rechten Maustaste auf "LaunchUI.bat", und klicken Sie auf "Als Administrator ausführen".

Kapitel 6: Implementieren der Mandantenfähigkeit

Dieses Kapitel enthält folgende Themen:

[Mandantenfähigkeit](#) (siehe Seite 119)

[Service Provider](#) (siehe Seite 120)

[Mandantenfähigkeit - Funktionsweise](#) (siehe Seite 120)

[Auswirkung auf die Benutzeroberfläche](#) (siehe Seite 122)

[Implementieren der Mandantenfähigkeit](#) (siehe Seite 123)

[Aktivieren der Mandantenfähigkeit](#) (siehe Seite 124)

[Verwaltung von Mandant, untergeordnetem Mandant und Mandantengruppen](#) (siehe Seite 125)

Mandantenfähigkeit

Mit *Mandantenfähigkeit* können mehrere unabhängige Mandanten (und ihre Anwender) eine einzige Implementierung von CA APM gemeinsam nutzen. Mandanten interagieren miteinander nur auf bestimmte Weise, wie von ihren Rollen und Mandantenhierarchien definiert. Solange kein Zugriff von einer Rolle oder Hierarchie gewährt wird, sieht jeder Mandant die CA APM-Implementierung in der Regel nur für die eigene Verwendung und kann die Daten eines anderen Mandanten nicht aktualisieren oder anzeigen.

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

Mandantenfähigkeit wird während der CA APM-Installation automatisch installiert. Nachdem Sie CA APM installiert haben, folgen Sie den Schritten zur Implementierung der Mandantenfähigkeit in diesem Abschnitt.

Weitere Informationen:

[Implementieren der Mandantenfähigkeit](#) (siehe Seite 123)

Service Provider

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

CA APM verbindet den berechtigten Anwender (normalerweise uapmadmin) mit dem Mandanten "Service Provider".

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

- Erstellen, Bearbeiten oder Löschen von Mandanten
- Zulassen von untergeordneten Mandanten für Mandanten
- Aktualisieren öffentlicher Daten

Hinweis: Der CA APM-Administrator kann Mandantenanwendern auch Zugriff auf Daten von anderen gewähren. Außerdem kann eine Anwenderrolle separaten Schreib- und Lesezugriff auf bestimmte Mandantengruppen für Anwender innerhalb dieser Rolle festlegen. Weitere Informationen zum Erstellen einer Anwenderrolle und Zuweisen einer Rolle zu einem Anwender finden Sie im *Administrationshandbuch*.

Mandantenfähigkeit - Funktionsweise

Wenn Sie [Mandantenfähigkeit](#) (siehe Seite 124) aktivieren, können Sie jedem Kontakt Zugriff auf alle Mandanten (öffentlich), einen einzelnen Mandanten oder eine Gruppe von Mandanten (anwenderdefiniert oder produktverwaltet) gewähren. Die Rolle für einen Kontakt steuert den Zugriff, der den Lese- und Schreibzugriff festlegt.

Hinweis: Weitere Informationen zum Erstellen einer Anwenderrolle und Zuweisen einer Rolle zu einem Anwender finden Sie im *Administrationshandbuch*.

Wenn "Mandantenfähigkeit" aktiviert ist, schließen die meisten CA APM-Objekte ein Mandantenattribut mit ein, das den Mandanten angibt, dem 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, und jeder Anwender kann öffentliche Daten ohne Mandant erstellen und aktualisieren.

Mandant erforderlich

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

Mandant optional

Definiert Objekte mit einem Mandantenattribut, das NULL sein kann. Sie können diese Objekte als Mandantendaten oder öffentliche Daten erstellen. Wenn Sie einen Mandanten in einem Mandanten-Dropdown-Menü auswählen, um ein Objekt zu erstellen, wird das Objekt ein Mandantenobjekt. Wenn Sie jedoch die Option "Öffentliche Daten" in einem Mandanten-Dropdown-Menü auswählen, wird das Objekt ein öffentliches Mandantenobjekt. Anwender, die einer Rolle zugewiesen sind, die nur einen allein stehenden Mandanten darstellt, sehen bei der Dateneingabe keine Mandanten-Dropdown-Liste.

Wenn ein Anwender die Datenbank abfragt, beschränkt das Produkt die Ergebnisse auf Objekte, auf die der Anwender zugreifen darf. Das heißt, dass Sie niemals Daten in Tabellen vom Typ "Mandant erforderlich" sehen können, mit Ausnahme der Daten, die zu Mandanten gehören, auf die Sie Zugriff haben. Wenn die Daten öffentliche Daten über die Mandantenfähigkeit sind, können Sie die Daten in optionalen Mandantentabellen sehen, weil die Daten auch öffentliche Daten sind.

Wenn ein Mandantenanwender das Erstellen oder Aktualisieren eines Datenbankobjekts anfordert, überprüft das Produkt, ob das Objekt einem Mandanten gehört, der die aktuelle Rolle für den Anwender aktualisieren kann. Das Produkt überprüft auch, ob alle Referenzen vom Objekt auf andere Objekte auf öffentliche Objekte (ohne Mandant), auf Objekte vom gleichen Mandanten oder auf Objekte von Mandanten in der Mandantenhierarchie über dem Mandanten für das Objekt erfolgen. Das heißt, ein Mandantenobjekt darf sich auf Objekte beziehen, die sich auf seinen übergeordneten Mandanten beziehen, auf dessen übergeordneten Mandanten usw.

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

Hinweis: Die referenzierte Objektebeschränkung hat eine Ausnahme. Bestimmte Referenzen können Objekte referenzieren, die Mandanten in der Mandantenhierarchie ihres enthaltenden Objekts gehören. Diese Referenzen werden als SERVICE_PROVIDER_ELIGIBLE im CA APM-Objektschema festgelegt. Das Flag SERVICE_PROVIDER_ELIGIBLE wirkt sich nur dann aus, wenn sich der Service Provider-Mandant in der Mandantenhierarchie nicht über dem Mandantenobjekt befindet. Wenn sich der Service Provider-Mandant in der Hierarchie befindet, erlauben die Mandantenvalidierungsregeln das Erstellen von Service Provider-Referenzen.

Ein Service Provider-Anwender, der das Erstellen oder Aktualisieren eines Objekts anfordert, unterliegt den gleichen Beschränkungen wie Mandantenanwender, außer dass es Service Provider-Anwendern genehmigt werden kann, öffentliche Objekte zu erstellen oder zu aktualisieren. Die aktive Rolle des Service Provider-Anwenders steuert diese Autorisierung. Ein Service Provider-Anwender mit Genehmigung auf mehrere Mandanten, der ein Objekt mit Mandanten erstellt, muss den Mandanten direkt oder indirekt angeben.

Auswirkung auf die Benutzeroberfläche

Durch die Installation der Mandantenfähigkeitsfunktion ändert sich die Benutzeroberfläche je nach Genehmigung und Mandantenzugriff, der der Rolle des Anwenders zugeordnet ist.

Hinweis: Weitere Informationen zum Erstellen einer Anwenderrolle und Zuweisen einer Rolle zu einem Anwender finden Sie im *Administrationshandbuch*.

Mandantenanwender

Ein Mandantenanwender, der auf einen einzelnen Mandanten beschränkt ist und der kein Administrator ist, hat die folgenden Berechtigungen zu Benutzeroberflächenänderungen:

- Jeder Anwender, der mehr als einem Mandanten gehört, kann bei der Eingabe von Informationen und beim Generieren eines Berichts einen Mandanten in einer Dropdown-Liste auswählen.

Hinweis: Wenn Sie nicht wollen, dass ein Anwender einen Mandanten beim Generieren eines Berichts auswählt, können Sie die Mandanten-Dropdown-Liste aus dem Bericht entfernen. Weitere Informationen über das Entfernen der Mandanten-Dropdown-Liste finden Sie im *Benutzerhandbuch*.

- Jeder Anwender mit Lesezugriff auf mehr als einen Mandanten besitzt eine Spalte "Mandantennamen" in den Suchergebnissen.

Implementieren der Mandantenfähigkeit

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

So implementieren Sie die Mandantenfähigkeit in CA APM:

1. Stellen Sie sicher, dass der CA CASM-Dienst gestartet ist.
2. Überprüfen Sie, dass der Anwender, der die Mandantenfähigkeit implementiert, einer Rolle zugewiesen ist, in der der Zugriff auf die Verwaltung der Mandantenfähigkeit aktiviert ist.

Hinweis: Weitere Information über die Definition von Rollen und das Zuweisen einer Rolle zu einem Anwender finden Sie im *Administrationshandbuch*.
3. [Aktivieren Sie Mandantenfähigkeit](#). (siehe Seite 124)
4. [Definieren Sie Mandanten, untergeordnete Mandanten und Mandantengruppen](#) (siehe Seite 125).
5. Starten Sie den CA APM-Webserver und Anwendungsserver neu.
6. Melden Sie sich mit dem berechtigten Anwendernamen (in der Regel *uapmadmin*) am Produkt an, und führen Sie die folgenden Schritte aus:
 - a. Definieren Sie Anwenderrollen mit Mandantenzugriff.
 - b. Definieren Sie Kontakte, oder importieren und synchronisieren Sie Anwender.

Hinweis: Weitere Information über das Importieren und Synchronisieren von Anwendern finden Sie im *Administrationshandbuch*.
 - c. Genehmigen Sie Anwendern die Verwendung des Produkts.

Hinweis: Weitere Informationen über das Genehmigen von Anwendern finden Sie im *Administrationshandbuch*.
 - d. Weisen Sie Anwenderrollen Kontakte zu.
7. Melden Sie sich mit dem privilegierten Anwendernamen am Produkt an, und stellen Sie sicher, dass die Mandantenfähigkeitsbeschränkungen angewendet werden.

Aktivieren der Mandantenfähigkeit

Aktivieren Sie Mandantenfähigkeit, so dass mehrere unabhängige Mandanten (und ihre Anwender) eine einzelne Implementierung von CA APM gemeinsam nutzen können. Bevor Sie die Mandantenfähigkeit aktivieren, definieren Sie Mandanten, untergeordnete Mandanten, Mandantengruppen und erstellen Anwenderrollen und weisen Anwendern Rollen zu. Sobald Sie die Mandantenfähigkeit aktivieren, wird die Erzwingung der Mandantenfähigkeit aktiviert. Das Erzwingen der Mandantenfähigkeit bedeutet, dass Sie einen Datensatz nicht speichern können, ohne die Mandantenbeschränkungen zu erfüllen, wenn für ein Objekt ein Mandant erforderlich ist.

Hinweis: Weitere Informationen über das Erstellen von Anwenderrollen und das Zuweisen von Rollen zu den Anwendern finden Sie im *Administrationshandbuch*.

So aktivieren Sie die Mandantenfähigkeit:

1. Klicken Sie auf "Verwaltung", "Mandantenverwaltung".
Die Seite für die Verwaltung der Mandantenfähigkeit wird angezeigt.
2. Klicken Sie auf "Bearbeiten".
3. Wählen Sie in der Dropdown-Liste "Status" eine der folgenden Optionen aus:
aus
Deaktiviert die Mandantenfähigkeit.
ein
Aktiviert die Mandantenfähigkeit.
4. Geben Sie im Feld "Maximale Mandantentiefe" die größtmögliche Tiefe einer Mandantenhierarchie an.
5. Klicken Sie auf "Speichern".
Die Mandantenfähigkeit wird aktiviert.
6. Starten Sie den Webserver und Anwendungsserver neu.

Weitere Informationen:

[Browser-Fehlermeldung, dass Mandantenverwaltungs-Seite nicht angezeigt werden kann, wird angezeigt](#) (siehe Seite 171)

Verwaltung von Mandant, untergeordnetem Mandant und Mandantengruppen

Definieren Sie die Mandanten, Mandantengruppen und untergeordneten Mandanten, um eine einzelne Implementierung von CA APM gemeinsam zu nutzen. Durch Mandantenfähigkeit können Mandanten Hardware- und Anwendungs-Support-Ressourcen gemeinsam nutzen. Dadurch werden Kosten für beide gespart und gleichzeitig viele Vorteile einer unabhängigen Implementierung erzielt.

Definieren eines Mandanten

Sie können so viele Mandanten definieren, wie zum Verwalten von separaten Unternehmen erforderlich sind, die Klienten Unterstützung bieten. Sie müssen einen Mandanten erstellen, bevor eine Instanz eines mandantenabhängigen Objekts aktualisiert werden kann.

Wichtig! Der zuerst erstellte Mandant, der Service Provider, ist der erste Mandant (Eigentümer) in einer CA APM-Installation mit Mandantenfähigkeit. Der Mandant "Service Provider" kann keinen übergeordneten Mandanten haben. Nachdem Sie den Mandanten "Service Provider" erstellt haben, melden Sie sich beim Produkt ab und erneut als Mitglied des Service Providers an. Wir empfehlen, dass Sie sich als der berechnigte Anwender (uapmadmin) anmelden, weil dieser Anwender automatisch zum Mandanten "Service Provider" gehört.

So definieren Sie eine TACL:

1. Klicken Sie auf "Verwaltung", "Mandantenverwaltung".
Die Seite für die Verwaltung der Mandantenfähigkeit wird angezeigt.
2. Klicken Sie im linken Bereich auf "Mandant".
Die Mandanten-Seite wird angezeigt.
3. Klicken Sie auf "Create Tenant".
Die Seite "Neuer Mandant" wird angezeigt.
4. Geben Sie die entsprechenden Informationen ein. Die folgenden Felder bedürfen einer Erklärung:

Mandantennummer

(Nur zur Information) Zeigt die Mandantennummer an. CA APM verwendet dieses Feld nicht.

Datensatzstatus

Aktiviert oder deaktiviert den Mandanten. Nachdem Sie den Mandanten "Service Provider" definiert haben, ist diese Option für den Mandanten schreibgeschützt.

Nutzungsbedingungen

(Nur zur Information) Zeigt die Begriffe der Nutzungserklärung für den Mandanten an. CA APM verwendet dieses Feld nicht.

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.

Logo

(Nur zur Information) Zeigt die URL für eine Imagedatei an, die das Logo für den Mandanten enthält, das ein beliebiger Webbildtyp sein kann. CA APM verwendet dieses Feld nicht.

