CA Identity Manager™

Implementierungshandbuch

12.6.5

CA Technologies-Produktreferenzen

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

- CA CloudMinder™ Identity Management
- CA Directory (NeteAuto-Verzeichnis)
- CA Identity Manager ™
- CA Identity Governance (früher CA GovernanceMinder)
- CA SiteMinder®
- CA Berichte zu Benutzeraktivitäten
- CA AuthMinder ™

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: Verwalten von Identitäten und Zugriff

Dieses Kapitel enthält folgende Themen:

Benutzerverwaltung und Anwendungszugriff

Die meisten IT-Abteilungen haben ständig damit zu tun, Benutzerkonten zu verwalten. IT-Administratoren müssen dringende Benutzeranforderungen erfüllten, wie vergessene Kennwörter zurückzusetzen, neue Konten erstellen sowie Materialien und Bürogeräte bereitstellen.

Gleichzeitig müssen IT-Administratoren Benutzern verschiedene Ebenen von Zugriff auf Anwendungen ermöglichen. Zum Beispiel generiert ein Abteilungsmanager Bestellungen und benötigt ein Konto in einer Finanzanwendung.

Um die steigenden Anforderungen an die IT zu bewältigen, bietet CA Identity Manager eine integrierte Methode zur Verwaltung von Benutzern und ihren Zugriff auf Anwendungen, einschließlich:

- Zuweisung von Berechtigungen durch Rollen. Genaue Erläuterung:
  - Rollen, die Administratoren ermöglichen, Benutzerkonten zu erstellen und zu verwalten
  - Rollen, die zusätzliche Konten zu vorhandenen Benutzern bereitstellen (erfordert Bereitstellungsunterstützung)
- Delegation der Verwaltung von Benutzern und Anwendungszugriff
- Self-Service-Optionen, sodass Benutzer ihre eigenen Konten verwalten können
- Integration von Unternehmensanwendungen in CA Identity Manager
- Optionen zum Anpassen und Erweitern von CA Identity Manager

Rollenbasierte Berechtigungen

Sie weisen Benutzern Berechtigungen durch das Zuweisen von Rollen zu. Eine *Rolle* enthält Aufgaben, die Anwendungsfunktionen in CA Identity Manager entsprechen, wie die Aufgabe "Benutzer erstellen", Funktionen in einer Anwendung, wie eine Funktion "Auftrag erstellen" oder Kontovorlagen, die dem Benutzer Konten, z. B. ein SAP-Konto, zuweisen. Wenn Benutzern eine Rolle zugewiesen wird, bekommen sie die entsprechenden Berechtigungen.

CA Identity Manager bietet die folgenden Typen von Rollen:

- Benutzerverwaltungs-Rollen, die *Admin-Rollen* genannt werden.

  Admin-Rollen können auch jede Aufgabe einschließen, die in der Benutzerkonsole angezeigt wird.
- Kontozuweisungs-Rollen, die *Bereitstellungsrollen* genannt werden.
- Anwendungsfunktions-Rollen, die *Zugriffsrollen* genannt werden.

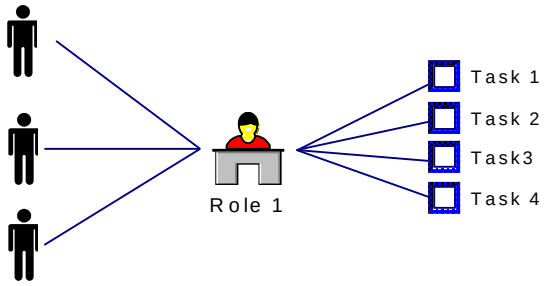
Wenn Sie eine Aufgabe oder Kontovorlage von einer Rolle entfernen, kann der Benutzer diese Aufgabe nicht mehr ausführen, ein Endpunkt-Benutzerkonto nicht mehr verwenden oder eine Anwendungsfunktion nicht mehr verwenden.

Admin-Rollen

Die Admin-Rollen steuern, was ein Benutzer in CA Identity Manager tun kann. Ein Systemadministrator weist einem Benutzer eine Rolle zu. Diese Rolle definiert einen Satz von Aufgaben, die der Benutzer ausführen kann. Benutzer können administrative *Aufgaben* auf Benutzerkonten ausführen, wie ein Kennwort zu ändern oder einen Jobtitel zu aktualisieren.

Verschiedene Benutzer haben unterschiedliche Ebenen von Zugriff auf diese Aufgaben. Zum Beispiel könnte eine Mitarbeiter-Rolle Aufgaben enthalten, die es Benutzern ermöglichen, ihren Namen und ihre Adresse zu ändern, während die Personalmanager-Rolle Aufgaben enthält, um den Titel und das Gehalt des Benutzers zu ändern.

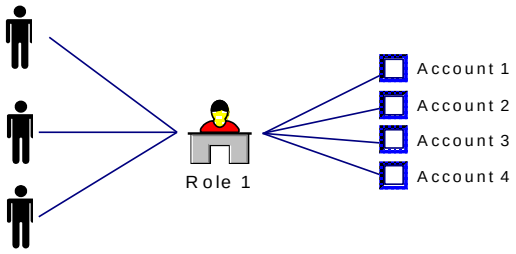
Die folgende Abbildung zeigt vier Aufgaben, die in einer Admin-Rolle zusammengefasst und drei Benutzern zugewiesen werden:



Bereitstellungsrollen

Um Benutzern Zugriff auf Konten in zusätzlichen Anwendungen wie z. B. einem E-Mail-System zu erteilen, weisen Sie Bereitstellungsrollen zu. Bereitstellungsrollen enthalten Kontovorlagen, die die Attribute definieren, die in einem Typ von Konto vorhanden sind. Zum Beispiel definiert eine Kontovorlage für ein Exchange-Konto Attribute wie die Größe des Postfachs. Kontovorlagen definieren auch, wie CA Identity Manager Benutzerattribute Konten zugeordnet werden.

Die folgende Abbildung zeigt vier Konten, die in einer Admin-Rolle zusammengefasst und drei Benutzern zugewiesen werden: Jeder Benutzer erhält vier Konten, wenn Sie die Bereitstellungsrolle diesem Benutzer zuweisen



Zugriffsrollen

Zugriffsrollen bieten eine zusätzliche Möglichkeit, Berechtigungen in CA Identity Manager oder einer anderen Anwendung anzugeben. Sie können Zugriffsrollen z. B. für Folgendes verwenden:

- Angeben von indirektem Zugriff auf ein Benutzerattribut
- Erstellen komplexer Ausdrücke
- Festlegen eines Attributs in einem Benutzerprofil, das von einer anderen Anwendung verwendet wird, um Berechtigungen zu bestimmen

Zugriffsrollen sind insofern ähnlich zu Identitätsrichtlinien, als sie einen Satz von Geschäftsänderungen auf einen Benutzer oder eine Gruppe von Benutzern anwenden. Wenn Sie eine Zugriffsrolle verwenden, um Geschäftsänderungen anzuwenden, können Sie jedoch feststellen, auf welche Benutzer sich die Änderungen beziehen, indem Sie die Mitglieder der Zugriffsrolle anzeigen.

In den meisten Fällen werden Zugriffsrollen nicht zu Aufgaben zugeordnet.