Kontakt

Zeigt die Seite zur Suche von Kontakten an.

Lokation

Zeigt die Seite zur Suche von Lokationen an.

5. Klicken Sie auf "Speichern".

Der Mandant ist jetzt definiert.

Aktualisieren eines Mandanten

Gegebenenfalls können Sie die Informationen für einen vorhandenen Mandanten aktualisieren.

So aktualisieren Sie einen Mandanten:

1. Klicken Sie auf "Verwaltung", "Mandantenverwaltung".
Die Seite für die Verwaltung der Mandantenfähigkeit wird angezeigt.
2. Klicken Sie im linken Bereich auf "Mandant".
Die Mandanten-Seite wird angezeigt.

3. Suchen Sie nach dem Mandanten, den Sie aktualisieren möchten.
Alle mit den Suchkriterien übereinstimmenden Mandanten werden in der Mandantenliste angezeigt.
4. Klicken Sie auf den zu aktualisierenden Mandanten.
Die Mandanteninformationen werden angezeigt.
5. Klicken Sie auf "Bearbeiten".
6. Geben Sie die neuen Informationen für den Mandanten ein.
7. Klicken Sie auf "Speichern".
Der Mandant wird aktualisiert.

Aktivieren eines Mandanten

Wenn Anwender Informationen für einen bestimmten inaktiven Mandanten anzeigen und eingeben müssen, können Sie den Mandanten aktivieren. Zum Beispiel erhielt der Service Provider keine Zahlung für Dienste, die einem bestimmten Mandanten zur Verfügung gestellt wurden. Basierend auf der Servicevereinbarung macht der Service Provider den Mandanten inaktiv und hört auf, Dienste anzubieten, bis die Zahlung geleistet wurde. Nachdem der Mandant die Zahlung für den Service bereitgestellt hat, aktiviert der Service Provider den Mandanten.

So aktivieren Sie einen Mandanten:

1. Klicken Sie auf "Verwaltung", "Mandantenverwaltung".
Die Seite für die Verwaltung der Mandantenfähigkeit wird angezeigt.
2. Klicken Sie im linken Bereich auf "Mandant".
Die Mandanten-Seite wird angezeigt.
3. Suchen Sie nach dem Mandanten, den Sie aktivieren möchten.
Alle mit den Suchkriterien übereinstimmenden Mandanten werden in der Mandantenliste angezeigt.
4. Klicken Sie auf den zu aktivierenden Mandanten.
Die Mandanteninformationen werden angezeigt.
5. Klicken Sie auf "Bearbeiten".
6. Wählen Sie in der Dropdown-Liste "Datensatzstatus" die Option "Aktiv" aus.
7. Klicken Sie auf "Speichern".
Der Mandant ist jetzt aktiv.

Initialisieren eines neuen Mandanten

Als Service Provider können Sie einen Standarddatensatz für einen neuen Mandanten, z.B. Kostenstellen, Kostentypen und Abteilungen definieren. Weitere Informationen über das Importieren von Daten für Mandanten finden Sie im *Administrationshandbuch*.

Definieren von Mandantengruppen

Sie können eine Mandantengruppe definieren, um den Zugriff auf Mandanten zu klassifizieren, zu verwalten und zu steuern. Zum Beispiel können Sie Asset-Manager einer Mandantengruppe zuweisen, die Mandanten enthält, die zu einer bestimmten geographischen Lokation gehören.

So definieren Sie eine Mandantengruppe:

1. Klicken Sie auf "Verwaltung", "Mandantenverwaltung".
Die Seite für die Verwaltung der Mandantenfähigkeit wird angezeigt.
2. Klicken Sie im linken Bereich auf "Mandantengruppe".
Die Mandantengruppen-Seite wird angezeigt.
3. Klicken Sie auf "Mandantengruppe erstellen".
Die Seite "Neue Mandantengruppe - Details" wird angezeigt.
4. Geben Sie die Mandantengruppeninformationen ein.
5. Klicken Sie auf "Speichern".
Die Mandantengruppe ist jetzt definiert.
6. Klicken Sie auf "Mandanten zuweisen".
Die Mandanten-Suchseite wird angezeigt.
7. Suchen und wählen Sie den Mandanten aus, den Sie der Gruppe hinzufügen möchten.
Der Mandant wird der Gruppe hinzugefügt.

Aktualisieren von Mandantengruppen

Sie können eine Mandantengruppe aktualisieren, um ihre Mitglieder und Detailinformationen zu verwalten.

So aktualisieren Sie eine Mandantengruppe:

1. Klicken Sie auf "Verwaltung", "Mandantenverwaltung".
Die Seite für die Verwaltung der Mandantenfähigkeit wird angezeigt.
2. Klicken Sie im linken Bereich auf "Mandantengruppe".
Die Mandantengruppen-Seite wird angezeigt.
3. Suchen Sie nach dem Mandanten, den Sie aktualisieren möchten.
Alle mit den Suchkriterien übereinstimmenden Mandantengruppen werden in der Mandantengruppen-Liste angezeigt.
4. Klicken Sie auf die Mandantengruppe in der Liste.
Die Seite "Mandantengruppe - Details" wird angezeigt.
5. Klicken Sie auf "Bearbeiten".
6. Geben Sie die neuen Informationen für die Mandantengruppe ein.
7. (Optional) Klicken Sie auf "Mandanten zuweisen", um einem Mandanten der Gruppe hinzuzufügen.
Hinweis: Durch das Hinzufügen oder Entfernen eines Mandanten werden auch die untergeordneten Mandanten dieses Mandanten hinzugefügt oder entfernt.
8. Klicken Sie auf "Speichern".
Die Mandantengruppe wird aktualisiert.

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.

CA APM 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: Obwohl nicht benötigt, kann der Service Provider an Mandantenhierarchien teilnehmen. Der Service Provider kann keinen übergeordneten Mandanten haben.

Definieren von untergeordneten Mandanten

Untergeordnete Mandanten ermöglichen Ihnen die Definition und Änderung von Mandantenhierarchien zu organisatorischen Zwecken und zur gemeinsamen Datennutzung. Um einen Mandanten in eine Mandantenstruktur aufzunehmen, geben Sie einen übergeordneten Mandanten an.

So definieren Sie einen untergeordneten Mandanten:

1. Klicken Sie auf "Verwaltung", "Mandantenverwaltung".
Die Seite für die Verwaltung der Mandantenfähigkeit wird angezeigt.
2. Klicken Sie im linken Bereich auf "Mandant".
Die Mandanten-Seite wird angezeigt.
3. Klicken Sie auf "Create Tenant".
Die Seite "Neuer Mandant" wird angezeigt.
4. Geben Sie die entsprechenden Informationen ein. Die folgenden Felder bedürfen einer Erklärung:

Übergeordneter Mandant

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

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

5. Klicken Sie auf "Speichern".
Der Mandant ist ein untergeordneter Mandant des übergeordneten Mandanten.

Hinweis: Wenn ein Mandant ein untergeordneter Mandant wird, gehört der Mandant der untergeordneten Mandantengruppe des übergeordneten Mandanten an, zusätzlich zu seinen anderen untergeordneten Mandanten (falls vorhanden), usw. Der übergeordnete Mandant wird Mitglied der übergeordneten Mandantengruppe seines neuen untergeordneten Mandanten, zusätzlich zu seinen anderen übergeordneten Mandanten (falls vorhanden), usw. Alle diese Mandanten treten der Gruppe zugehöriger Mandanten der anderen bei.

Aktualisieren von untergeordneten Mandanten

Gegebenenfalls können Sie die Informationen für einen vorhandenen untergeordneten Mandanten aktualisieren.

So erstellen Sie einen untergeordneten Mandanten:

1. Klicken Sie auf "Verwaltung", "Mandantenverwaltung".
Die Seite für die Verwaltung der Mandantenfähigkeit wird angezeigt.
2. Klicken Sie im linken Bereich auf "Mandant".
Die Mandanten-Seite wird angezeigt.
3. Suchen Sie nach dem Mandanten, den Sie aktualisieren möchten.
Alle mit den Suchkriterien übereinstimmenden Mandanten werden in der Mandantenliste angezeigt.
4. Klicken Sie auf den Mandanten in der Liste. Der Name des untergeordneten Mandanten wird in der Spalte "Name" der Mandantenliste angezeigt.
Die Mandanteninformationen werden angezeigt.
5. Klicken Sie auf "Bearbeiten".
6. Geben Sie die neuen Information für den untergeordneten Mandanten ein.
7. Klicken Sie auf "Speichern".
Der untergeordnete Mandant wird aktualisiert.

Systemverwaltete Mandantengruppen

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

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

Systemverwaltete Gruppen können wie anwenderdefinierte Mandantengruppen verwendet werden. Allerdings können nur der Name und die Beschreibung geändert werden.

Kapitel 7: Integration mit anderen Produkten

Dieses Kapitel enthält folgende Themen:

[CA Business Intelligence-Integration](#) (siehe Seite 133)

[CA EEM-Integration](#) (siehe Seite 136)

[CA CMDB-Integration](#) (siehe Seite 136)

[CA Process Automation-Integration](#) (siehe Seite 144)

[CA Service Catalog-Integration](#) (siehe Seite 151)

CA Business Intelligence-Integration

CA Business Intelligence ist eine Berichts- und Analyse-Softwaresuite, die von mehreren CA Produkten zur Präsentation von Informationen sowie zur Unterstützung von Geschäftsentscheidungen eingesetzt wird. CA Produkte nutzen CA Business Intelligence, um die für ein effektives IT-Unternehmensmanagement erforderlichen wichtigen Informationen zu integrieren, zu analysieren und anschließend zu präsentieren.

CA Business Intelligence installiert SAP-BusinessObjects Enterprise als ein selbstständiges Produkt, das eine vollständige Suite von Informationsmanagement-, Berichterstellungs-, Abfrage- und Analyse-Tools bereitstellt. Die Installation funktioniert unabhängig von CA-Produkten, wodurch es den Produkten ermöglicht wird, den gleichen CA Business Intelligence-Dienst gemeinsam zu nutzen.

CA-Produkte bieten eine Vielzahl von Business Intelligence-Möglichkeiten einschließlich Berichtgenerierung, Abfragen und Analysen unter Verwendung der BusinessObjects Enterprise-Technologie. CA APM bietet vordefinierte BusinessObjects Enterprise-Berichte. Weitere Informationen über die vordefinierten Berichte finden Sie im *Benutzerhandbuch*. CA Business Intelligence bietet Anwendern zusätzliche konfigurierbare Berichterstellungsfunktionen.

Die BusinessObjects Enterprise-Installationsdatenträger und Dokumentation werden mit dem CA APM-Installationsdatenträger und der entsprechenden Dokumentation bereitgestellt.

Wichtig! Sie müssen CA Business Intelligence installieren, bevor Sie CA APM installieren.

Integration von CA APM und CA Business Intelligence

Wichtig! Sie müssen CA Business Intelligence installieren, bevor Sie CA APM installieren.

CA APM liefert die erforderlichen Daten, damit Sie die BusinessObjects Enterprise-Berichte starten können. Nachdem Sie BusinessObjects Enterprise und CA APM installiert haben, führen Sie die erforderlichen Konfigurationstasks durch, bevor Sie die Berichte verwenden. Um CA APM in BusinessObjects Enterprise zu integrieren, führen Sie die folgenden Schritte durch:

1. Werden Sie vertraut mit BusinessObjects Enterprise, einschließlich der Dokumentation, so dass Sie das Produkt verwalten und verwenden können. Sie müssen mindestens die folgenden Funktionen durchführen können:
 - Installieren von CA Business Intelligence, das BusinessObjects Enterprise installiert.
 - Verwenden von vordefinierten Berichten in BusinessObjects Enterprise.
2. Installieren Sie CA Business Intelligence-BusinessObjects Enterprise, und notieren Sie sich die folgenden Anmelde- und Verbindungsinformationen, zu deren Eingabe Sie während der CA APM-Installation aufgefordert werden:
 - BusinessObjects Enterprise-Administrator-ID
 - BusinessObjects Enterprise-Administratorkennwort
 - BusinessObjects Enterprise-CMS-Port. Der CMS (Central Management Server) verwaltet eine Datenbank mit Informationen über Ihre BusinessObjects, die Sie mit CA Business Intelligence verwenden. Die standardmäßige CMS-Portnummer lautet 6400.
3. Wenn Sie Oracle als CA MDB verwenden, definieren Sie einen Oracle-Net Service-Namen (NSN), auf dem CA Business Intelligence installiert ist. Notieren Sie den NSN, zu dessen Eingabe Sie während der CA APM-Installation aufgefordert werden.
4. Stellen Sie sicher, dass BusinessObjects Enterprise installiert ist, indem Sie BusinessObjects Enterprise starten.
5. Installieren Sie CA APM. Die CA APM-Installation installiert und konfiguriert die BIAR-Datei sowohl für die Oracle- als auch für die SQL Server-Datenbanken. Die BIAR-Datei enthält CA Business Intelligence-Universe, vordefinierte Berichte und den CA APM-Standardverwaltungsanwender (uapmadmin).

Hinweis: Wenn Sie CA APM installieren, geben Sie die BusinessObjects Enterprise-Anmeldeinformationen, den BusinessObjects Enterprise-CMS-Port und den Oracle-NSN ein, die Sie sich notiert haben. Falls .NET Framework nicht auf dem CA Business Intelligence-Server installiert ist, geben Sie 6400 ein, sobald Sie zur Eingabe des CMS-Ports aufgefordert werden.

6. Werden Sie mit den vordefinierten Berichten vertraut, und verwenden Sie diese. Weitere Informationen über die vordefinierten CA APM-Berichte finden Sie im *Benutzerhandbuch*.

7. Befolgen Sie diese bewährten Methoden bei der Verwaltung und Verwendung von BusinessObjects Enterprise:
- Für jedes CA-Produkt sollten Sie ein Universum installieren und verwalten.
 - Ändern Sie das Standard-Universum nicht. Kopieren Sie stattdessen das Universe, und ändern Sie die Kopie. Andernfalls werden sämtliche anwenderdefinierte Änderungen, die Sie vornehmen, nicht beibehalten, wenn Sie Service Packs, Patches und andere Updates anwenden.
 - Sichern Sie Ihre Änderungen, bevor Sie Service Packs, Patches und andere Updates auf Ihr anwenderdefiniertes Universe anwenden.
 - Wenn Berichte nicht richtig funktionieren, überprüfen Sie, ob der CMS betriebsbereit ist.
 - Überschreiben Sie keine vordefinierten Berichte.
 - Verwenden Sie immer einen vordefinierten Bericht als Basis, um einen anwenderdefinierten Bericht zu erstellen, mit dessen Hilfe eine konsistente Formatierung in allen Berichten beibehalten wird.
 - Vergessen Sie nicht, dass die Administratoren alle Berichte ändern und neue basierend auf dem vorhandenen Universe erstellen können. Allerdings können Administratoren dem vorhandenen CA APM-Ordner keine Berichte hinzufügen.
 - Administratoren und Endanwender sollten vordefinierte Berichte nicht ändern, da Änderungen dieser Berichte auf alle anderen Anwender angewendet werden, die die gleiche CA Business Intelligence-Instanz verwenden. Erstellen Sie stattdessen anwenderdefinierte Ordner, kopieren Sie die Berichte in die anwenderdefinierten Ordner, benennen Sie die Berichte um und passen Sie die Berichte an.
 - Sowohl Administratoren als auch Anwender müssen ihren anwenderdefinierten Ordnern neue Berichte hinzufügen, die sie erstellen.

Berichtskonfigurationen und Produktupdates

Wenn Sie Updates (Patches, Service Packs oder andere Updates) nach CA APM installieren, überschreibt der Updateprozess die vorhandenen Produktkomponenten, einschließlich in einigen Fällen die Berichterstellungskomponenten. Dadurch können Berichterstellungskonfigurationen, die Sie früher ausführten, verloren gehen. CA Technologies bietet Ihnen jedoch eine Methode, Ihre Berichtskonfigurationen beizubehalten, wenn Sie CA APM-Updates anwenden. Folgen Sie den Anweisungen in einem von CA Technologies bereitgestellten Whitepaper, das Sie unter <http://ca.com/support> öffnen können.

Navigieren Sie unter "Technischer Support" zur Produktseite für CA Technologies-IT-Asset-Manager. Durchsuchen Sie die Liste mit Empfehlungen nach *Whitepaper: Berichtskomponenten-Upgrade und Versionskontrolle zur Beibehaltung von Anwenderanpassungen*. Sie können Ihre Berichtskonfigurationen sichern, indem Sie die im Whitepaper beschriebene Strategie implementieren.

Hinweis: Weitere Informationen über die Konfiguration von Berichten finden Sie im *CA Business Intelligence-Implementierungshandbuch*.

CA EEM-Integration

CA APM verwendet CA EEM für die Authentifizierung. Sie müssen CA EEM installieren, bevor Sie mit der Produktinstallation beginnen.

Andere Produkte, die CA EEM für die Authentifizierung benötigen, können den gleichen CA EEM-Server verwenden, den CA APM verwendet.

- Sie können CA EEM verwenden, um die Sicherheit für mehrere CA Technologies-Produkte zentral zu verwalten. Geben Sie während des CA APM-Installationsvorgangs den Namen, die Lokation und die Anmeldeinformationen für den vorhandenen Server an.
- Sie können die CA APM-Sicherheit auch unabhängig von anderen CA Technologies-Produkten verwalten. Installieren Sie CA EEM auf jedem einzelnen Anwendungs- oder Webserver, auf dem das vorhandene CA EEM nicht installiert ist.

CA CMDB-Integration

Dieser Abschnitt erklärt, wie CA APM mit CA CMDB Version 12.7 und CA CMDB, die in CA Service Desk Manager Version 12.7 enthalten ist, integriert wird.

CA CMDB ist eine umfassende, integrierte Lösung für die Verwaltung der IT-Komponenten und Dienste in einem Unternehmen und ihrer Beziehungen in heterogenen Datenverarbeitungsumgebungen. CA CMDB ermöglicht es, zuverlässige, aktuelle Informationen über Assets, so genannte CIs (Configuration Items, Konfigurationselemente) und ihre Beziehungen zueinander anzugeben und zu speichern. Diese Beziehungen bilden die Grundlage für die Auswirkungsanalyse, ein wichtiges Tool für das Steuern der Änderungen innerhalb einer Organisation.

CA CMDB wird in CA APM in einigen Bereichen, einschließlich der folgenden, integriert:

- Die CA APM-Änderungshistoriendatensätze können alle Änderungen, die von CA Service Desk Manager, CA CMDB und CA APM an Asset/CI-Datensätzen vorgenommen wurden, einschließen.
- Wenn CA Service Desk Manager und CA CMDB installiert sind, schließen die Asset/CI-Änderungshistoriendatensätze CA APM-Änderungshistoriendatensätze auf der CA CMDB-Registerkarte "Versionskontrolle" ein.
- Wenn Sie ein Asset in CA APM definieren, können Sie die Asset- und CI-Datensätze kategorisieren und steuern, indem Sie die Kontrollkästchen "Asset" und "CI" aktivieren oder deaktivieren. Diese Flexibilität ist gegeben, da CIs, die CA CMDB erstellt, möglicherweise nicht relevant für CA APM sind. Umgekehrt sind Assets, die CA APM erstellt, möglicherweise nicht relevant für CA CMDB.
- CA APM kann die Felder in einem Asset/CI innerhalb des Kontexts von *Asset-Familien erweitern*. Die zusätzlichen Felder können in CA APM gemeinsam genutzt werden. Zum Beispiel kann ein CA APM-Administrator die Asset-Seite konfigurieren und ein zusätzliches Asset-Feld definieren, damit die Anwender ein in CA Service Desk Manager und CA CMDB erstelltes CI anzeigen und aktualisieren können.
- Sie können ein Ereignis in einem Feld definieren, das mit CA CMDB in CA APM gemeinsam genutzt wird, und das Ereignis entweder in CA APM oder in CA CMDB auslösen. Weitere Informationen über das Verwalten von Ereignissen und Benachrichtigungen finden Sie im *Benutzerhandbuch*.
- Ein CA Service Desk Manager- und CA CMDB-Anwender kann ein Management Data Repository (MDR) definieren und dem CA CMDB-CI erlauben, im Zusammenhang des entsprechenden Assets in CA APM zu starten.

Integration in CA APM und CA CMDB

Wenn Sie CA APM und CA CMDB integrieren, integrieren und trennen Sie die Assets, die CA APM von den Configuration Items (CIs) verwaltet, die CA CMDB in einer einfachen und präzisen Weise verwaltet. CA APM-Anwender können zu einem gemeinsam genutzten Klassifizierungsmodell für die Assets und CIs übergehen. Um CA APM und CA CMDB zu integrieren, führen Sie die folgenden Schritte aus:

1. [Nutzen Sie die Änderungshistoriendatensätze von Assets und Configuration Items gemeinsam](#) (siehe Seite 138).
2. [Kategorisieren Sie die Asset- und CI-Datensätze](#) (siehe Seite 138).
3. [Definieren Sie ein zusätzliches Asset-Feld](#) (siehe Seite 141).
4. [Definieren Sie ein Ereignis in einem gemeinsam genutzten Feld](#) (siehe Seite 143).
5. [Definieren Sie ein Management Data Repository \(MDR\) von CA Service Desk Manager und CA CMDB](#) (siehe Seite 143).

Nutzen Sie die Änderungshistoriendatensätze von Assets und Configuration Items gemeinsam.

Um CA APM und CA CMDB zu integrieren, können die CA APM-Audit-Verlaufsdatensätze alle Änderungen enthalten, die an Asset/CI-Datensätzen von CA Service Desk Manager, CA CMDB und CA APM vorgenommen wurden. Wenn CA Service Desk Manager, CA CMDB oder beide installiert sind, schließen die Asset/CI-Änderungshistoriendatensätze in CA CMDB (Registerkarte "Versionskontrolle") alle CA APM-Änderungshistoriendatensätze ein.

CA CMDB 11.2 und höher bietet Änderungshistoriendatensätze von CA APM. Die Änderungshistoriendatensätze werden sowohl in CA CMDB als auch in CA APM aktualisiert, wenn der Dienst "CA Asset Portfolio Management - Event-Service" gestartet wird. Weitere Informationen finden Sie unter [Starten der Dienste](#) (siehe Seite 58).

Kategorisieren von Asset- und Configuration Item-Datensätzen

In diesem Schritt zur Integration von CA APM und CA CMDB können Sie die Asset- und CI-Datensätze kategorisieren und steuern, wenn Sie ein Asset in CA APM definieren, indem Sie die Kontrollkästchen "Asset" und "CI" aktivieren und deaktivieren. Diese Flexibilität wird bereitgestellt, weil CIs, die von CA CMDB erstellt werden, eventuell für CA APM nicht relevant sein dürften, und umgekehrt Assets, die von CA APM erstellt werden, für CA CMDB nicht relevant sein dürften.

Berücksichtigen Sie die folgenden Informationen, wenn Sie diese Kontrollkästchen verwenden:

Standardwerte

- Alle neuen Asset-Datensätze, die CA APM erstellt, werden ursprünglich nur als ein Asset festgelegt und von CA APM verwaltet. Auf der Seite "Neues Asset" in CA APM werden das Kontrollkästchen "Asset", das Kontrollkästchen "Verwaltet von CA APM" und das Kontrollkästchen "CI" nicht ausgewählt.
- Alle Asset-Datensätze, die CA CMDB erstellt (mit oder ohne CA Service Desk Manager) werden ursprünglich nur auf "CI" festgelegt. Auf den CI-Seiten in CA CMDB ist die Spaltenüberschrift "CI?" auf "Ja" und die Spaltenüberschrift "Asset?" auf "Nein" festgelegt.
- Für CA APM und CA CMDB stehen die Felder "Asset" und "CI" auf den Seiten "Neues Asset" und "CI" zur Verfügung. Jedoch kann das Kontrollkästchen "Verwaltet von CA APM" nur in CA APM angezeigt werden. Die vorhandenen Audit- und Sicherheitsfunktionen für jedes Produkt gelten für diese Kontrollkästchen.

Darstellung

- Die Felder "Asset" und "CI" werden in CA APM und CA CMDB sogar angezeigt, wenn andere CA Technologies-Produkte installiert sind. Die Felder "Asset" und "CI" werden in CA Service Desk Manager nicht angezeigt, wenn CA CMDB nicht installiert ist.
- Der CA APM-Administrator kann die Benutzeroberfläche konfigurieren und die Felder "Asset" und "CI" an eine neue Lokation verschieben, die Felder schreibgeschützt, erforderlich oder optional machen, und die Felder ausblenden.

Hinweis: Weitere Informationen über die Konfiguration der Benutzeroberfläche finden Sie im *Administrationshandbuch*.

Anzeigen und Aktualisieren

CA CMDB

- Der CA CMDB-Analyst und -Administrator können die Asset- und CI-Feldwerte standardmäßig aktualisieren.
- CA CMDB erlaubt es dem Asset?-Wert nicht, standardmäßig geändert zu werden, wenn der Asset?-Wert auf "Ja" festgelegt ist.

CA APM

- Standardmäßig werden in CA APM Asset- und CI-Datensätze angezeigt.
- Der CA APM-Administrator kann die Benutzeroberfläche konfigurieren und die Felder "Asset" und "CI" an eine neue Lokation verschieben, die Kontrollkästchen auf schreibgeschützt, erforderlich oder optional setzen und die Kontrollkästchen ausblenden. Nachdem Sie das CI-Kontrollkästchen ausgewählt und das Asset gespeichert haben, steht das Kontrollkästchen "CI" nicht zur Verfügung und Sie können die Einstellung nicht ändern.

Wichtig! Wir empfehlen, das Kontrollkästchen "CI" in CA APM als schreibgeschützt zu konfigurieren und Änderungen des Kontrollkästchens lediglich auf den CA CMDB-Analysten und Administrator zu beschränken.

- Ein Asset in CA APM, für das das Kontrollkästchen "Verwaltet von CA APM" ausgewählt ist, ist immer ein Asset. Sie können kein Asset in CA APM speichern, in dem das Kontrollkästchen "Verwaltet von CA APM" ausgewählt ist, ohne auch das Kontrollkästchen "Asset" auszuwählen.

Suchen

CA CMDB

- Die CA CMDB-Suche zeigt ursprünglich alle Datensätze standardmäßig an. Jedoch steht eine Option zum Filtern der Datensätze zur Verfügung.

Hinweis: Wenn CA Service Desk Manager installiert ist, gelten die gleichen Standardsuchregeln.

CA APM

- Die Standard-Asset-Suche schließt eine Dropdown-Liste für "Verwaltet von CA APM", "CI" und "Asset" ein. Diese Flexibilität ist geboten, so dass Sie zwischen Assets und CIs unterscheiden können.

Hardware-Abgleich

Der Hardware-Abgleich analysiert alle Asset- und CI-Datensätze. Suchen bieten eine Möglichkeit, CIs anzuzeigen, die sich auf erkannte Assets als Folge des Ausführens des Hardware-Abgleichs beziehen. Ein CA APM-Anwender kann die Ausnahmen anzeigen und entscheiden, ob sie das Kontrollkästchen "Asset" auswählen möchten. Als Folge der Auswahl des Kontrollkästchens "Asset" stehen die Asset-Datensätze in einer CA APM-Asset-Suche zur Verfügung.

Definieren eines zusätzlichen Asset-Feldes

In diesem Schritt zur Integration von CA APM und CA CMDB kann CA APM die Felder in einem Asset innerhalb des Kontexts von *Asset-Familien erweitern*. Die zusätzlichen Felder können in CA APM gemeinsam genutzt werden. Zum Beispiel kann ein CA APM-Administrator die Asset-Seite konfigurieren und ein zusätzliches Asset-Feld definieren, damit die Anwender ein in CA Service Desk Manager und CA CMDB erstelltes CI anzeigen und aktualisieren können.