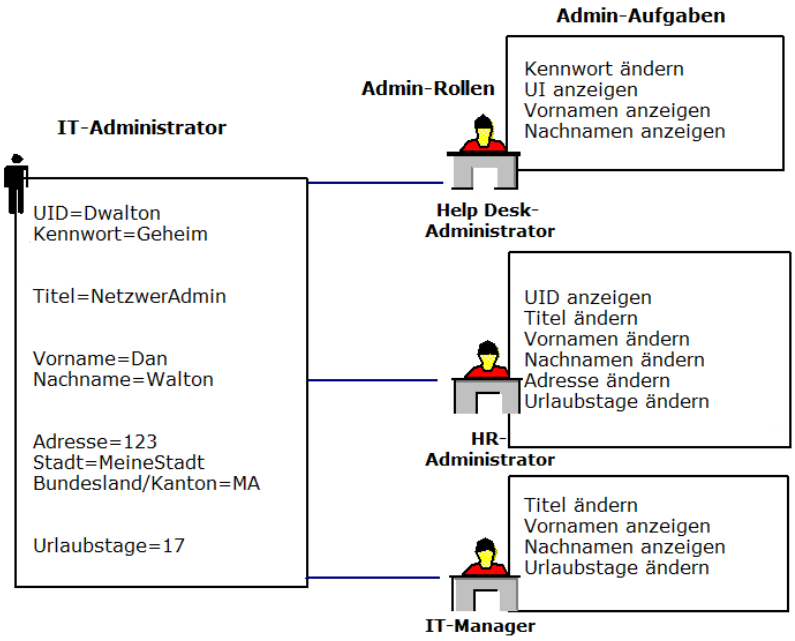
Hinweis: Wenn CA Identity Manager mit CA SiteMinder integriert ist, können Zugriffsrollen auch Zugriff auf Anwendungen ermöglichen, die von CA SiteMinder geschützt werden. In diesem Fall schließen Zugriffsrollen Zugriffsaufgaben ein. Weitere Informationen finden Sie im Kapitel zur SiteMinder-Integration im *Konfigurationshandbuch*.

Admin-Rollen für Benutzerkontenverwaltung

In CA Identity Manager verwalten Sie Benutzerspeicherobjekte (Benutzer, Gruppen und Organisationen) durch Admin-Rollen. Sie verwenden auch Admin-Rollen, um die Rollen und Aufgaben zu verwalten, durch die Sie Benutzerspeicherobjekte verwalten. Zum Beispiel verwenden Sie Admin-Rollen, um Profilattribute von Benutzern zu ändern, Benutzern das Verwalten ihrer eigenen Konten zu ermöglichen und um Aufgaben zu genehmigen, die Workflow verwenden.

Profilverwaltung auf Attributebene

Sie können Admin-Rollen für verschiedene Administratoren erstellen, die unterschiedliche Profilattribute lesen oder schreiben müssen. Zum Beispiel kann ein Unternehmen einige Mitarbeiter haben, die Vorgänge zu Benutzerprofilen ausführen und dabei jeder auf unterschiedliche Attribute zugreifen. Die folgende Abbildung zeigt drei Rollen und ihre zugeordneten Aufgaben. Jede Rolle hat unterschiedlichen Zugriff auf Profilattribute.



In diesem Beispiel können drei Rollen unterschiedliche Attribute für den gleichen Benutzer, Dan Walton, verwalten:

- Ein Helpdesk-Administrator zeigt Benutzernamen an und kann Benutzerkennwörter einrichten oder löschen.
- Ein Personal-Administrator ändert Benutzer-IDs, Benutzernamen, Adressen, Jobtitel und die Anzahl von Urlaubstagen.
- Ein IT-Manager ändert den Jobtitel von Benutzern und zeigt ihren Namen und die Anzahl von Urlaubstagen an.

Gleich welche Rollen Sie haben, wenn Sie sich bei CA Identity Manager anmelden, wird eine Reihe von Registerkarten, sogenannten Kategorien, basierend auf der Ihrem CA Identity Manager-Konto zugewiesenen Admin-Rolle angezeigt. Sie klicken auf eine Registerkarte, um die Aufgaben anzuzeigen, die Sie in dieser Kategorie ausführen können, wie in der folgenden Abbildung dargestellt:

Die Kategorien und die Aufgaben in diesen Kategorien, die ein Benutzer sieht, werden von den Admin-Rollen des Benutzers bestimmt.

Workflow-Genehmigung von Admin-Aufgaben

Um dabei zu helfen, Geschäftsprozesse zu automatisieren, können Sie eine Admin-Aufgabe entwerfen, um einen Workflow-Vorgang zu generieren. Ein *Workflow-Vorgang* automatisiert einen genau definierten Vorgang, den ein Unternehmen häufig wiederholt. CA Identity Manager umfasst die WorkPoint Workflow-Engine.

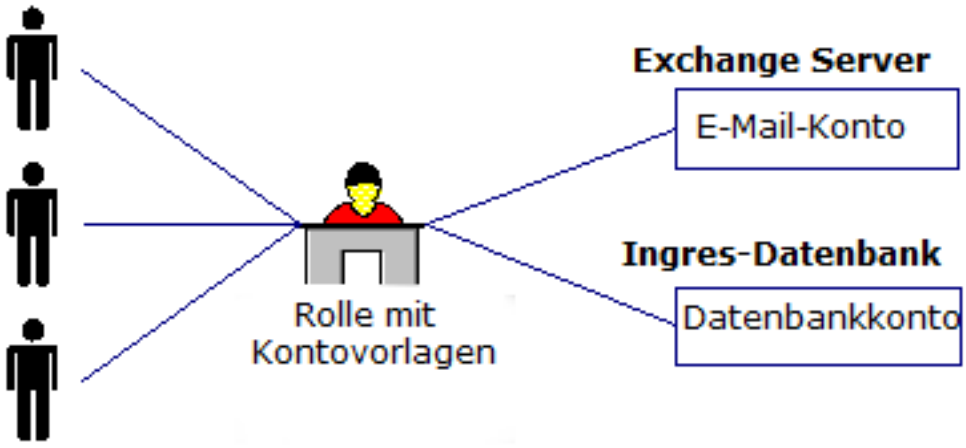
Workflow-Vorgänge werden von CA Identity Manager-Ereignissen ausgelöst, die Teil einer Admin-Aufgabe sind. Beispielsweise schließt die Aufgabe "Benutzer erstellen" die Ereignisse "CreateUserEvent" und "AddToGroupEvent" ein. Wenn ein Ereignis auftritt, kann die Workflow-Engine Folgendes ausführen:

- Genehmigungen anfordern – Ein Genehmiger muss ein Ereignis (wie ein Benutzerprofil zu ändern) genehmigen, bevor CA Identity Manager einen Benutzerspeicher aktualisiert. Genehmiger sind Administratoren, die die Genehmiger-Rolle für eine bestimmte Aufgabe haben.
- Benachrichtigungen senden – Die Workflow-Engine kann Benutzer über den Status eines Ereignisses in unterschiedlichen Phasen eines Prozesses informieren, beispielsweise wenn ein Benutzer ein Ereignis initiiert oder wenn ein Ereignis genehmigt wird.
- Arbeitslisten generieren – Arbeitslisten geben die Aufgaben an, die ein bestimmter Benutzer ausführen muss. Die Workflow-Engine aktualisiert die Arbeitslisten der Administratoren automatisch.

Für häufig auftretende Ereignisse können Sie die mit CA Identity Manager gelieferten Workflow-Vorgänge verwenden. Alternativ können Sie benutzerdefinierte Workflow-Vorgänge erstellen.

Bereitstellungsrollen für zusätzliche Konten

In CA Identity Manager geben Sie zusätzliche Konten für Benutzer durch die Verwendung von Bereitstellungsrollen an. Bereitstellungsrollen enthalten Kontovorlagen, die Konten definieren, die in verwalteten Endpunkten vorhanden sind, z. B. auf einem E-Mail-Server. Sobald Sie Benutzer in CA Identity Manager haben, können Sie einigen dieser Benutzer Bereitstellungsrollen zuweisen. Der Benutzer bekommt die von den Vorlagen definierten Konten in der Rolle.



Die Kontovorlagen definieren die Merkmale des Kontos. Zum Beispiel definiert eine Kontovorlage für ein Exchange-Konto die Größe des Postfachs. Kontovorlagen definieren auch, wie Benutzerattribute Konten zugeordnet werden.

Um Bereitstellungsrollen verwenden zu können, müssen Sie den Bereitstellungsserver mit dem Identity Manager-Server installieren. Dann erstellen Sie Kontovorlagen in der Benutzerkonsole.

Kennwortverwaltung

Identity Manager enthält mehrere Funktionen zur Verwaltung von Benutzerkennwörtern:

- Kennwortrichtlinien: Mit Kennwortrichtlinien werden Benutzerkennwörter verwaltet, wobei Regeln und Einschränkungen im Hinblick auf Ablauf, Zusammensetzung und Verwendung von Kennwörtern erzwungen werden.

  Hinweis: Konfigurieren Sie für erweiterte Kennwortrichtlinien die Integration mit SiteMinder. Weitere Informationen dazu finden Sie im *Installationshandbuch*.

- Kennwort-Manager: Administratoren, die die Rolle des Kennwort-Manager innehaben, können ein Kennwort zurücksetzen, wenn ein Benutzer den Helpdesk anruft.

- Self-Service-Kennwort-Management: Identity Manager enthält mehrere Self-Service-Aufgaben, mit denen der Benutzer sein eigenes Kennwort verwalten kann. Zu diesen Verwaltungsaufgaben gehören:

  - Selbstregistrierung: Der Benutzer gibt bei seiner Registrierung bei einer Firmen-Website ein Kennwort an.

  - Mein Kennwort ändern: Der Benutzer kann sein Kennwort ohne Hilfe von IT- oder Helpdesk-Arbeitnehmern ändern.

  - Kennwort vergessen: Der Benutzer kann ein vergessenes Kennwort zurücksetzen oder anfordern, nachdem Identity Manager seine Identität überprüft hat.

  - Benutzer-ID vergessen: Der Benutzer kann eine vergessene Benutzer-ID anfordern, nachdem Identity Manager seine Identität überprüft hat.

- Kennwortsynchronisierung (nur zur Verwendung mit Bereitstellung): Kennwortänderungen in Identity Manager und in Konten auf Zielsystemen (Endpunkte genannt) werden synchronisiert. Neue Kennwörter werden gemäß den Kennwortrichtlinien in Identity Manager überprüft.

Self-Service-Optionen für Benutzer

Um die IT-Auslastung weiter zu reduzieren, umfasst CA Identity Manager Funktionen zur Registrierung neuer Benutzer zu registrieren und Bereitstellung von vergessenen Kennwörtern. Diese Funktionen benötigen keinen Administrator. Der Benutzer erhält über eine *öffentliche Konsole* Zugriff auf CA Identity Manager, die kein Anmeldekonto erfordert. Über diese Konsole kann sich ein Benutzer an einem Standort selbst registrieren oder eine Erinnerung für ein vergessenes Kennwort anfordern.

Um IT-Administratoren Zeit zu sparen, können CA Identity Manager-Benutzer ihre eigenen Konten verwalten. Da Benutzer eine Selbstverwaltungsrolle haben, können sie:

- Persönliche Daten verwalten
- Eigenes Kennwort ändern
- Selbstabonnierenden Gruppen beitreten

Anpassung und Erweiterbarkeit von Identity Manager

Sie passen folgende CA-CA Identity Manager-Funktionen an:

- Das Identity Manager-Verzeichnis, das eine Benutzerspeicherstruktur für CA Identity Manager beschreibt.
- Die Erscheinung und Funktionalität der Benutzeroberfläche.
- Benutzereingabefenster, die die Felder und das Layout jedes Aufgabenfensters bestimmen.
- Validierung von Benutzerdateneingaben, durch reguläre Ausdrücke, JavaScript oder Java-Implementierungen.
- Workflow, der automatisierte Workflow-Vorgänge definiert. Erstellen oder ändern Sie Prozesse durch das Verknüpfen von Genehmigern und Aktionen im WorkPoint-Prozess-Designer.
- E-Mail-Nachrichten, die Benutzer über den Status einer Aufgabe informieren.
- Aufgabenübermittlung, die von einer Drittanbieteranwendung zur Task Execution Web Service (TEWS)-Schnittstelle von Identity Manager gesendet werden kann. TEWS bearbeitet die Remote-Aufgabenanfrage. Remote-Aufgabenanfragen entsprechen WSDL-Standards.

Sie können die CA Identity Manager-Funktionalität mithilfe der folgenden APIs erweitern:

- Logical Attribute-API – Ermöglicht eine andere Anzeige des Attributs als es physisch in einem Benutzerverzeichnis gespeichert ist.
- Business Logic Task-Handler-API – Ermöglicht Ihnen, während Datenprüfungen oder Transformationsvorgängen benutzerdefinierte Business-Logik auszuführen.

- Workflow-API – Bietet Informationen zu einem benutzerdefinierten Skript in einem Workflow-Vorgang. Das Skript wertet die Informationen aus und bestimmt dementsprechend den Pfad des Workflow-Vorgangs.
- Teilnehmerauflösung-API – Lässt Sie eine Liste von Teilnehmern angeben, die autorisiert sind, eine Workflow-Aktivität zu genehmigen.
- EventListener-API – Ermöglicht Ihnen, einen benutzerdefinierten Ereignis-Listener zu erstellen, der nach einem bestimmten Identity Manager-Ereignis oder einer Gruppe von Ereignissen sucht. Wenn das Ereignis auftritt, kann der Ereignis-Listener benutzerdefinierte Business-Logik ausführen.
- Benachrichtigungsregel-API – Lässt Sie die Benutzer bestimmen, die eine E-Mail-Benachrichtigung bekommen sollen.
- E-Mail-Vorlage-API – Schließt ereignisspezifische Informationen in einer E-Mail-Benachrichtigung ein.

Hinweis: Weitere Informationen zu den CA Identity Manager APIs finden Sie im *Programmierhandbuch für Java*.

Wenn CA Identity Manager Bereitstellung einschließt, können Sie auch die Bereitstellungsfunktionalität folgendermaßen erweitern:

- Benutzerdefinierte Connectors – Ermöglichen die Kommunikation zwischen einem Bereitstellungsserver und einem Endpunktsystem. Der Code, der einen Connector bildet, kann ein GUI-Plug-in, Server-Plug-in oder Agenten-Plug-in einschließen.

  Ein dynamischer Connector kann von Connector Xpress generiert werden, und ein benutzerdefinierter statischer Connector kann in Java oder C++ entwickelt werden.
- Programmausgänge – Ermöglichen den Verweis auf benutzerdefinierten Code vom Bereitstellungsserver-Prozessablauf.

Hinweis: Weitere Informationen zur Erweiterung der Bereitstellungsfunktionalität finden Sie im *Programmierhandbuch für die Bereitstellung*.

CA Identity Governance-Integration

CA Identity Governance ist ein Produkt von Identity Lifecycle Management, mit dem Sie Rollenmodelle schnell und präzise entwickeln, beibehalten und analysieren können. Es bietet auch zentralisierte Identitätscompliance-Richtlinienkontrollen und automatisiert Prozesse, die mit der Erfüllung von Richtilinien und Sicherheitsanforderungen in Verbindung stehen. Mit CA Identity Governance haben Sie folgende Möglichkeiten:

- Überprüfen, dass CA Identity Manager-Benutzerberechtigungen in Übereinstimmung mit Geschäfts-Compliance-Richtlinien erteilt werden
- Vorgeschlagene Rollen übernehmen und Compliance-Überprüfung, wenn CA Identity Manager-Benutzer, Rollen und Konten erstellt oder geändert werden
- Verstehen, welche Rollen in Ihrer Organisation vorhanden sind, ein Rollenmodell speziell für Ihre Organisation festlegen und das gewünschte Rollenmodell innerhalb von CA Identity Manager wiedererstellen
- Sie können dieses Rollenmodell entsprechend der Geschäftsentwicklung analysieren und aufrecht erhalten.