Wichtig! Diese Schritte funktionieren nur, wenn Sie den Assistenten zum ersten Mal ausführen und das zusätzliche Asset-Feld definieren. Bevor Sie das zusätzliche Feld definieren, überprüfen Sie, dass Ihnen die folgenden Informationen von der `usp_owned_resource`-Tabelle in CA CMDB als Referenz zur Verfügung stehen: Tabellename, Format (Zeichen, boolescher Wert, Währung, Datum, Dezimalwert oder Ganzzahl), Feldname, Attributname und Feldgröße. Nachdem Sie den Assistenten abgeschlossen haben, können Sie das zusätzliche Feld wie ein Feld in CA APM konfigurieren.

Beispiel: Definieren eines zusätzlichen Asset-Feldes für das Gewährleistungsstartdatum

In diesem Beispiel definieren Sie ein zusätzliches Asset-Feld für das Gewährleistungsstartdatum. In CA Service Desk Manager/CA CMDB auf der Registerkarte "Inventar" zeigen Sie die Bezeichnung im CI als Gewährleistungsstartdatum an. Als nächstes zeigen Sie die Informationen für die zugeordnete `nr_wrty_st_dt`-Spalte aus der `usp_owned_resource`-Tabelle in CA CMDB an. In diesem Beispiel ist das `nr_wrty_st_dt`-Spaltenformat eine Ganzzahl, der Feldname ist `nr_wrty_st_dt`, der Attributname ist `nr_wrty_st_dt` und die Feldgröße ist 4. Zeichnen Sie diese Informationen auf, und geben Sie sie genau so ein, wie sie in den entsprechenden Feldern "Format", "Feldname", "Attributname" und "Feldgröße" angezeigt werden. Wir empfehlen auch, dass Sie die gleiche Bezeichnung für das CI (Warranty-Anfangsdatum) im Feld "Bezeichnung" im Assistenten verwenden, um so Verwirrungen zu vermeiden.

So definieren Sie ein zusätzliches Asset-Feld:

1. Ermitteln Sie den CA Service Desk Manager- und CA CMDB-Erweiterungstabellennamen und den Datenbankfeldnamen, indem Sie die CA Service Desk Manager- und CA CMDB-Schemadateien prüfen.

Hinweis: Weitere Informationen über die CA Service Desk Manager- und CA CMDB-Schemadateien finden Sie in der CA Service Desk Manager- und CA CMDB-Dokumentation.

2. Melden Sie sich bei CA APM mit den Anmeldeinformationen an, die Ihnen die Definition einer Erweiterung erlauben.

3. Klicken Sie auf "Asset", "Neues Asset".
4. Klicken Sie links auf KONFIGURIEREN: AN.
Die Konfiguration der Seite wird aktiviert.
5. Definieren Sie im Bereich der Konfigurationsinformationen der Seite eine globale Konfiguration, und speichern Sie diese.
6. Klicken Sie auf "Erweiterung hinzufügen".
Ein Assistent wird angezeigt.
7. Befolgen Sie die Bildschirmanweisungen, um die Informationen für das zusätzliche Feld einzugeben.
8. Führen Sie auf der Seite "Typ" des Assistenten die folgenden Schritte durch:
 - a. Wählen Sie die Option "Einfaches Feld" aus.
 - b. Wählen Sie den Teil der Seite aus, auf der das neue Feld angezeigt wird.
 - c. Aktivieren Sie das Kontrollkästchen "Für alle zusätzlichen Typen".
 - d. Klicken Sie auf "Weiter".
9. Führen Sie auf der Seite "Felder" des Assistenten die folgenden Schritte durch:

Wichtig! Geben Sie die Spalteninformation aus der `usp_owned_resource`-Tabelle in CA CMDB ein. Wir empfehlen auch, dass Sie die gleiche Bezeichnung für das CI im Feld "Bezeichnung" verwenden, um Verwirrungen zu vermeiden.

 - a. Klicken Sie auf "Feld hinzufügen".
 - b. Geben Sie die Feldbezeichnung ein, die auf der Seite angezeigt werden soll.
 - c. Wählen Sie das Datumsformat aus.
 - d. Geben Sie den Datenbanknamen ein.
 - e. Geben Sie den Attributnamen ein.
 - f. Geben Sie die Feldgröße ein.
 - g. (Optional) Geben Sie eine Beschreibung für das Feld ein.
 - h. Geben Sie an, ob eine Eingabe für das Feld benötigt wird.
 - i. Klicken Sie auf das Häkchensymbol, um das Feld zu speichern.
Das Produkt zeigt die von Ihnen eingegebenen Feldinformationen an.
 - j. Klicken Sie auf "Weiter".
10. Überprüfen Sie auf der Seite "Zusammenfassung" des Assistenten die Feldinformationen, und klicken Sie auf "Speichern und beenden".
11. Überprüfen Sie, ob das Feld auf der Asset-Seite angezeigt wird.

12. Klicken Sie auf "Konfiguration speichern".

Alle Anwender können das zusätzliche Feld auf der Seite anzeigen. Sie können ein Ereignis in CA APM angeben und das Ereignis entweder in CA APM oder in CA CMDB auslösen. Weitere Informationen über das Verwalten von Ereignissen finden Sie im *Benutzerhandbuch*.

Definieren eines Ereignisses in einem gemeinsam genutzten Feld

Sie können ein Ereignis in CA APM in einem Feld definieren, das von CA APM und CA CMDB gemeinsam genutzt wird. Wenn die Kriterien für das Ereignis durch eine Änderung in CA Service Desk Manager/CA CMDB oder CA APM auftreten, wird das Ereignis beendet und die Benachrichtigung wird gesendet. Zum Beispiel können Sie ein Ereignis auf der Asset-Seite für das Kontakt-Feld definieren. Wenn das Ereignis ein Change-Event ist, kann das Ereignis beendet werden, wenn Sie das Kontakt-Feld entweder im Asset oder im verwandten Configuration Item (CI) ändern. Sobald das Ereignis beendet ist, wird eine Benachrichtigung gesendet.

Hinweis: Weitere Informationen über die Verwaltung von Ereignissen und Benachrichtigungen finden Sie im *Benutzerhandbuch*.

Definieren eines Management Data Repository (MDR) von CA Service Desk Manager und CA CMDB

In diesem Schritt zur Integration von CA APM und CA CMDB kann ein CA Service Desk Manager- und CA CMDB-Anwender ein Management Data Repository (MDR) definieren und dem CA CMDB-CI erlauben, im Kontext des entsprechenden Assets in CA APM zu starten.

So definieren Sie ein MDR in CA Service Desk Manager und CA CMDB:

1. Melden Sie sich auf der CA Service Desk Manager-Webbenutzeroberfläche als Administrator an.
2. Klicken Sie auf die Registerkarte "Administration". Wählen Sie im Administrationsbrowser die Option "CACMDB", "MDR-Management", "MDR-Liste" aus.
3. Klicken Sie auf "Neu erstellen".

Die MDR-Providerdefinition wird angezeigt.

4. Geben Sie die folgenden obligatorischen MDR-Provider-Informationen ein:

Button Name

Geben Sie *ITAM* als Schaltflächenname an.

MDR Name

Geben Sie *ITAM* als MDR-Name an.

MDR Class

Geben Sie *GLOBAL* als MDR-Klasse an.

Hostname

Geben Sie den CA APM-Servernamen mit Hilfe der Netzwerkadresse oder des DNS-Namens des CA APM-Webservers an.

Wichtig! Das MDR-Provider-Formular füllt automatisch das Feld "URL für Start in Kontext" basierend auf den Informationen aus, die Sie angeben. Geben Sie also *keinen Wert* für dieses Feld ein.

5. Klicken Sie auf "Speichern".
Der CA APM-MDR-Provider ist nun definiert.
6. Definieren Sie in CA CMDB ein CI.
7. Klicken Sie im CI-Detailformular auf die Registerkarte "Attribut".
8. Klicken Sie auf die ITAM-Schaltfläche, die Sie zuvor definiert haben.
Das entsprechende Asset in CA APM wird angezeigt.

CA Process Automation-Integration

CA APM und CA Process Automation werden integriert, damit Sie einen Benachrichtigungsprozess einrichten und konfigurieren können, der Benachrichtigungen an bestimmte Empfänger liefert, nachdem ein angegebenes Ereignis aufgetreten ist. CA APM bietet E-Mail-Benachrichtigungsprozesse mit dem Produkt. Diese Prozesse werden in Dateien geliefert, die auf dem Produktinstallationsdatenträger enthalten sind. Sie importieren die Dateien in CA Process Automation und geben Prozessparameter in CA Process Automation und CA APM an.

Konfigurieren des CA Process Automation-Benachrichtigungsprozesses

Verwenden Sie die folgenden Schritte, um die E-Mail-Benachrichtigungsprozesse einzurichten, die mit CA APM mitgeliefert werden.

1. Installieren Sie CA APM und CA Process Automation.
2. [Importieren Sie die Workflow-Provider-Benachrichtigungsprozessdateien](#) (siehe Seite 145).

3. [Konfigurieren Sie in CA Process Automation den Mail-Server](#) (siehe Seite 146).
4. [Ändern Sie in CA Process Automation die Einstellungen für die Workflow-Prozessparameter](#) (siehe Seite 147).
 - a. Ändern Sie die Standard-E-Mail-Adresse für den Administrator (Admin_Email_To-Parameter), um Ihre erforderliche Einstellung anzugeben.
 - b. Ändern Sie die CA APM-Standard-URL (ITAM_URL-Parameter), um Ihre erforderliche Einstellung anzugeben.
 - c. Ändern Sie die CA APM-Standard-URL (ITPAM_URL-Parameter), um Ihre erforderliche Einstellung anzugeben.
 - d. (Optional) Ändern Sie einen der anderen Parameter, für die Sie Ihre erforderlichen Einstellungen angeben wollen.
5. [Erlauben Sie in CA APM und CA EEM CA APM-Anwendern, CA Process Automation zu verwend](#) (siehe Seite 149)en.
6. Erstellen Sie in CA EEM CA Process Automation-Anwenderkonten für Nicht-CA APM-Anwender.
7. Geben Sie in CA APM die Workflow-Prozessparameter ein, wenn Sie ein Ereignis definieren.

Hinweis: Weitere Informationen über die Definition eines Ereignisses in CA APM finden Sie im *Benutzerhandbuch*. Weitere Informationen über die Verwendung von CA Process Automation und CA EEM finden Sie in der Dokumentation zu CA Process Automation und CA EEM.

Importieren der Workflow-Provider-Benachrichtigungsprozessdateien

CA APM bietet Standard-E-Mail-Benachrichtigungsprozessdateien. Sie importieren diese Dateien in CA Process Automation, bevor Sie E-Mail-Benachrichtigungen in den Produkten einrichten und konfigurieren können.

Hinweis: Weitere Informationen über das Importieren von Dateien und über das Arbeiten mit Dateien finden Sie in der CA Process Automation-Dokumentation.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei CA Process Automation als Administrator an.
2. Navigieren Sie zum CA Process Automation-Client.

- Suchen Sie die ITAM.xml-Datei auf den CA APM-Installationsdatenträgern im folgenden Pfad:

CD1\SetupFiles\ITPAM\

- Importieren Sie die ITAM.xml-Datei in den /-Knoten.

Hinweis: In CA Process Automation-Version 3.1 importieren Sie die XML-Datei aus dem Client. In Version 4.0 SP1 importieren Sie die XML-Datei aus der Registerkarte "Bibliothek".

Wählen Sie die Importoptionen aus, um die importierten Versionen als aktuell festzulegen und die importierten anwenderspezifischen Operatoren und Sensoren verfügbar zu machen.

Die Benachrichtigungsprozessdateien werden in den /ITAM-Standardordner importiert.

Konfigurieren des CA Process Automation-Mailservers

Um E-Mail-Benachrichtigungen zwischen CA Process Automation und CA APM zu implementieren, konfigurieren Sie den Mail-Server für CA Process Automation.

Hinweis: Spezifische Anweisungen zur Konfiguration des CA Process Automation-Warnmoduls zum Konfigurieren des Mail-Servers finden Sie im *CA IT Process Automation Manager-Administrationshandbuch*.

- Melden Sie sich bei CA Process Automation als Administrator an.
- Navigieren Sie zum CA Process Automation-Client.
- Navigieren Sie zum Bibliotheksbrowser.
- Suchen und sperren Sie die Standardumgebung.
- Suchen Sie das Warnmodul, und deaktivieren Sie das Kontrollkästchen "Erben".
- Geben Sie den SMTP-(Mail)-Server an

Beispiel: mail.company.com

- Geben Sie die Absenderadresse ein.

Beispiel: admin@company2.com

- Speichern Sie die Änderungen.
- Entsperren Sie die Standardumgebung.

Es dauert einige Minuten, bis die Änderungen in Kraft treten.

Hinweis: Sie können eine E-Mail-Benachrichtigung an eine externe E-Mail-Adresse senden, wenn Ihre SMTP-(Mail)-Servereinstellungen eine E-Mail-Übermittlung an die externe Adresse erlauben. Überprüfen Sie Ihre Mail-Server-Einstellungen, um sicherzustellen, dass Sie E-Mail an externe Adressen senden können.

Ändern der CA Process Automation-Workflow-Prozessparameter

Nachdem Sie CA APM und CA Process Automation installiert und die Benachrichtigungsprozessdateien in CA Process Automation importiert haben, werden die Standard-Workflowprozessparameter in CA Process Automation definiert. Sie können die Standardprozessparameter ändern, um Ihre erforderlichen Einstellungen einzuschließen. Sie geben tatsächliche (hart-kodierte) Werte als Prozessparameter an. Sie müssen überprüfen, ob die von Ihnen eingegebenen Werte gültig sind.

Sie können die Parameter des Benachrichtigungsprozesses in dem Datensatz ändern, der auf alle Benachrichtigungsprozesse oder in den Startanforderungsformularen des individuellen Prozesses angewendet wird. Die Parameter, die Sie für einen individuellen Prozess angeben, überschreiben die Parameter im Hauptdatensatz für diesen Prozess.

Hinweis: Sie geben einige Parameter des Benachrichtigungsprozesses für den Workflow-Provider an, wenn Sie ein Ereignis in CA APM definieren. Weitere Informationen über das Festlegen von Prozessparametern in CA APM finden Sie im *Benutzerhandbuch*.

So ändern Sie die CA Process Automation-Workflow-Prozessparameter

Wichtig! CA APM und CA Process Automation validieren nicht die Informationen, die Sie für die Parameter eingeben. Sie müssen überprüfen, dass Ihre Eingabe gültig ist und dass Sie die Daten im richtigen Format eingaben.