CA Identity Manager kann auf zwei Arten in CA Identity Governance integriert werden:

- CA Identity Governance-Connector für CA Identity Manager

  Ein besonderer Typ von Connector, der automatisch die Berechtigungsdaten zwischen CA Identity Manager und CA Identity Governance synchronisiert. Wenn Sie den Connector verwenden, können Sie Daten aus CA Identity Manager nach CA Identity Governance importieren oder aus CA Identity Governance nach CA Identity Manager exportieren.

- Smart Provisioning

  Wenn CA Identity Manager in CA Identity Governance integriert wird, lassen sich zusätzliche Funktionalitäten konfigurieren, mit denen Sie Rollen- und Richtlinieninformationen aus einem Rollenmodell verwenden können, um tägliche Identitätsmanagementoperationen zu unterstützen. Änderungen, die in CA Identity Manager vorgenommen werden, aktualisieren das Rollenmodell in CA Identity Governance dynamisch.

Hinweis: Weitere Informationen zur CA Identity Governance-Integration mit CA Identity Manager finden Sie im *CA Identity Manager-Integrationshandbuch* im CA Identity Governance-Bookshelf.

CA User Activity Reporting-Integration

CA Enterprise Log Manager wird ab CA Identity Manager r12.6 in CA User Activity Reporting (CA UAR) umbenannt.

CA UAR nutzt die ELM-Schemadefinition von CA (Common Event Grammar – CEG), um Ereignisse aus verschiedenen Systemen einem Standardformat zuzuordnen und speichert alle Ereignisse – selbst jene, die noch nicht zugeordnet wurden – zur Überprüfung und Analyse. Darüber hinaus bietet CA UAR den Benutzern eine umfassende Lösung, um gesammelte Daten zu verwalten und über sie zu berichten, und verwendet konfigurierbare Datenbankanfragen und/oder -berichte für die Suche nach verschiedenen Informationstypen und -Ereignissen.

CA UAR verleiht auch besseren, breiteren und tieferen Einblick in unverwaltete Systeme und solche, die außerhalb des Zuständigkeitsbereichs und der Kontrolle von CA Identity Manager liegen, und ermöglicht Ihnen intensivere Nachforschungen über Identitäten.

Eine Integration mit CA Identity Manager zeigt Ihnen zentrierte Berichte und/oder dynamische Anfragen von CA UAR an die Benutzerkonsole von CA UAR an, wenn Sie die Benutzerkonsole von CA Identity Manager verwenden. Über die Benutzerkonsole können Sie konfigurieren, wie bestehende CA Identity Manager/CA UAR-Berichte und/oder -Anfragen angezeigt und geändert werden, während Sie intensivere Nachforschungen über eine bestimmte Identität betreiben.

CA-UAR-Berichte

Die folgenden CA-UAR-Berichte werden standardmäßig mit CA-UAR-Rollendefinitionen bereitgestellt:

Aufgabe	Startet den Bericht
Alle Ereignisse des Systems nach Benutzer	CA Identity Manager - Alle Ereignisse des Systems gefiltert nach Benutzer-ID
Kontenverwaltung nach Host	Kontenverwaltung nach Host
Kontenerstellungen nach Konto	Kontenerstellungen nach Konto
Kontenlöschungen nach Konto	Kontenlöschungen nach Konto
Kontensperrungen nach Konto	Kontensperrungen nach Konto
Zertifizierungsprozessaktivität nach Host	CA Identity Manager - Prozessaktivität von Host
Kennwortrichtilinien-Änderungsaktivität	CA Identity Manager - Richtlinienänderungsaktivität

Kapitel 2: Adressierung von Geschäftsanforderungen

Dieses Kapitel enthält folgende Themen:

Verarbeitung von Geschäftsänderungen

Sie können die Verarbeitung von gewissen Identitätsverwaltungsaufgaben durch die Verwendung von Identitätsrichtlinien automatisieren. Eine Identitätsrichtlinie bezeichnet einen Satz von Geschäftsänderungen, die eintreten, wenn ein Benutzer eine bestimmte Bedingung oder Regel erfüllt. Mit Identitätsrichtliniensätzen können Sie folgende Schritte ausführen:

- Automatisieren bestimmter Identitätsmanagementaufgaben wie z. B. Zuweisen von Rollen und Gruppenmitgliedschaften, Zuordnen von Ressourcen oder Ändern von Attributen von Benutzerprofilen.
- Durchsetzen, dass Pflichten getrennt werden (siehe Seite 26). Sie können z. B. einen Identitätsrichtliniensatz erstellen, der verhindert, dass Mitglieder der Rolle "Scheckunterzeichner" über die Rolle "Scheckgenehmiger" verfügen, und der für alle Angehörigen der Firma das Ausstellen von Schecks auf $10.000 beschränkt.
- Konformität durchsetzen. Sie können z. B. Benutzer überprüfen, die einen bestimmten Titel haben und mehr als $100.000 verdienen.

  Identitätsrichtlinien, die für Konformität sorgen, werden als *Konformitätsrichtlinien* bezeichnet.

Die Geschäftsänderungen, die mit einer Identitätsrichtlinie verknüpft sind, umfassen:

- Zuweisen oder Widerrufen von Rollen einschließlich Bereitstellungsrollen (wenn CA Identity Manager Bereitstellung einschließt)
- Zuweisen oder Entziehen einer Gruppenmitgliedschaft
- Aktualisieren der Attribute in einem Benutzerprofil

Eine Firma kann z. B. möglicherweise eine Identitätsrichtlinie erstellen, die angibt, dass alle stellvertretenden Vorsitzenden zu der Gruppe "Country-Club-Mitglied" gehören und über die Rolle "Gehaltsgenehmiger" verfügen. Wenn sich der Titel eines Benutzers in "stellvertretender Vorsitzender" ändert und dieser Benutzer mit der Identitätsrichtlinie synchronisiert wird, fügt CA Identity Manager den Benutzer zu der entsprechenden Gruppe und Rolle hinzu. Wenn ein stellvertretender Vorsitzender zum Vorstandsvorsitzenden befördert wird, erfüllt er oder sie die Bedingung in der Identitätsrichtlinie "stellvertretender Vorsitzender" nicht mehr. Daher werden die durch diese Richtlinien übernommenen Änderungen widerrufen, und es werden neue Änderungen basierend auf der Vorstandsvorsitzenden-Richtlinie übernommen.

Die Änderungsaktionen, die basierend auf einer Identitätsrichtlinie ausgeführt werden, enthalten Ereignisse, die unter Workflow-Steuerung gestellt und überprüft werden können. Im vorhergehenden Beispiel gewährt die Rolle "Gehaltsgenehmiger" ihren Mitgliedern weitreichende Berechtigungen. Um die Rolle "Gehaltsgenehmiger" zu schützen, kann die Firma einen Workflow-Prozess erstellen, der einen Satz von Genehmigungen erfordert, bevor die Rolle zugewiesen wird. Außerdem kann sie CA Identity Manager so konfigurieren, dass er die Zuweisung der Rolle überprüft.

Zur Vereinfachung des Identitätsrichtlinienmanagements sind Identitätsrichtlinien in einem Identitätsrichtliniensatz gruppiert. Die Richtlinien "stellvertretender Vorsitzender" und "Vorstandsvorsitzender" können z. B. Teil des Identitätsrichtliniensatzes "Führungskräfteberechtigungen" sein.

Konformität mit Geschäftsrichtlinien

Konformität ist eine Governance-Regel für Unternehmen, die eine Vielzahl von Verfahren einschließt. Diese Verfahren sollen sicherstellen, dass ein Unternehmen und seine Arbeitnehmer Geschäftsrichtlinien erfüllen. Die Konformitätsverfahren umfassen die Dokumentierung, Automatisierung und Überwachung der Zuweisung von Berechtigungen auf Anwendungen und Systeme.

CA Identity Manager beinhaltet die folgenden Funktionen zur Unterstützung des Konformitätsmanagement:

- **Smart Provisioning**

  Smart Provisioning besteht aus mehreren Funktionen, die die Bereitstellungsrollenzuordnung vereinfachen, wenn CA Identity Manager in CA Identity Governance integriert wird. Zu diesen Funktionen gehören Folgende:

  - Vorgeschlagene Bereitstellungsrollen

    Administratoren können von CA Identity Manager eine Liste der Bereitstellungsrollen erhalten, die einem Benutzer möglicherweise zugewiesen werden können. Die Liste der Bereitstellungsrollen wird von CA Identity Governance basierend auf Kriterien ermittelt, die der Administrator eingegeben hat.

    Vorgeschlagene Bereitstellungsrollen helfen dabei, sicherzustellen, dass Benutzer über die richtigen Privilegien verfügen und gleichzeitig das Rollenmodell der Firma beibehalten wird.

  - Konformitäts- und Mustermeldungen

    CA Identity Manager-Administratoren können vorgeschlagene Änderungen in CA Identity Governance anhand eines Rollenmodells überprüfen, bevor sie die Änderungen übernehmen. Die Änderungen vor ihrer Übernahme zu überprüfen, gewährleistet, dass Firmen das Rollenmodell beibehalten, das für ihre Betriebsführung definiert wurde.

    Benutzer können vorgeschlagene Änderungen an Bereitstellungsrollen überprüfen (und sie zuweisen oder entfernen) sowie Änderungen an Benutzerattributen überprüfen.

    CA Identity Manager führt zwei Arten von Richtlinienvalidierungen durch:

    - Konformität

      Vorgeschlagene Änderungen werden anhand des CA Identity Governance-Rollenmodells überprüft. Auf diese Weise kann festgestellt werden, ob sie die Regeln expliziter, vordefinierter CA Identity Governance-Geschäftsrichtlinien verletzen.

    - Muster

      Vorgeschlagene Änderungen werden mit dem Rollenmodell in CA Identity Governance verglichen, um festzustellen, ob das Subjekt der Änderungen den Status "Out-Of-Pattern" erhalten würde. Darüber hinaus stellt CA Identity Manager sicher, dass bewährte Muster im Rollenmodell durch die Änderungen nicht signifikant modifiziert werden.

      Sie können CA Identity Manager so konfigurieren, dass diese Validierungen automatisch durchgeführt werden, wenn Benutzer bestimmte Aufgaben ausführen, oder Sie können Benutzern ermöglichen, die Validierung manuell zu initiieren.

Sie können Smart Provisioning in einer CA Identity Manager-Umgebung implementieren, sobald ein Rollenmodell basierend auf CA Identity Manager-Daten in CA Identity Governance bereit steht.

Hinweis: Weitere Informationen finden Sie im *Administrationshandbuch*.

- **Identitätsrichtlinien**

  Sie können eine Konformitätsrichtlinie erstellen (ein bestimmter Typ von Identitätsrichtlinie (siehe Seite 21)), die nicht zulässt, dass Benutzern bestimmte Berechtigungen gewährt werden, falls sie andere Berechtigungen aufweisen. Beispielsweise können Sie verhindern, dass Benutzer, die Schecks bewilligen können, diese auch ausstellen können.

  Konformitätsrichtlinien setzen in Umgebungen die Trennung von Pflichten durch.

- **Konformitätsberichte**

  CA Identity Manager schließt Beispielberichte ein, die den Konformitätsstatus für Benutzer in Ihrer Umgebung anzeigen. Anhand dieser Berichte können Sie sehen, welche Benutzer Ihre Geschäftsrichtlinien nicht erfüllen.

Konformitätsberichte

CA Identity Manager umfasst die Beispielberichte in der folgenden Tabelle, die Sie verwenden können, um die Konformität mit Geschäftsrichtlinien im Unternehmen zu überwachen.

Bericht	Beschreibung
Rollenmitglieder	Zeigt die Rollen in der Berichtsdatenbank an und listet die Mitglieder dieser Rollen auf
Rollen	Zeigt für jede Rolle in der Berichtsdatenbank die folgenden Informationen an: ■ Der Rolle zugeordnete Aufgaben ■ Mitgliederrichtlinien und Rollenmitglieder ■ Administratorrichtlinien und Rollenadministratoren ■ Eigentümerrichtlinien und Rolleneigentümer
Aufgabenrollen	Zeigt die Aufgaben in der Berichtsdatenbank und die Rollen an, denen sie zugeordnet sind

Bericht	Beschreibung
Benutzerrollen	Zeigt die Benutzer in der Berichtsdatenbank an und listet die Rollen jedes Benutzers auf
Non-Standard Accounts Trend (Sonderkontentrend)	Zeigt Sonderkontentrends für verwaiste Konten, Systemkonten und Ausnahmekonten an
Non-Standard Accounts (Sonderkonten)	Zeigt alle verwaisten, System- und Ausnahmekonten an
Orphan Accounts (Verwaiste Konten)	Zeigt alle Endpunkt-Benutzerkonten ohne globalen Benutzer im Bereitstellungsserver an
Richtlinien	Zeigt alle Identitätsrichtlinien an
Benutzerprofil	Zeigt die folgenden Informationen für Benutzer an: ■ Name ■ User ID (Benutzer-DN) ■ Gruppen, in denen der Benutzer Mitglied oder Administrator ist ■ Rollen, wo der Benutzer Mitglied, Administrator oder Besitzer ist
Endpunkt-Benutzerkonten	Zeigt die Konten pro Endpunkt an (Sie können auswählen, welchen Endpunkt Sie anzeigen möchten)
Rollenadministratoren	Zeigt Rollen und ihre Administratoren an
Rolleneigentümer	Zeigt Rollen und ihre Eigentümer an
Snapshots	Zeigt alle exportierten Snapshots an
Benutzerkonto	Zeigt eine Liste von Benutzern und ihren Konten an
Benutzerberechtigungen	Zeigt Rollen von Benutzern, Gruppen und Konten an
Synchronisierungsstatus von Benutzerrichtlinie	Zeigt den Status des Benutzers pro Richtlinie an (welche Richtlinien zugewiesen, aufgehoben oder erneut zugewiesen werden sollten)

Hinweis: Weitere Informationen zu Berichten finden Sie im *Administrationshandbuch*.

Anforderungen für das Durchsetzen der Trennung von Pflichten

Anforderungen für die Trennung von Pflichten (Segregation of Duties, SoD) verhindern, dass Benutzer Berechtigungen erhalten, die in einem Interessenskonflikt oder Betrugs resultieren können. CA Identity Manager stellt die folgende Funktionalität bereit, um SoD zu unterstützen:

- **Präventive Identitätsrichtlinien**

  Diese Richtlinien werden vor dem Senden einer Aufgabe ausgeführt. Mit ihnen kann ein Administrator nach Richtlinienverletzungen suchen, bevor er Berechtigungen zuweist oder Profilattribute ändert. Wenn eine Verletzung vorliegt, kann sie der Administrator beheben, bevor er die Aufgabe sendet.

  Beispielsweise kann ein Unternehmen eine präventive Identitätsrichtlinie erstellen, die nicht zulässt, dass Benutzer, die die Rolle "Benutzer-Manager" besitzen, auch die Rolle "Genehmiger für Benutzer" besitzen. Wenn ein Administrator die Aufgabe "Benutzer ändern" verwendet, um einem Benutzer-Manager die Rolle "Genehmiger für Benutzer" zu geben, zeigt CA Identity Manager eine Meldung über die Verletzung an. Der Administrator kann die Rollenzuweisungen ändern, um die Verletzung zu beheben, bevor er die Aufgabe sendet.