1. Melden Sie sich bei CA Process Automation an, und navigieren Sie zum CA Process Automation-Client.
2. Suchen Sie im ITAM-Ordner nach dem Datensatz, der Dataset heißt.
3. Geben Sie die Informationen für die Parameter ein.

Die folgenden Felder bedürfen einer Erklärung:

Ack_Interaction_Form_Full_Path

Vollständiger Pfad zu der Datei, die das Interaktionsbestätigungsformular in CA Process Automation enthält. Der E-Mail-Benachrichtigungs-Empfänger verwendet dieses Formular, um den Empfang der Benachrichtigung zu quittieren. Jeder Workflow-Prozess muss ein einmaliges Anwenderinteraktionsformular und einen eindeutigen Pfad zum Formular haben. Sie können die Interaktionsbestätigungs-Formulardateien, die mit dem Produkt mitgeliefert werden, in dem Ordner finden, der die Prozesse und den Hauptdatensatz enthält (/ITAM oder der Ordner, in den Sie die Prozesse importiert haben).

Admin_Email_CC

E-Mail-Adresse der Kopienempfänger für die E-Mail, die dem Administrator gesendet wird, wenn ein Benachrichtigungsfehler auftritt.

Admin_Email_To

E-Mail-Adresse des Administrators für die E-Mail, die gesendet wird, wenn ein Benachrichtigungsfehler auftritt. Ändern Sie den Standardwert in die erforderliche Einstellung.

Log_Folder_Path

Vollständiger Pfad der Fehlerprotokolldatei, die erstellt wird, wenn ein Fehler im Benachrichtigungsprozess auftritt. Wenn Sie keinen Pfad angeben, verwendet die Protokolldatei den CA Process Automation-Standard-Protokolldateipfad.

ITAM_Username

Anwendername, um sich in CA APM anzumelden. CA Process Automation benötigt Zugriff auf CA APM, um Benachrichtigungsempfänger- und Eskalationsinformationen abzurufen.

ITAM_Password

Anwenderkennwort, um sich in CA APM anzumelden. CA Process Automation benötigt Zugriff auf CA APM, um Benachrichtigungsempfänger- und Eskalationsinformationen abzurufen.

Admin_Email_Subject

Thema für die E-Mail, die dem Administrator gesendet wird, wenn ein Benachrichtigungsfehler auftritt. Dieser Parameter kann im Hauptdatensatz oder im Startanforderungsformular für den individuellen Prozess festgelegt werden.

Admin_Email_Header

Header oder Einleitung für die E-Mail, die dem Administrator gesendet wird, wenn ein Benachrichtigungsfehler auftritt (z.B. "Hallo"). Dieser Parameter kann im Hauptdatensatz oder im Startanforderungsformular für den individuellen Prozess festgelegt werden.

Admin_Email_Footer

Signatur für die E-Mail, die dem Administrator gesendet wird, wenn ein Benachrichtigungsfehler auftritt (z.B. "Danke"). Dieser Parameter kann im Hauptdatensatz oder im Startanforderungsformular für den individuellen Prozess festgelegt werden.

Log_File_Name

Name der Fehlerprotokolldatei, die erstellt wird, wenn ein Fehler im Benachrichtigungsprozess auftritt. Die E-Mail, die bei einem Benachrichtigungsfehler an den Administrator gesendet wird, enthält den Protokolldateinamen. Wenn Sie keinen Namen angeben, verwendet die Protokolldatei den folgenden CA Process Automation-Standard-Protokolldateinamen:

Prozessname_Prozess-Instanznummer.log

ITAM_URL

CA APM-URL, die CA Process Automation verwendet, um auf CA APM für Informationen über Benachrichtigungsempfänger und Eskalation zuzugreifen. Ändern Sie den Standardwert in die erforderliche Einstellung.

ITPAM_URL

CA Process Automation-URL, die in der E-Mail-Benachrichtigung enthalten ist. Ändern Sie den Standardwert in die erforderliche Einstellung.

4. Speichern Sie die Änderungen in CA Process Automation.

Hinweis: Weitere Informationen über das Konfigurieren eines Benachrichtigungsprozesses finden Sie in Ihrer Workflow-Provider-Dokumentation.

Gestatten der CA Process Automation-Verwendung für CA APM-Anwender

Die CA APM-Anwender, die Benachrichtigungen erhalten, müssen auf CA Process Automation zugreifen, um die Benachrichtigungen zu quittieren. Diese Anwender müssen über die Berechtigung verfügen, CA Process Automation zu verwenden. Sie erlauben Anwendern die Verwendung von CA Process Automation, indem Sie zunächst Schritte in CA APM und dann in CA EEM durchführen. In CA APM definieren und genehmigen Sie Anwendern, sich bei CA APM anzumelden und es zu verwenden. In CA EEM erlauben Sie den genehmigten CA APM-Anwendern die Verwendung von CA Process Automation.

So erlauben Sie CA APM-Anwendern die Verwendung von CA Process Automation:

1. Melden Sie sich bei CA APM an.
2. Stellen Sie sicher, dass sowohl neue als auch vorhandene Anwender autorisiert sind, sich bei CA APM anzumelden und es zu verwenden.

Hinweis: Weitere Informationen über das Definieren und Genehmigen von neuen und bereits vorhandenen Anwendern in CA APM finden Sie im *Administrationshandbuch*.

Das Produkt definiert und genehmigt die CA APM-Anwender. CA EEM schließt jetzt die CA APM-Anwender in die Liste verfügbarer Anwender ein.

3. Melden Sie sich bei CA EEM an, indem Sie CA Process Automation aus der Dropdown-Liste der Anwendungen auswählen.

Wichtig! Sie müssen die CA Process Automation-Anwendung auswählen, wenn Sie sich bei CA EEM anmelden, um CA APM-Anwendern die Verwendung von CA Process Automation zu erlauben.

4. Wählen Sie einen CA APM-Anwender aus der Liste aller Anwender aus, und klicken Sie auf die Anwendungsanwenderdetails für den Anwender.
5. Wählen Sie eine CA Process Automation-Anwendergruppe für den Anwender aus, und speichern Sie die Auswahl.

Hinweis: Weitere Informationen über die Verwendung von CA EEM zum Hinzufügen von Anwendungen zu Anwenderdetails finden Sie in der CA EEM-Dokumentation.

Der CA APM-Anwender kann jetzt auf CA Process Automation zugreifen und es verwenden.

Erforderliche Indikatoren und mehrzeilige Textfelder für Parameter

Die Standardbenachrichtigungsprozesse, die mit dem Produkt geliefert werden, enthalten die Parameter, die in der Benutzeroberfläche zur Definition von Produktereignissen angezeigt werden, und die Parameter, die Sie im Workflow-Provider angeben. Die Standardprozesse enthalten auch XML-Formatierung, die Sie einen erforderlichen Indikator und ein mehrzeiliges Textfeld in der Produktbenutzeroberfläche anzeigen lässt. Diese Elemente werden vom Workflow-Provider nicht automatisch bereitgestellt und deshalb im Prozess angegeben. Im Anforderungsformular für den CA Process Automation-Start wird für jeden Standardprozess die folgende XML-Anweisung vor der Beschreibung der einzelnen Benutzeroberflächenparameter angezeigt:

```
<FieldDescriptor><IsRequired>true_or_false</IsRequired><Length>number</Length></FieldDescriptor>
```

IsRequired

Gibt an, ob der Parameter benötigt (wahr) oder nicht benötigt wird (falsch). Wenn der Parameter benötigt wird, zeigt das Produkt den standardmäßigen erforderlichen Indikator in der Benutzeroberfläche an.

Beispiel: <FieldDescriptor><IsRequired>true</IsRequired></FieldDescriptor>

Länge

Gibt die Länge des Parametertexteingabefelds an. Um ein mehrzeiliges Textfeld zu definieren, geben Sie einen Wert ein, der größer als 255 ist.

Beispiel: <FieldDescriptor><Length>275</Length></FieldDescriptor>

Sie können die Standardbenachrichtigungsprozesse ändern, die mit dem Produkt geliefert werden, und Sie können auch Ihren eigenen neuen Benachrichtigungsprozess erstellen. Um Informationen über die erforderliche Indikatoren- und Feldlänge in Ihren geänderten oder neuen Prozess aufzunehmen, müssen Sie die XML-Anweisung vor der Beschreibung der einzelnen Benutzeroberflächenparameter in Ihrem Prozess einfügen.

Hinweis: Wenn Sie einen neuen Benachrichtigungsprozess erstellen, müssen Sie über ein entsprechendes Anforderungsformular für den Start des Prozesses verfügen. Weitere Informationen über das Ändern oder Erstellen der Benachrichtigungsprozesse finden Sie in Ihrer Workflow-Provider-Dokumentation.

CA Service Catalog-Integration

CA Service Catalog wird in CA APM integriert, damit Sie angefragte Elemente von einem Serviceantrag mit CA APM-Assets verbinden können. Sie können CA APM-Assets Elementen zuordnen, die während der Anforderungsabwicklung von CA Service Catalog angefordert wurden. Assets, die bereits einer Anforderung zugewiesen sind, können angezeigt und ggf. aus der Anforderung entfernt werden. Außerdem können Sie die Abwicklung einer Assets-Anforderung ablehnen

Wichtig! CA APM und CA Service Catalog müssen die gleiche CA MDB und das gleiche CA EEM gemeinsam nutzen, damit die Integration richtig funktioniert.

Hinweis: Weitere Informationen über das Abwickeln von Anforderungen von Inventar finden Sie im *Benutzerhandbuch*. Weitere Informationen über das Erstellen und Verwalten von Anforderungen in CA Service Catalog finden Sie im *CA Service Catalog-Integrationshandbuch*.

Kapitel 8: Implementieren von CA SAM mit CA APM

Dieses Kapitel enthält folgende Themen:

[Überblick](#) (siehe Seite 153)

[CA APM- und CA SAM-Datensynchronisation](#) (siehe Seite 154)

[So implementieren Sie CA SAM mit CA APM](#) (siehe Seite 155)

[Empfehlungen zur Datenverwaltung](#) (siehe Seite 164)

[So deinstallieren Sie CA Software Compliance Manager](#) (siehe Seite 169)

Überblick

CA APM koordiniert mit CA SAM, sodass Sie Software Asset Management-Funktionen ausführen können. CA SAM ist die nächste Entwicklung von Software Asset Management und Software Compliance Management, das CA Software Compliance Manager (CA SCM) ersetzt. Auf der Produkt-Support-Site auf CA Support Online finden Sie weitere Informationen zu Plänen für CA Software Compliance Manager.

Wichtig! Wir empfehlen Ihnen nicht, Software-Assets in CA APM zu verwalten. Um die Verbesserungen zu nutzen, die CA APM Version 12.8 bereitstellt, empfehlen wir, dass Sie CA SAM verwenden, um Ihre Software-Assets und Lizenzen zu verwalten.

CA SAM hat folgende Vorteile:

- Unterstützt den Vorgang, Ihre Position der Softwarelizenz-Compliance festzulegen, indem die Anzahl der verfügbaren Lizenzen mit der Anzahl der verwendeten Lizenzen verglichen wird.
- Integriert eine Importfunktion der Softwarelizenz in die CA SAM-Anwenderoberfläche.
- Erleichtert die Erstellung und Wartung eines Softwarelizenzkatalogs mit detaillierten Geschäftsinformationen der Lizenzen.
- Weist Installationen und Nutzungsdaten zu definierten Produkten im Softwarelizenzkatalog zu.
- Führt Software-Produktanerkennung aus.
- Ermöglicht Finanzanalyse von Produktpreisen, Lizenzkosten und Vertragszahlungen (diese Funktion ist über ein zusätzliches Modul verfügbar).

Wenn Sie sowohl CA APM als auch CA SAM implementieren, können Sie das Management der Hardware- und Software-Assets in Ihrer Organisation koordinieren. CA APM verwaltet Hardware-Asset-Daten und CA SAM verwaltet Software-Asset und Lizenzdaten. Es werden allgemeine Daten freigegeben, die sowohl CA APM als auch CA SAM benötigen.

CA APM- und CA SAM-Datensynchronisation

Wenn Sie CA APM mit CA SAM implementieren, dann nutzen CA APM und CA SAM Daten gemeinsam, die für Hardware Asset Management und Software Asset Management erforderlich sind. Um die Integrität von Daten und dem Asset-Management-Prozess zu verwalten, müssen Daten zwischen CA APM und CA SAM synchronisiert sein. Die Datensynchronisation stellt sicher, dass Objekte, die sowohl in CA APM als auch in CA SAM identisch sind, die gleichen Datenwerte enthalten. Die Datensynchronisation findet auf folgende Weise statt:

- **Automatisch:** Wenn Sie die folgenden Objekte in CA APM erstellen, aktualisieren oder löschen (über die Anwenderoberfläche, Webservices oder Data Importer), werden die Objekte automatisch in CA SAM synchronisiert. Erstellen, aktualisieren oder löschen Sie nur die folgenden Objekte in CA APM.
 - Unternehmen
 - Lokation
 - Kostenstelle
 - Division
 - Kontakt

Wichtig! Der CA SAM-Administrator muss diese Objekte in CA SAM als schreibgeschützt festlegen, um unbefugte Änderung zu verhindern und um sicherzustellen, dass Daten richtig synchronisiert werden. Weitere Informationen zu dieser Anforderung finden Sie unter "Empfehlungen zur Datenverwaltung". Weitere Informationen über das Festlegen der schreibgeschützten Objekte in CA SAM finden Sie in der CA SAM-Dokumentation.

Hinweis: Diese Objekte verwenden die gleichen Bezeichnungen in CA APM und CA SAM, mit Ausnahme von "Kontakt". In CA SAM wird das Kontaktobjekt als "Anwender" bezeichnet.