- **Richtlinienvalidierung durch Smart Provisioning**

  CA Identity Manager-Administratoren können vorgeschlagene Änderungen an Bereitstellungsrollen und Benutzerattribute anhand von Geschäftsrichtlinienregeln (BPR) in CA Identity Governance validieren, bevor sie Änderungen übernehmen. BPRs stellen verschiedene Einschränkungen von Berechtigungen dar. Eine BPR kann beispielsweise Benutzern mit der Rolle "Einkauf", die Mitglieder zum Bestellen von Waren von Zulieferern berechtigt, die Rolle "Zulieferer bezahlen" verweigern. Ein Systemadministrator, Manager, Auditor oder Rolleningenieur erstellt BPRs in CA Identity Governance.

  Hinweis: Weitere Informationen zu BPRs finden Sie im *CA Identity GovernanceSage DNA User Guide*.

Hinweis: Weitere Informationen zu präventiven Identitätsrichtlinien und Smart Provisioning finden Sie im *CA Identity Manager Administrationshandbuch*.

Transformieren von Daten im Benutzerspeicher

Unter Umständen möchten Sie, dass CA Identity Manager Daten transformiert, bevor sie im Benutzerspeicher gespeichert werden. Vielleicht wollen Sie Informationen in einem anderen Format speichern, als sie eingegeben wurden, oder Sie möchten Änderungen anwenden, wenn gewisse Informationsarten vorhanden sind.

CA Identity Manager schließt die folgenden Funktionen für die Transformierung von Daten ein:

- Identitätsrichtlinien
- Logical-Attribute-Handler

Hinweis: Sie können auch Identitätsrichtlinien und Logical-Attribute-Handler verwenden, um benutzerdefinierte Business-Logik zu implementieren.

Logical-Attribute-Handler

Logical-Attribute-Handler sind benutzerdefinierter Java-Code, der Benutzerattributwerte transformiert, die in CA Identity Manager-Aufgabenfenstern verwendet werden. Mithilfe von Logical-Attribute-Handlern können Sie steuern, wie ein physisches Attribut in einem Aufgabenfenster angezeigt wird. Sie können auch Logical-Attribute-Handler verwenden, um einen Anzeigewert, wie Kosten, im Aufgabenfenster zu einem oder mehr physischen Attributen, wie Einheitspreis und Menge, zu transformieren, die im Benutzerspeicher gespeichert werden.

Hinweis: Weitere Informationen zu Logical-Attribute-Handler finden Sie im *Programmierhandbuch für Java*.

Anwenden von benutzerdefinierter Business-Logik

Sie können CA Identity Manager anpassen, um die Business-Logik zu implementieren, die Ihr Unternehmen benötigt. CA Identity Manager schließt die folgenden Optionen für die Implementierung von benutzerdefinierter Business-Logik ein:

- Identitätsrichtlinien – Sie können Identitätsrichtlinien verwenden, um ein Set von Geschäftsänderungen zu definieren, die eintreten, wenn ein Benutzer eine bestimmte Bedingung oder Regel erfüllt. Zum Beispiel können Identitätsrichtlinien gewisse Identitätsverwaltungsaufgaben automatisieren, wie Rollen zuweisen oder Geschäftsregeln durchsetzen, die Benutzer davon abhalten, Schecks über 20.000 Euro zu unterzeichnen und zu genehmigen.

  Hinweis: Weitere Informationen zu Identitätsrichtlinien finden Sie im *Administrationshandbuch*.

- Logical-Attribute-Handler – Sie können diese Handler zu CA Identity Manager-Aufgabenfenstern zuordnen, um die Anzeige und Änderung von Attributwerten zu steuern.

  Weitere Informationen finden Sie im *Programmierhandbuch für Java*.

- Business Logic Task-Handler – Ermöglicht Ihnen, benutzerdefinierte Business-Logik während Datenprüfungsvorgängen für eine CA Identity Manager-Aufgabe auszuführen, wie Folgende:

  - Benutzerdefinierte Geschäftsregeln durchsetzen (zum Beispiel kann ein Administrator nicht mehr als fünf Gruppen verwalten).
  - Kundenspezifische Aufgabenfensterfelder validieren (zum Beispiel muss der Wert eines Mitarbeiter-ID-Felds in der Master-Personaldatenbank vorhanden sein).

  Business Logic Task-Handler können in Java oder JavaScript implementiert werden.

  Hinweis: Weitere Informationen finden Sie im *Programmierhandbuch für Java*.

- Workflow – Erlaubt Ihnen, benutzerdefinierte Prozessdefinitionen zu erstellen, die einem CA Identity Manager-Ereignis zugeordnet werden.

Hinweis: Bevor Sie entscheiden, ob Sie Business-Logik in einem Business Logic Task-Handler oder einem Workflow-Vorgang implementieren sollten, lesen Sie die folgenden Abschnitte:

- Überlegungen zu Business Logic Task-Handlern (siehe Seite 29)
- Überlegungen zu Workflow-Vorgängen (siehe Seite 29)

Überlegungen zu Business Logic Task-Handlern

Business Logic Task-Handler führen Business-Logik-Validierung während der synchronen Verarbeitungsphase der Aufgabe aus, die vor der Ereignisgenerierung erfolgt. Dies ermöglicht Folgendes:

- Ausführen der Validierung auf Aufgabenebene. Zum Beispiel können Sie Mitglieder einer Gruppe hinzufügen oder entfernen, basierend auf ihrem Bürostandort, der im Benutzerprofilfenster angegeben ist.
- Eine Aufgabe davon abhalten, gesendet zu werden, wenn die Validierung fehlschlägt.
- Transformieren Sie vor der Aufgabenübermittlung automatisch die gesamte Information in einem Aufgabenfenster, sodass sie Ihren Geschäftsrichtlinien entspricht.

Hinweis: Sie sollten keine Aktivitäten in einem Business Logic Task-Handler implementieren, die lange Zeit brauchen. Lang andauernde Aktivitäten verzögern die Übermittlung der Aufgabe und sind für die synchrone Phase nicht gut geeignet, wo Benutzerinteraktionen auftritt. Verwenden Sie stattdessen einen Workflow-Vorgang, der während der asynchronen Phase der Aufgabe ausgeführt wird.

Überlegungen zu Workflow-Vorgängen

Workflow-Vorgänge werden während der asynchronen Phase der Aufgabe aufgerufen und werden mit der Ausführung von individuellen Ereignissen verknüpft. Dies ermöglicht Folgendes:

- Führen Sie basierend auf individuellen Ereignisdaten Genehmigungsaktivitäten aus
- Führen Sie lang dauernde benutzerdefinierte Business-Logik-Aktivitäten aus

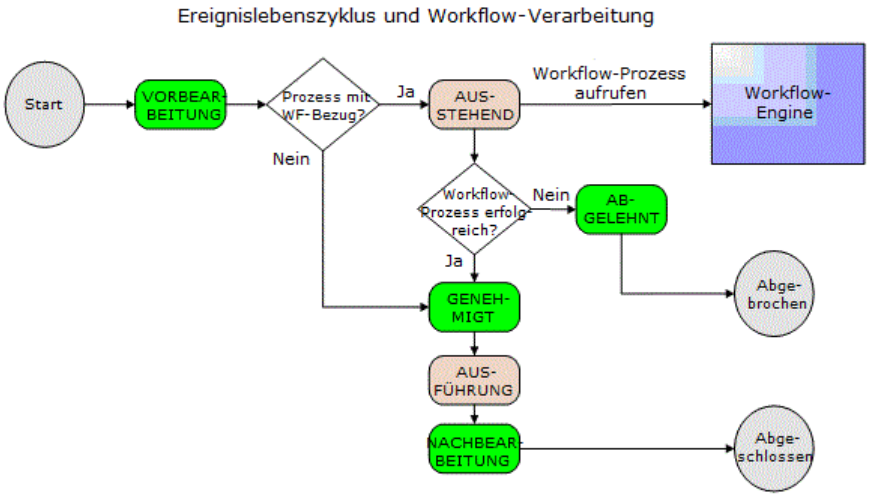
Während Ihnen die Workflow-API erlaubt, Aufgabenebenendaten von einer Workflow-Aktivität zu erhalten, operieren Sie normalerweise im Kontext dieses bestimmten Ereignisses im Workflow.

Genehmigung von Geschäftsänderungen

Workflow beschreibt einen Prozess, der aus einem oder mehreren Schritten besteht, die ausgeführt werden müssen, um einige Geschäftsziele zu erfüllen, wie einen Einstellungsprozess auszuführen oder die Kreditwürdigkeit eines Benutzers von einem externen System zu erhalten. Normalerweise bedeutet einer der Schritte in einem Workflow-Vorgang, die Geschäftsänderung zu genehmigen oder abzulehnen.

In CA Identity Manager wird ein Workflow-Vorgang einem Ereignis zugeordnet, einer Aktion, die während der Prozessverarbeitung auftritt. Wenn ein Ereignis in den Status "Ausstehend" in seinem Lebenszyklus eintritt, ruft CA Identity Manager einen zugeordneten Workflow-Vorgang auf und hält die Ereignisausführung an, bis der Prozess abgeschlossen ist. CA Identity Manager führt dann das Ereignis aus oder lehnt es ab, basierend auf den Ergebnissen des Workflow-Vorgangs.

Diese Reihenfolge wird in der folgenden Abbildung dargestellt:



CA Identity Manager schließt die InSession-WorkPoint-Workflow-Engine ein, um Workflow-Vorgänge zu erstellen und zu verwalten.

Hinweis: Weitere Informationen finden Sie im *Administrationshandbuch*.

Kapitel 3: CA Identity Manager-Architektur

Dieses Kapitel enthält folgende Themen:

CA Identity Manager-Komponenten

Eine CA Identity Manager-Implementierung kann einige oder alle der folgenden Komponenten einschließen:

- Server
- Benutzerspeicher
- Datenbanken
- Connectors

Server

Eine CA Identity Manager-Implementierung schließt einen oder mehrere Typen von Servern ein, je nach der Funktionalität, die Sie benötigen.

CA Identity Manager-Server (erforderlich)

Führt Aufgaben innerhalb von CA Identity Manager aus. Die J2EE-CA Identity Manager-Anwendung schließt die Management-Konsole und die Benutzerkonsole ein.

CA Identity Manager-Bereitstellungsserver

Verwaltet Konten auf Endpunktsystemen.

Dieser Server ist erforderlich, wenn die CA Identity Manager-Installation Kontobereitstellung unterstützt.

Hinweis: Sie müssen das Bereitstellungsverzeichnis remote (oder lokal für eine Demonstrationsumgebung) auf einem CA Directory Server installiert haben, bevor Sie den Bereitstellungsserver installieren.

SiteMinder-Richtlinienserver

Gibt erweiterte Authentifizierung für CA Identity Manager an und gewährt Zugriff auf SiteMinder-Funktionen, wie Kennwortservices und Single Sign-On.

Dieser Server ist optional.

Benutzerspeicher und Bereitstellungsverzeichnis

CA Identity Manager koordiniert zwei Benutzerspeicher:

- Der *CA Identity Manager-Benutzerspeicher*, der von CA Identity Manager verwaltete Benutzerspeicher. Normalerweise ist dies ein vorhandener Speicher, der die Benutzeridentitäten enthält, die ein Unternehmen verwalten muss.

  Der Benutzerspeicher kann ein LDAP-Verzeichnis oder eine relationale Datenbank sein.

  In der Management-Konsole erstellen Sie ein CA Identity Manager-Verzeichnisobjekt, um eine Verbindung mit dem Benutzerspeicher herzustellen und die Benutzerspeicherobjekte, die von CA Identity Manager verwaltet werden sollen, zu beschreiben.

- Das *Bereitstellungsverzeichnis*, der vom Bereitstellungsserver verwaltete Benutzerspeicher.

  Dies ist eine Instanz von CA Directory und schließt globale Benutzer ein, die Benutzer im Bereitstellungsverzeichnis zu Konten auf Endpunkten wie Microsoft Exchange, Active Directory und SAP zuordnen.

  Nur manche CA Identity Manager-Benutzer verfügen über einen entsprechenden globalen Benutzer. Wenn ein CA Identity Manager-Benutzer eine Bereitstellungsrolle erhält, erstellt der Bereitstellungsserver einen globalen Benutzer.

Trennung von Benutzerspeicher und Bereitstellungsverzeichnissen

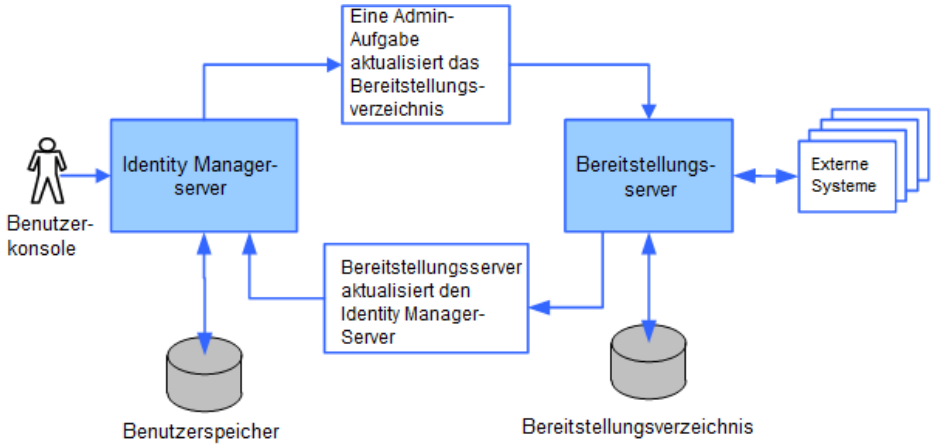
In der folgenden Abbildung sind ein separates Benutzerverzeichnis sowie ein separates Bereitstellungsverzeichnis veranschaulicht. Dies entspricht dem unterstützten Szenario für Neuinstallationen von CA Identity Manager. In dieser Abbildung sehen Sie Folgendes:

- Ein CA Identity Manager-Administrator verwendet eine Admin-Aufgabe, die einen Benutzer in dem Benutzerspeicher bearbeitet, der sich auf das Bereitstellungsverzeichnis auswirkt.

  Diese Änderung kann auch einen Endpunkt (wie einen E-Mail-Server) aktualisieren, der einen Connector zum Bereitstellungsserver hat.

  Eine im Bereitstellungsserver (oder einem Endpunkt mit einem Connector zum Bereitstellungsserver) vorgenommene Änderung aktualisiert den CA Identity Manager-Benutzerspeicher und das Bereitstellungsverzeichnis.

Zum Beispiel könnte ein Endpunkt, wie eine Personalanwendung, die E-Mail-Adressen von Benutzern aktualisieren.



Datenbanken

CA Identity Manager verwendet Datenquellen, um mit Datenbanken Verbindung aufzunehmen, die Informationen speichern, die zur Unterstützung von CA Identity Manager-Funktionalität erforderlich sind. Diese Datenbanken können sich in einer einzelnen physischen Instanz einer Datenbank oder in getrennten Instanzen befinden.

Objektdatenbank (erforderlich)

Enthält CA Identity Manager-Konfigurationsinformationen.

Aufgabenpersistenz-Datenbank (erforderlich)

Verwaltet Informationen zu CA Identity Manager-Aktivitäten und den zugehörigen Ereignissen im Laufe der Zeit. Dies ermöglicht dem System, die CA Identity Manager-Aktivitäten genau zu verfolgen, auch wenn Sie den CA Identity Manager-Server neu starten.