Für "Kontakt", "Unternehmen" und "Lokation" tritt die automatische Synchronisierung nur für bestimmte Datentypen, wie in der folgenden Tabelle angezeigt, auf:

Objekt	Bei folgendem Typ automatisch synchronisieren
Kontakt	Anwender
Unternehmen	Intern

Objekt	Bei folgendem Typ automatisch synchronisieren
Lokation	NULL

- Manuell: Wenn Sie die folgenden Objekte in CA APM oder CA SAM erstellen oder aktualisieren, dann synchronisieren Sie die Objekte manuell. Erstellen oder aktualisieren Sie die folgenden Objekte in CA APM oder CA SAM.
 - Country
 - Region

Wenn Sie zum Beispiel ein Regionsobjekt in CA SAM erstellen, dann erstellen Sie manuell das gleiche Objekt in CA APM. Wenn Sie ein Regionsobjekt in CA APM aktualisieren, dann aktualisieren Sie manuell dieses Objekt in CA SAM.

Hinweis: Weitere Informationen zur manuellen Datensynchronisation finden Sie unter "Empfehlungen zur Datenverwaltung".

- Data Loading (Laden von Daten): Wenn Sie ein Upgrade von einer früheren Installation von CA APM Version 12.6 auf CA APM Version 12.8 durchführen, können Sie Ihre vorhandenen CA APM-Daten für Unternehmen, Lokation, Kostenstelle, Bereich und Kontakt in CA SAM laden. Weitere Informationen über das Laden von Daten finden Sie unter [Laden von CA APM-Daten in CA SAM](#) (siehe Seite 163).

So implementieren Sie CA SAM mit CA APM

Führen Sie folgende Schritte aus, um CA SAM mit CA APM zu implementieren:

1. [Überprüfen der Voraussetzungen](#) (siehe Seite 156).
2. [Überprüfen der Installation der Internetinformationsdienste](#) (siehe Seite 157).
3. [Installieren des CA SAM-Import- und Exportservices](#) (siehe Seite 158).
4. [Konfigurieren des CA SAM-Import- und Exportservices](#) (siehe Seite 158).
5. [Planen des Windows-Tasks für den Hardware-Import](#) (siehe Seite 160).
6. [Starten des CA APM-Event-Service](#) (siehe Seite 161).
7. [Aktivieren der Software Asset Management-Funktionen](#) (siehe Seite 161).
8. [Laden von CA APM-Daten in CA SAM](#) (siehe Seite 163).

Hinweis: Um CA SAM zu implementieren, müssen Sie auch die aktuelle Version des CA SAM-Katalogs von CA Support Online herunterladen und den Katalog in CA SAM anwenden. Sie können den Katalog herunterladen, bevor oder nachdem Sie CA SAM mit CA APM implementiert haben. Weitere Informationen über den CA SAM-Katalog finden Sie in der CA SAM-Dokumentation.

Überprüfen der Voraussetzungen

Überprüfen Sie folgende Voraussetzungen, um sicherzustellen, dass Sie CA SAM mit CA APM erfolgreich implementieren können.

- Sie haben CA APM installiert. Während der Installation haben Sie die Option für "Configure CA SAM Integration" (CA SAM-Integration konfigurieren) aktiviert.

Wichtig! Wenn Sie zuvor nicht die optionale Komponente "Event-Service" installiert haben, dann installieren Sie jetzt diese Komponente. Stellen Sie außerdem sicher, dass die CA APM-Workflow-Provider-URL zugreifbar ist und dass die entsprechenden Anmeldeinformationen gültig sind.

Hinweis: Wenn Ihre CA APM-Umgebung mit CA Service Desk Manager (CA SDM) integriert ist, stellen Sie sicher, dass der CA SDM-Audit-Verlauf aktiviert ist.

- Sie haben CA SAM vom CA SAM-Installationsdatenträger installiert. Weitere Informationen zur Installation von CA SAM finden Sie in der CA SAM-Dokumentation.

Wichtig! Microsoft .NET Framework 4.0 muss auch auf dem CA SAM-Server installiert sein.

Hinweis: Wenn Sie CA SAM verwenden, um Software-Assets für mehr als 250.000 Hardware-Assets zu verwalten, empfehlen wir folgende Installationskonfiguration, um eine bessere Systemleistung zu erzielen:

- Installieren Sie einen CA SAM-Staging-Server nur für die Verarbeitung von Discovery-Daten. Implementieren Sie den Staging-Server auf einer MySQL-Datenbank, um eine bessere Leistung und Skalierbarkeit zu erzielen.
- Installieren Sie den CA SAM-Betriebsserver entweder auf einer SQL Server-Datenbank oder auf einer Oracle-Datenbank.
- Übertragen Sie die Discovery-Daten auf den CA SAM-Betriebsserver, wenn die Verarbeitung auf dem Staging-Server abgeschlossen ist.

Überprüfen der Installation der Internetinformationsdienste

Der CA SAM-Import- und Export-Service wird installiert, wenn Sie die neuen CA APM-Komponenten installieren, die für die CA SAM-Implementierung erforderlich sind. Die Installation des CA SAM-Import- und Export-Services benötigt Internetinformationsdienste (IIS) 7.5, wobei die Funktionen "ASP.NET" und "WCF-Aktivierung" aktiviert sein müssen. Bevor Sie mit der Installation des CA SAM-Import- und Export-Services beginnen, stellen Sie sicher, dass IIS installiert ist und dass die erforderlichen Funktionen auf dem Server, wo CA SAM installiert ist, aktiviert sind.

So überprüfen Sie die Installation der Internetinformationsdienste:

1. Melden Sie sich für jede Anwendung und jeden Webserver am Server an.
2. Öffnen Sie die Systemsteuerung (Verwaltung, Dienste).
3. Stellen Sie sicher, dass sich der IIS-Admin-Dienst auf dem Server befindet.

So installieren Sie IIS-Version 7.5 unter Windows Server 2008 R2:

1. Wählen Sie über "Server-Manager" die Option "Rollen" aus.
2. Klicken Sie im Bereich "Rollenübersicht" auf "Rollen hinzufügen", und klicken Sie auf "Weiter".

Das Dialogfeld "Serverrollen auswählen" wird angezeigt.

3. Wählen Sie "Anwendungsserver" aus der Liste "Rollen" aus, und klicken Sie zweimal auf "Weiter".

Das Dialogfeld "Rollendienste auswählen" für die Rolle "Anwendungsserver" wird angezeigt.

4. Wählen Sie "Unterstützung von Webservern (IIS)" aus, und wählen Sie unter "Unterstützung des Aktivierungsdienstes für Windows-Prozesse" die Option "HTTP-Aktivierung".
5. Wenn Sie aufgefordert werden, mehr weitere Rollendienste und Funktionen zu installieren, klicken Sie auf "Erforderliche Rollendienste hinzufügen", und klicken Sie zweimal auf "Weiter".
6. Stellen Sie sicher, dass die Zusammenfassung der Auswahl korrekt ist, und klicken Sie auf "Installieren".
7. Klicken Sie auf "Schließen", nachdem die Installation fertiggestellt wurde.

Installieren des CA SAM-Import- und Exportservices

Installieren Sie die Komponente des CA SAM-Import- und Exportservices auf dem CA SAM-Server.

Wichtig! Microsoft .NET Framework 4.0 muss auf dem CA SAM-Server installiert sein, bevor Sie den CA SAM-Import- und Exportservice installieren.

Gehen Sie wie folgt vor:

1. Melden Sie sich beim CA SAM-Server an.
2. Navigieren Sie zum Ordner "SetupFiles\SAMImportExportService" auf dem CA APM-Installationsdatenträger. Kopieren Sie den Ordner und den gesamten Inhalt in einen lokalen Ordner auf dem CA SAM-Server.
3. Führen Sie im Ordner "SAMImportExportService" auf dem CA SAM-Server den Befehl "SAMService.bat" aus.

Es wird eine Aufforderung für den Installationsstammpfad angezeigt.

4. Geben Sie den ITAM-Stammpfad für die Installation der CA SAM-Import- und Export-Service-Komponente ein.

Folgendes Beispiel zeigt den empfohlenen Pfad an.

Beispiel:

C:\Programme\CA\ITAM

Sie haben die Installation des CA SAM-Import- und Exportservices abgeschlossen.

Konfigurieren des CA SAM-Import- und Export-Services

Der CA SAM-Import und Export-Service exportiert erkannte Hardware-Daten nach CA APM. Dieser Service erhält Exporte von Eigentumsdaten von CA APM und aktualisiert Asset-Informationen in CA SAM. Dieser Service erhält auch die Exporte der automatischen Datensynchronisation (Unternehmen, Lokation, Kostenstelle, Bereich und Kontakt) von CA APM, und der Service aktualisiert die Informationen in CA SAM.

Gehen Sie wie folgt vor:

1. Melden Sie sich beim CA SAM-Server an.
2. Navigieren Sie zum folgenden Speicherort:
[ITAM-Stammverzeichnis]\ITAM\SAMImportExportService
3. Öffnen Sie die Datei "web.config" in einem Texteditor.

4. Bearbeiten Sie den Pfad des Importordners, indem Sie folgende Schritte durchführen.

- a. Suchen Sie nach der folgenden Anweisung:

```
<add key="ImportFolderPath" value="[Pfad des Importordners]"/>
```

- b. Ersetzen Sie [Pfad des Importordners] durch den Pfad des Superuser-Ordners unter dem Ordner für Datenaustausch. Der Ordner für Datenaustausch befindet sich im CA SAM-Installationsordner.

Beispiel: C:\Programme(x86)\ca_sam\app\uploads\
prod\data_exchange\superuser

5. Bearbeiten Sie den Pfad des Exportordners, indem Sie folgende Schritte durchführen.

- a. Suchen Sie nach der folgenden Anweisung:

```
<add key="ExportFolderPath" value="[Pfad des Exportordners]"/>
```

- b. Ersetzen Sie [Pfad des Exportordners] durch den Pfad des "in"-Ordners unter dem Superuser-Ordner. Der Ordner "superuser" befindet sich unter dem Ordner für Datenaustausch, der sich unter dem CA SAM-Installationsordner befindet.

Beispiel: C:\Programme(x86)\ca_sam\app\uploads\
prod\data_exchange\superuser\in

6. Speichern Sie die Datei "web.config".

7. Navigieren Sie zum folgenden Speicherort:

[ITAM-Stammverzeichnis]\ITAM\SAMImportExportService\data_exchange

8. Konfigurieren Sie den Geräteexport, indem Sie eine der folgenden Dateien in den Exportordnerpfad kopieren:

- CA_SAM_Device_Export_SQL.xml (für eine SQL Server-Datenbank)
- CA_SAM_Device_Export_ORA.xml (für eine Oracle-Datenbank)

Beispiel: C:\Programme(x86)\ca_sam\app\uploads\
prod\data_exchange\superuser\in

9. Bearbeiten Sie den cron-Job "data_exchange" von CA SAM, um das Zeitintervall mithilfe der folgenden Schritte anzupassen.

- a. Melden Sie sich bei CA SAM als Administrator an.
- b. Klicken Sie auf "Admin", "Konfiguration", "Cron-Jobs".
- c. Klicken Sie auf das Bearbeitungssymbol für den Cron-Job "data_exchange".
Das Dialogfeld "Datensatz bearbeiten" wird angezeigt.

- d. Löschen Sie die folgenden Felder: Startzeit (Stunde), Startzeit (Minute).
 - e. Geben Sie einen Wert (zum Beispiel "5") in das folgende Feld ein: Intervall (Minuten).
 - f. Klicken Sie auf "Speichern".
Das Dialogfeld wird geschlossen.
 - g. Klicken Sie auf das Startsymbol für den Cron-Job "data_exchange".
Das Dialogfeld "Start cron job" (Cron-Job starten) wird angezeigt.
 - h. Klicken Sie auf "Start cron job" (Cron-Job starten).
Das Dialogfeld wird geschlossen.
- Die Konfiguration des CA SAM-Import- und Export-Services ist abgeschlossen.

Planen der Windows-Aufgabe für den Hardware-Import

Verwenden Sie den Windows-Taskplaner, um den Import der erkannten Hardware-Daten von CA SAM in CA APM zu planen. Folgender Vorgang plant den Importvorgang zur täglichen Ausführung.

Hinweis: Dieser Vorgang beschreibt die Verwendung des Windows-Taskplaners. Sie können allerdings auch einen anderen Aufgabenplaner oder ein anderes Prozessabstimmungs-Tool verwenden.

Befolgen Sie diese Schritte für Windows Server 2008:

1. Öffnen Sie auf dem CA APM-Anwendungsserver das Startmenü und den Windows-Taskplaner.
Gehen Sie zum Beispiel unter Windows Server 2008 auf "Systemsteuerung", "System und Sicherheit", "Systemverwaltung", "Aufgaben planen".
2. Klicken Sie auf "Aufgabe erstellen".
3. Geben Sie auf der Registerkarte "Allgemein" einen Namen für die Aufgabe ein.
4. Aktivieren Sie das Kontrollkästchen "Unabhängig von der Benutzeranmeldung ausführen".
5. Navigieren Sie zur Registerkarte "Aktionen", und klicken Sie auf "Neu".
6. Wählen Sie im Feld "Aktion" die Option "Programm starten" aus.
7. Suchen Sie über das Feld "Programm/Skript" den Ordner "Import Driver Program", wählen Sie die Datei "ImportDriver.exe" aus, und klicken Sie auf "OK".
8. Navigieren Sie zur Registerkarte "Trigger", und klicken Sie auf "Neu".
9. Wählen Sie im Einstellungsfeld die Option "Täglich" aus.
10. Wählen Sie im Startfeld "12:00:00" aus.

11. Wählen Sie "Jeden 1 Tag" aus, und klicken Sie auf "OK".
 12. Klicken Sie im Dialogfeld "Aufgabe erstellen" auf "OK".
- Sie haben die Planung der Windows-Aufgabe zum Importieren von erkannten Hardware-Daten fertiggestellt.

Starten des CA APM-Event-Service

Wenn Sie ein Upgrade von einer früheren CA APM-Version durchführen, starten Sie den CA APM-Event-Service, um die Implementierung von CA SAM mit CA APM abzuschließen:

Gehen Sie wie folgt vor:

1. Öffnen Sie im Startmenü auf dem CA APM-Anwendungsserver die Systemsteuerung, Verwaltung, Dienste.
 2. Suchen Sie den Eintrag für CA Asset Portfolio Management - Event-Service.
 3. Klicken Sie mit der rechten Maustaste auf den Dienst, und wählen Sie "Starten" aus.
- Der Service wird gestartet.

Aktivieren der Software Asset Management-Funktionen

Nachdem Sie alle CA APM-Komponenten installiert und konfiguriert haben, aktivieren Sie die Software Asset Management-Funktionen in CA APM.

Hinweis: Wenn Sie derzeit eine Integration zwischen CA APM und CA Software Compliance Manager haben, deinstallieren Sie CA SCM, bevor Sie die Software Asset Management-Funktionen aktivieren. Weitere Informationen zur Deinstallation von CA SCM finden Sie unter "So deinstallieren Sie CA Software Compliance Manager". Für weitere Informationen darüber, wie und wann CA SCM deinstalliert werden sollte, kontaktieren Sie Ihrer CA Services-Beauftragten.

Hinweis: Wenn Sie Software Asset Management-Funktionen in einer früheren Version aktiviert haben und Sie jetzt ein Upgrade durchführen, dann überspringen Sie die folgenden Schritte. Sie müssen allerdings die Konfigurationsdatei "web.config" auf dem CA APM-Webserver aktualisieren, um den CA SAM-Abschnitt der allgemeinen Startseite anzuzeigen. Aktualisieren Sie folgende Anweisung:

```
<add key="CASAMWebClientUrl" value="http://CA_SAM_server_name/prod" />
```

Beispiel:

```
<add key="CASAMWebClientUrl" value="http://itamsam/prod" />
```

Gehen Sie wie folgt vor:

1. Melden Sie sich bei CA APM auf dem Webserver als Administrator an.
2. Navigieren Sie zu "Verwaltung", "Systemkonfiguration", "Software Asset Management".
3. Geben Sie die Web-Client-URL für die CA SAM-Startseite ein.

Hinweis: Sie können die Web-Client-URL auf der CA SAM-Startseite kopieren, nachdem Sie sich angemeldet haben.

4. Geben Sie die Webservice-URL für CA SAM-Import/-Export im folgenden Format ein:

`http://[CA SAM-Systemname]:[Portnummer]/SAMImportExportService/Service.svc`

- a. Ersetzen Sie [CA SAM-Systemname] durch den Namen des CA SAM-Servers.
 - b. Ersetzen Sie [Portnummer] durch die Portnummer, wo der CA SAM-Import- und Export-Service gehostet wird.
5. Aktivieren Sie das Kontrollkästchen "SAM-Funktionen aktivieren", und klicken Sie auf "Speichern".
 6. Starten Sie die Internetinformationsdienste (IIS) neu, indem Sie folgende Schritte ausführen:
 - a. Öffnen Sie auf den CA APM-Webservern und -Anwendungsservern ein Fenster zur Eingabeaufforderung.
 - b. Führen Sie folgenden Befehl aus:

```
iisreset
```

Software Asset Management-Funktionen werden aktiviert, und CA SCM-Felder werden aus der CA APM-Anwenderoberfläche entfernt.

Hinweis: Die Schaltfläche "Daten laden" wird aktiviert, wenn CA APM-Daten vorhanden sind (wenn Sie z. B. eine vorhandene Installation von CA APM 12.6 hätten und ein Upgrade durchführen). Diese Schaltfläche ermöglicht es Ihnen, vorhandene CA APM-Daten für ausgewählte Objekte in CA SAM zu laden. Weitere Informationen über das Laden von Daten finden Sie unter [Laden von CA APM-Daten in CA SAM](#) (siehe Seite 163). Diese Schaltfläche wird nicht aktiviert, wenn Sie eine neue Installation von CA APM ausführen, da Sie keine vorhandenen Daten mit einer neuen Installation haben.

Laden von CA APM-Daten in CA SAM

Nachdem Sie Software Asset Management-Funktionen in CA APM aktiviert haben, können Sie vorhandene CA APM-Daten für ausgewählte Objekte in CA SAM laden. Diese Datenladung ermöglicht es Ihnen, die Daten zu synchronisieren, sodass Objekte, die in CA APM und CA SAM übereinstimmen, die gleichen Datenwerte haben. Zu den CA APM-Daten, die Sie laden können, gehören folgende Objekte:

- Lokation
- Division
- Unternehmen
- Kostenstelle
- Kontakt

Wenn Sie eine frühere Installation von CA APM hatten, haben Sie vorhandene CA APM-Daten für diese Objekte. Wenn Sie eine neue Installation von CA APM ausführen, haben Sie keine vorhandenen Daten.

Hinweis: Bevor Sie CA APM-Daten in CA SAM laden, stellen Sie sicher, dass Ihre CA APM-Daten die CA SAM-Anforderungen erfüllen. Diese Anforderungen sind unter "Feldanforderungen für automatische Datensynchronisation" angegeben.

Gehen Sie wie folgt vor:

1. Auf der Seite "Verwaltung", "Systemkonfiguration", "Software Asset Management" müssen Sie sicherstellen, dass die Schaltfläche "Daten laden" aktiviert ist.

Hinweis: Die Schaltfläche "Daten laden" wird aktiviert, wenn CA APM-Daten vorhanden sind (wenn Sie z. B. eine vorhandene Installation von CA APM 12.6 hätten und ein Upgrade durchführen).

2. Klicken Sie auf "Daten laden".

Die Datenladung kopiert die Objektwerte von "Lokation", "Bereich", "Unternehmen", "Kostenstelle" und "Kontakt" nach CA SAM. Eine Statustabelle zeigt den Fortschritt der Datenladung an.

Wenn einige Objekte nicht CA SAM synchronisiert werden können, dann werden die Fehlerdatensätze in eine Protokolldatei geschrieben. Sie können diese Protokolldatei anzeigen, indem Sie auf die Schaltfläche "Fehlerdatensätze abrufen" klicken. Die Schaltfläche "Fehlerdatensätze abrufen" ist nur verfügbar, nachdem Sie die SAM-Funktionen aktiviert haben.

3. Klicken Sie auf "Fehlerdatensätze abrufen", um zu überprüfen, ob Datensynchronisationsfehler aufgetreten sind.

Sie werden aufgefordert, eine CSV-Datei zu öffnen oder zu speichern. Wenn Fehler in der CSV-Datei vorhanden sind, werden die Fehler nach Objekt in der folgender Reihenfolge gruppiert:

- Lokation
- Division
- Unternehmen
- Kostenstelle
- Kontakt

4. Überprüfen Sie die Fehler und Erklärungen in der CSV-Datei, und korrigieren Sie die CA APM-Objektdaten.

Die korrigierten Objekte werden während der nächsten Datensynchronisation mit CA SAM synchronisiert.

Empfehlungen zur Datenverwaltung

Die Empfehlungen in diesem Abschnitt helfen Ihnen dabei, Ihre Daten zu verwalten, wenn CA APM mit CA SAM implementiert ist.

Manuelle Datensynchronisation

Daten müssen zwischen CA APM und CA SAM synchronisiert werden, um die Integrität von den Daten und vom Asset-Management-Prozess beizubehalten. Die Datensynchronisation stellt sicher, dass Objekte, die sowohl in CA APM als auch in CA SAM identisch sind, die gleichen Datenwerte enthalten.

Wenn Sie die Objekte "Land" und "Region" in CA APM oder CA SAM erstellen oder aktualisieren, dann synchronisieren Sie die Objekte manuell. Wenn Sie zum Beispiel ein Regionsobjekt in CA SAM erstellen, dann erstellen Sie manuell das gleiche Objekt in CA APM. Wenn Sie ein Regionsobjekt in CA APM aktualisieren, dann aktualisieren Sie manuell dieses Objekt in CA SAM.

Manuelle Datensynchronisationsregeln

Um sicherzustellen, dass Daten richtig synchronisiert werden, verwenden Sie folgende Regeln, wenn Sie die Objekte "Land" und "Region" erstellen oder aktualisieren:

- Land: Die CA APM-Abkürzung für ein Land muss mit der CA SAM-Datensatzimport-ID für das gleiche Land übereinstimmen.
- Region: Der CA APM-Name für eine Region muss mit der CA SAM-Datensatzimport-ID für die gleiche Region übereinstimmen.

Datenverwaltung der Kostenstelle

Die Datensynchronisation zwischen CA APM und CA SAM stellt die Integrität von den Daten und vom Asset-Management-Prozess sicher. Diese Synchronisation tritt für die folgenden Objekte automatisch auf:

- Unternehmen
- Lokation
- Kostenstelle
- Division
- Kontakt

Hinweis: Diese Objekte verwenden die gleichen Bezeichnungen in CA APM und CA SAM, mit Ausnahme von "Kontakt". In CA SAM wird das Kontaktobjekt als "Anwender" bezeichnet.

Wenn Sie die Objekte "Kontakt", "Unternehmen", "Lokation" und "Unternehmensbereiche" in CA APM erstellen, aktualisieren oder löschen, werden die Objekte automatisch in CA SAM synchronisiert. Der CA SAM-Administrator muss "Kontakt", "Unternehmen", "Lokation" und "Unternehmensbereiche" in CA SAM als schreibgeschützt festlegen. Dadurch wird verhindert, dass der CA SAM-Anwender diese Objekte ändert, die überschrieben werden, wenn die nächste Datensynchronisation durchgeführt wird. Allerdings kann der Administrator das Objekt "Kostenstelle" in CA SAM nicht als schreibgeschützt festlegen, da die Berichterstellungshierarchie der Kostenstelle in CA SAM verwaltet werden muss.

Empfohlene Richtlinien für die Datenverwaltung der Kostenstelle

Um die Datenverwaltung der Kostenstelle zu erleichtern, empfehlen wir, dass Sie folgende Richtlinien verwenden:

- Fügen Sie einer Administratorrolle in CA SAM Berechtigungen hinzu, um das Objekt "Kostenstelle" zu verwalten. Andere Anwenderrollen können nicht auf das Objekt "Kostenstelle" zugreifen.
- Verwenden Sie CA APM, wenn Sie folgende Aktionen ausführen:
 - Einfügen oder Löschen von Kostenstellen.
 - Aktualisieren des Namens oder der Beschreibung der Kostenstelle.

Wichtig! Wenn Sie den Namen oder die Beschreibung der Kostenstelle in CA SAM ändern, werden die Änderungen nach der nächsten Datensynchronisation überschrieben.
- Verwenden Sie CA SAM, wenn Sie folgende Aktionen ausführen:
 - Verwalten der Berichterstellungshierarchie der Kostenstelle.
 - Zuweisen einer Kostenstelle zu einem Land.

Maßeinheiten des Inventars

CA SAM sendet CA APM Hardware-Discovery-Daten zur Hilfe beim Hardware-Asset-Management. CA APM benötigt bestimmte Maßeinheiten für folgende Hardware-Inventarelemente, die von CA SAM gesendet werden:

- Gesamter Festplattenspeicher: Gigabyte (GB)
- Gesamter Speicher: Megabyte (MB)
- Prozessorgeschwindigkeit (CPU): Megahertz (MHz)

Wenn Sie Hardware-Inventardaten für diese Elemente in CA SAM laden und verwalten, stellen Sie sicher, dass die CA SAM-Daten diese Maßeinheiten verwenden.

Feldanforderungen für automatische Datensynchronisation

Die automatische Datensynchronisation kopiert die CA APM-Daten für die Objekte "Unternehmen", "Lokation", "Kostenstelle", "Unternehmensbereiche" und "Kontakt" in die entsprechenden Objekte in CA SAM. Um eine erfolgreiche Synchronisierung sicherzustellen, befolgen Sie die Richtlinien der Feldanforderung für die Objekte in den folgenden Unterabschnitten.

Kontakt

Einige Felder für das Objekt "Kontakt" sind optional in CA APM, in CA SAM sind sie jedoch erforderliche Felder. Diese Felder sind in der folgenden Tabelle zusammengefasst. Stellen Sie sicher, dass alle Felder, die in CA SAM erforderlich sind, Daten in CA APM enthalten.

CA APM-Feld	Erforderlich in CA APM?	Erforderlich in CA SAM?
Anwender-ID/Anwendername	Nein	Ja
Kostenstelle	Nein	Ja
Nachname	Ja	Ja
Vorname	Nein	Ja

Unternehmen

CA SAM ermöglicht Ihnen eine Compliance-Berichterstellung für hierarchische Gruppierungen (Bereich, Unternehmen und Kostenstelle). Um über Unternehmensbereiche zu berichten, benötigt CA SAM Details zu Unternehmensbereichen für das Objekt "Unternehmen". Stellen Sie sicher, dass das Objekt "Unternehmen" von CA APM Details zu Unternehmensbereiche hat, um eine erfolgreiche Datensynchronisation zu sichern.

Hinweis: Um Details zu Unternehmensbereichen für ein Unternehmen in CA APM einzugeben, erstellen Sie zunächst Bereiche in "Verzeichnis", "Listenverwaltung", "Unternehmenslisten", "Unternehmensbereiche". Anschließend erstellen oder aktualisieren Sie ein Unternehmen auf der Seite "Details zum Unternehmen". Wählen Sie einen internen Unternehmenstyp aus. Das Textfeld "Unternehmensbereiche" wird angezeigt, und Sie können einen Bereich für das Unternehmen auswählen.

Kostenstelle

CA SAM ermöglicht Ihnen eine Compliance-Berichterstellung für hierarchische Gruppen (Bereich, Unternehmen und Kostenstelle). Um einen Bericht über Unternehmen erstellen zu können, benötigt CA SAM Unternehmensinformationen für das Objekt "Kostenstelle". Stellen Sie sicher, dass das Objekt "Kostenstelle" von CA APM Details zum Unternehmen hat, um eine erfolgreiche Datensynchronisation zu sichern.

Assets mit nicht definierten Betriebssystemen

Discovery-Daten, die CA APM erhält, können Betriebssystemnamen enthalten, die nicht in CA APM angegeben sind. In diesem Fall weist CA APM dem entsprechenden Asset den Betriebssystemwert "Nicht definiert" zu. CA APM zeigt den Wert ""Nicht definiert"" im Feld "Betriebssystem" auf der Seite "Asset-Details" an.

Sie können die ursprünglich erkannten Namen der nicht definierten Betriebssysteme anzeigen, und Sie können diese Namen zu den CA APM-Betriebssystemnamen hinzufügen. Sie können auch die Assets aktualisieren, die nicht definierte Betriebssysteme haben, um die neuen Namen einzuschließen.

Hinweis: CA APM kann Daten mit nicht definierten Betriebssystemen aus einer beliebigen Discovery-Quelle erhalten (einschließlich CA SAM).

Führen Sie diese Schritte aus, um die ursprünglichen Namen der nicht definierten Betriebssysteme anzuzeigen:

1. Melden Sie sich bei CA APM als Administrator an.
2. Navigieren Sie zu "Verwaltung", "Abgleichsverwaltung", "Abgleich - Nachrichtensuche".
Eine Liste der Abgleichsmeldungen wird angezeigt.
3. Suchen Sie die Meldungen, die die fehlenden Betriebssysteme identifizieren.

Hinweis: Sie können auf dieser Seite nach "Fehlendes Betriebssystem" im Nachrichtentext suchen.

Die Meldungen enthalten die ursprünglich erkannten Namen.

Führen Sie diese Schritte durch, um Assets mit nicht definierten Betriebssystemen zu aktualisieren:

1. Navigieren Sie zu "Verzeichnis", "Listenverwaltung", "Betriebssystem", und fügen Sie den CA APM-Namen die fehlenden Betriebssystemnamen hinzu.
2. Aktualisieren Sie ein individuelles Asset mit einem nicht definierten Betriebssystem, indem Sie folgende Schritte durchführen:
 - a. Navigieren Sie zur Seite "Asset-Details" für ein Asset mit einem nicht definierten Betriebssystem.
 - b. Klicken Sie auf das Symbol "Neue Auswahl" im Feld "Betriebssystem", und wählen Sie den neuen Namen aus.
3. Aktualisieren Sie mehrere Assets mit nicht definierten Betriebssystemen, indem Sie folgende Schritte durchführen:
 - a. Navigieren Sie zu "Verwaltung", "Abgleichsverwaltung".
 - b. Klicken Sie auf Sie den Regelnamen des Abgleichs.
Die Seite "Abgleichsregel - Details" wird für die ausgewählte Regel angezeigt.
 - c. Stellen Sie sicher, dass "Asset-Aktualisierungen überwachen" aktiviert ist.
 - d. Im Bereich "Aktualisierungsoptionen" wählen Sie "Betriebssystem" und "Datum der letzten Ausführung" aus.
 - e. Klicken Sie auf "Speichern".

Wenn CA APM neue Discovery-Daten für Assets mit nicht definierten Betriebssystemen erhält, aktualisiert CA APM die Betriebssysteme mit den neuen Namen, die Sie eingegeben haben.

So deinstallieren Sie CA Software Compliance Manager

Um SAM-Funktionen zu aktivieren, wenn CA APM mit CA Software Compliance Manager (CA SCM) integriert ist, deinstallieren Sie CA SCM.

Hinweis: Stellen Sie sicher, dass alle Anwender in CA SCM abgemeldet sind. Anwender, die sich nicht vom Produkt abgemeldet haben, bevor die Deinstallation beginnt, erhalten eine Fehlermeldung beim Versuch, eine Aufgabe abzuschließen.

Führen Sie diese Schritte durch, um CA SCM 12.0 zu deinstallieren:

1. Melden Sie sich bei dem Computer an, auf dem CA SCM 12.0 installiert ist.
2. Deinstallieren Sie kumulative Patches von CA SCM Version 12.0, sofern vorhanden, über "Systemsteuerung", "Programme hinzufügen oder entfernen".
3. Melden Sie sich beim CA APM-Anwendungsserver an, auf dem CA APM Version 12.8 installiert ist.
4. Navigieren Sie zum Ordner, wo Sie CA APM Version 12.8 installiert haben.
5. Kopieren Sie den Ordner "SWCM12.0Uninstall" mit dem gesamten Inhalt in einen temporären Speicherort auf jedem Computer (außer dem Datenbankserver), wo Sie CA SCM 12.0 installiert haben.

Beispiel für einen temporären Speicherort:

C:\Windows\Temp

6. Navigieren Sie zum Ordner "Uninstall" im temporären Speicherort auf dem CA SCM 12.0-Computer.
7. Starten Sie die Deinstallation, indem Sie zweimal auf die Datei "SWCM_Uninstall.bat" klicken.
8. Folgen Sie im Deinstallationsvorgang den Anweisungen auf dem Bildschirm.

Die Deinstallation wird ausgeführt und entfernt erfolgreich alle installierten CA SCM 12.0-Komponenten, außer CA Business Intelligence BusinessObjects Enterprise, CA EEM, CA MDB und Content Import Client.

Führen Sie diese Schritte durch, um CA SCM 12.6 zu deinstallieren:

Hinweis: Führen Sie für die standardmäßige und die Demo-Installation diese Schritte auf jedem Computer (außer dem Datenbankserver) aus, auf dem CA SCM 12.6 installiert ist.

1. Melden Sie sich bei dem Computer an, auf dem CA SCM 12.6 installiert ist.
2. Deinstallieren Sie kumulative Patches von CA SCM Version 12.6, sofern vorhanden, über "Systemsteuerung", "Programme hinzufügen oder entfernen".

3. Navigieren Sie zum Ordner "Uninstall", wo CA SCM 12.6 installiert ist.

Beispiel:

C:\Programme\CA\SWCM\Uninstall

4. Starten Sie die Deinstallation, indem Sie zweimal auf die Datei "SWCM_Uninstall.bat" klicken.
5. Folgen Sie im Deinstallationsvorgang den Anweisungen auf dem Bildschirm.

Die Deinstallation wird ausgeführt und entfernt erfolgreich alle installierten CA SCM 12.6-Komponenten, außer CA Business Intelligence BusinessObjects Enterprise, CA EEM, CA MDB und Content Import Client.

Kapitel 9: Fehlerbehebung

Dieses Kapitel enthält folgende Themen:

[Fehlermeldung, dass die Installation nicht gestartet oder der angezeigte Server nicht gefunden wird](#) (siehe Seite 171)

[Browser-Fehlermeldung, dass Mandantenverwaltungs-Seite nicht angezeigt werden kann, wird angezeigt](#) (siehe Seite 171)

[Mandantenverwaltungs-Seite wird nicht angezeigt](#) (siehe Seite 172)

[Webserver benannt mit Unterstreichungszeichen](#) (siehe Seite 172)

[Anmeldung schlägt mit einem Anwendernamen fehl, der zusätzliche Zeichen enthält](#) (siehe Seite 172)

[WCF-Services schlagen fehl, wenn IIS 7 auf Windows 2008 installiert ist](#) (siehe Seite 173)

[Meldungen über fehlende Betriebssysteme werden in der Nachrichtenwarteschlange angezeigt](#) (siehe Seite 173)

Fehlermeldung, dass die Installation nicht gestartet oder der angezeigte Server nicht gefunden wird

Gültig in allen unterstützten Betriebsumgebungen.

Symptom:

Beim Start der CA APM-Installation startet die Installation nicht oder Sie erhalten eine Fehlermeldung, dass der Server nicht gefunden werden konnte.

Lösung:

Starten Sie den Windows-Dienst "Utildev Web Server Pro" neu.

Browser-Fehlermeldung, dass Mandantenverwaltungs-Seite nicht angezeigt werden kann, wird angezeigt

Symptom:

Die folgende Browserfehlermeldung wird angezeigt, wenn ich auf "Verwaltung", "Mandantenverwaltung" klicke:

Seite kann nicht angezeigt werden.

Lösung:

Stellen Sie sicher, dass der CA CASM-Dienst gestartet ist.

Mandantenverwaltungs-Seite wird nicht angezeigt

Symptom:

Wenn ich auf die Registerkarte "Verwaltung" klicke, sehe ich keine Mandantenverwaltungsoption.

Lösung:

Ihr CA APM-Administrator hat Sie keiner Rolle zugewiesen, in der der Mandantenverwaltungszugriff aktiviert ist. Wenn Sie auf die Mandantenverwaltung zugreifen müssen, setzen Sie sich mit Ihrem CA APM-Administrator in Verbindung.

Webserver benannt mit Unterstreichungszeichen

Gültig in allen unterstützten Betriebsumgebungen.

Symptom:

Die Verwendung von Unterstreichungszeichen in Webserver-Hostnamen kann zu Problemen führen, wenn Sie sich am Produkt anmelden oder CA EEM für die Anwenderkonfiguration verwenden.

Lösung:

Wenn Sie ein virtuelles oder gehostetes System verwenden, konfigurieren Sie einen neuen Hostnamen, indem Sie ein anderes Image ohne Unterstreichungszeichen erstellen. Fügen Sie für ein Produktionssystem Ihrem internen Domain Name System (DNS) einen neuen Hostnamen hinzu, so dass auf das Produkt mit einer anderen URL zugegriffen werden kann.

Anmeldung schlägt mit einem Anwendernamen fehl, der zusätzliche Zeichen enthält

Symptom:

Wenn ich CA EEM mit einer einzelnen DB-Anmeldungsauthentifizierung verwende, kann ich mich nicht an der CA APM-Webbenutzeroberfläche anmelden.

Lösung:

Wählen Sie einen Anwendernamen aus, der keine zusätzlichen Zeichen enthält (d.h. japanische oder deutsche Zeichen).

WCF-Services schlagen fehl, wenn IIS 7 auf Windows 2008 installiert ist

Zulässig in Umgebungen, die Windows 2008 verwenden.

Symptom:

Wenn Microsoft-Internetinformationsdienste 7 (IIS) auf Windows 2008 installiert ist, funktionieren die WCF-Services nicht. CA APM verwendet einen WCF-Service, um die Webdienst-Funktion zu implementieren.

Lösung:

Dieses Problem tritt auf, weil die Typen der Dienstdatei falsch zugeordnet sind oder die Windows-Komponenten, einschließlich IIS 7, in der falschen Reihenfolge installiert wurden. Um das Problem zu beheben, überprüfen und ändern Sie (im Bedarfsfall) die IIS-Einstellungen. Microsoft stellt Informationen und Lösungen für das Problem bereit.

Führen Sie die folgenden Schritte durch, um das Problem zu lösen:

1. Öffnen Sie in einem Web-Browser die Microsoft-Website (<http://www.microsoft.com>) und suchen Sie nach "IIS-gehosteter Dienst schlägt fehl".
2. Folgen Sie den Anweisungen im Artikel.

Meldungen über fehlende Betriebssysteme werden in der Nachrichtenwarteschlange angezeigt

Symptom:

Während die Abgleichs-Engine Normalisierungsregeln verarbeitet, erhalte ich eine der folgenden Fehlermeldungen in der Nachrichtenwarteschlange:

- Folgende durch Discovery ermittelte Betriebssysteme fehlen in der Liste der öffentlichen Betriebssysteme:
Fehlendes Betriebssystem: *Name des Betriebssystems*
- Folgende durch Discovery ermittelte Betriebssysteme fehlen in der Liste der Betriebssysteme und müssen zur Liste der öffentlichen Betriebssysteme oder zur Liste für folgenden Mandanten hinzugefügt werden: *Mandantenname*
Fehlendes Betriebssystem: *Name des Betriebssystems*

Hinweis: Die Abgleichs-Engine schreibt Meldungen zur Nachrichtenwarteschlange in der Datenbank. Legen Sie die Debug-Ebene der Engine in den Konfigurationseinstellungen der Hardware-Abstimmungs-Engine auf "Schwerwiegend" fest (oder auf eine höhere Detailebene), damit diese Fehlermeldungen in der Nachrichtenwarteschlange angezeigt werden. Weitere Informationen über die Nachrichtenwarteschlange und die Konfigurationseinstellungen finden Sie im *CA APM-Administrationshandbuch*.

Lösung:

Die Normalisierungsregeln gelten für alle Mandanten und öffentlichen Daten und können über Mandanten verwendet werden. Wenn ein durch die Normalisierungsliste zugewiesener Betriebssystemwert nicht für den Mandanten existiert, erstellt die Abgleichs-Engine eine Fehlermeldung, die Sie darüber informiert, dass das Betriebssystem für diesen Mandanten oder als öffentliche Daten hinzugefügt werden muss.

Hinweis: Weitere Informationen zu Normalisierungsregeln finden Sie im *CA APM-Administrationshandbuch*.

Wenn ein oder zwei Betriebssysteme fehlen, können Sie das Problem beheben, indem Sie die Betriebssysteme manuell zu den Normalisierungsregeln hinzufügen. Informationen über die Definition der Normalisierungsregeln eines Betriebssystems finden Sie im *CA APM-Administrationshandbuch*.

Wenn mehrere Betriebssysteme fehlen, gehen Sie folgendermaßen vor, um das Problem zu beheben:

1. Melden Sie sich in CA APM an, und klicken Sie auf "Verwaltung", "Abgleichsverwaltung".
2. Klicken Sie im linken Bereich auf "Abgleichsmeldung - Suche".
Die Nachrichtenwarteschlange zeigt im Bereich "Suchergebnisse" Abgleichsprotokollmeldungen an.
3. Suchen Sie die Fehlermeldungen der Normalisierungsregeln für fehlende Betriebssysteme.
Die Nachrichtenwarteschlange zeigt alle Fehlermeldungen der Normalisierungsregeln für fehlende Betriebssysteme an.
4. Stellen Sie sicher, dass die E-Mail-Adresse des Systemadministrators im Produkt korrekt ist, und klicken Sie auf "Nach CSV exportieren".
Die fehlenden Betriebssysteme werden in eine CSV-Datei exportiert. Der Systemadministrator erhält eine E-Mail mit einer Verknüpfung zur CSV-Datei.

5. Bearbeiten Sie den Inhalt der CSV-Datei, um die Datei für den Data Importer vorzubereiten. Sie können beispielsweise doppelte Betriebssysteme oder überflüssige Wörter aus der Datei entfernen.

Hinweis: Weitere Informationen zur Verwendung von Data Importer finden Sie im *Administrationshandbuch*.

6. Melden Sie sich bei CA APM an, klicken Sie auf "Verwaltung", Data Importer, und wählen Sie den Mandanten oder die öffentlichen Daten aus, die in den Betriebssystemen fehlen.
7. Importieren Sie die CSV-Datei.

Die fehlenden Betriebssysteme werden in die CA MDB importiert und können während des Normalisierungsprozesses der Abgleichs-Engine verwendet werden.