Archivdatenbank (erforderlich)

Archivdaten aus der Aufgabenpersistenz-Datenbank.

Workflow-Datenbank

Speichert Workflow-Prozessdefinitionen, Jobs, Skripte und andere Daten, die von der Workflow-Engine benötigt werden.

Audit-Datenbank

Stellt einen Verlaufsdatensatz von Vorgängen zur Verfügung, die in einer CA Identity Manager-Umgebung stattfinden.

Hinweis: Sie können die Menge und Art der Informationen konfigurieren, die CA Identity Manager in der Audit-Datenbank speichert. Weitere Informationen finden Sie im *Konfigurationshandbuch.*

Berichtsdatenbank

Speichert Snapshot-Daten, die den aktuellen Zustand von Objekten in CA Identity Manager zum Zeitpunkt des Snapshots widerspiegeln. Sie können Berichte aus diesen Informationen generieren, um die Beziehung zwischen Objekten, wie Benutzern und Rollen, anzuzeigen.

Wenn Sie das Installationsprogramm verwenden, konfiguriert CA Identity Manager eine Verbindung zu einer einzelnen Datenbank, CA Identity Manager-Datenbank genannt, die die Tabellen für jeden Datenbanktyp enthält.

Hinweis: Sie können einen Datenspeicher für Aufgabenpersistenz, Workflow, Überwachung oder Berichterstellung in einer separaten Datenbank erstellen und CA Identity Manager konfigurieren, damit Verbindung aufzunehmen. Weitere Informationen dazu finden Sie im *Installationshandbuch*.

Connector-Komponenten

Ein Connector ist die Softwareschnittstelle zu einem Endpunkt. Der Bereitstellungsserver verwendet den Connector, um mit dem Endpunkt zu kommunizieren. Er übersetzt Bereitstellungsserver-Aktionen in Änderungen auf dem Endpunkt, wie "Ein neues E-Mail-Konto auf einem Microsoft-Exchange-Endpunkt erstellen".

Beispiele für Endpunkte sind UNIX-Workstation, Windows-PC oder eine Anwendung wie Microsoft Exchange (für E-Mail).

Connector-Server

Ein Connector-Server ist eine Bereitstellungsserver-Komponente, die Connectors verwaltet. Er kann auf dem Bereitstellungsserver-System oder auf einem Remote-System installiert werden.

Ein Connector-Server funktioniert mit mehreren Endpunkten. Wenn Sie zum Beispiel viele UNIX-Workstationsendpunkte haben, könnten Sie einen Connector-Server haben, der alle Connectors verarbeitet, die UNIX-Konten verwalten. Ein anderer Connector-Server könnte alle Connectors verarbeiten, die Windows-Konten anfordern.

Der verteilte Connector-Server funktioniert mit mehreren Connector-Servern. Es gibt Lastenausgleich an, wenn ein Connector-Server beschäftigt ist, und Hochverfügbarkeit, wenn ein Connector-Server ausfällt.

Es gibt zwei Arten von Connector-Servern:

- CA IAM-Connector-Server (CA IAM CS) verwaltet in Java geschriebene Connectors
- C++-Connector-Server (CCE) verwaltet in C++ geschriebene Connectors

C++ Connector Server

Der *C++-Connector-Server* ist ein Connector-Server, der C++-Connectors verwaltet. Er kann auf dem Bereitstellungsserver oder auf einem Remote-System installiert werden. Der C++-Connector-Server stellt ein objektorientiertes Anwendungsframework bereit, das die Entwicklung von Connectors vereinfacht, die verantwortlich für die Kommunikation zwischen C++-Connector-Server und dem Endpunkt sind.

CA IAM CS

CA IAM CS ist eine Server-Komponente, die Hosting, Routing und Verwaltung von Java-Connectors verarbeitet. CA IAM CS ist eine Java-Alternative zum C++-Connector-Server. Er ist architektonisch und funktionell dem C++-Connector-Server ähnlich, außer dass es eine Java-API anstelle einer C++ API hat, was Ihren Connectors ermöglicht, in Java implementiert zu werden. Außerdem ist CA IAM CS datengesteuert statt codegesteuert, was mehr Funktionssteuerung vom Container (oder CA IAM CS) anstelle von Connectors selbst erlaubt.

Der Bereitstellungsserver verarbeitet die Bereitstellung von Benutzern und delegiert dann an Connectors (mithilfe von dem C++-Connector-Server oder CA IAM CS), um Endpunkt-Benutzerkonten und Gruppen zu verwalten.

Connectors und Agenten

CA Identity Manager-Connectors werden als Teil der weiteren Bereitstellungsserver-Architektur ausgeführt und kommunizieren mit den in Ihrer Umgebung verwalteten Systemen. Ein Connector handelt als ein Gateway zu einer systemeigenen Endpunkttyp-Systemtechnologie. Zum Beispiel können Rechner, die Active Directory Services (ADS) ausführen, nur verwaltet werden, wenn der ADS-Connector auf einem Connector-Server installiert ist, mit dem der Bereitstellungsserver kommunizieren kann. Connectors verwalten die Objekte, die sich auf den Systemen befinden. Verwaltete Objekte schließen Konten, Gruppen und optional endpunkttypspezifische Objekte ein.

Connectors werden auf dem Connector-Server installiert und einige Komponenten werden auf dem Bereitstellungsserver (zum Beispiel Server-Plug-in) oder Bereitstellungsmanager (Benutzeroberflächen-Plug-ins) installiert.

Einige Connectors erfordern einen Agenten auf den Systemen, die sie verwalten, um den Kommunikationszyklus fertig zu stellen, in welchem Fall sie mithilfe des Bereitstellungs-Installationsprogramms installiert werden können. Agenten können in die folgenden Kategorien unterschieden werden:

Remote-Agenten

Auf den verwalteten Endpunktsystemen installiert

Umgebungsagenten

Auf Systemen wie CA ACF2, CA Top Secret und RACF installiert

Bestimmte Komponenten funktionieren unter UNIX und Windows, einschließlich der folgenden serverbasierten C++-Connector-Optionen:

- UNIX (ETC, NIS)
- Access Control (ACC)

  Hinweis: Der UNIX ACC-Connector kann nur UNIX ACC-Endpunkte verwalten. Der Windows ACC-Connector ist erforderlich, um die Windows ACC-Endpunkte zu verwalten, aber kann auch UNIX ACC-Endpunkte verwalten.
- CA-ACF2
- RACF
- CA Top Secret

Auf die anderen auf C++-Connector-Server basierten Connectors kann vom Solaris-Bereitstellungsserver zugegriffen werden, indem man sich auf das Connector Server Framework (CSF) verlässt. Das CSF erlaubt einem Bereitstellungsserver unter Solaris, mit unter Windows ausgeführten Connectors zu kommunizieren.

Hinweis: Das CSF muss unter Windows ausgeführt werden, um diese Connectors zu verwenden.

Connector Xpress

Connector Xpress ist ein CA Identity Manager-Hilfsprogramm, um dynamische Connectors zu verwalten, dynamische Connectors zu Endpunkten zuzuordnen und Routing-Regeln für Endpunkte festzulegen. Sie können es verwenden, um dynamische Connectors zu konfigurieren, um die Bereitstellung und Verwaltung von SQL-Datenbanken und LDAP-Verzeichnissen zu ermöglichen.

Connector Xpress lässt Sie benutzerdefinierte Connectors ohne die technischen Sachkenntnisse erstellen, die im Allgemeinen erforderlich sind, wenn man vom Bereitstellungsmanager verwaltete Connectors erstellt.

Sie können auch eine Connector-Server-Konfiguration (sowohl Java als auch C++) mithilfe von Connector Xpress einrichten, bearbeiten und entfernen.

Die primäre Eingabe in Connector Xpress ist das systemeigene Schema eines Endpunktsystems. Zum Beispiel können Sie Connector Xpress verwenden, um mit einem RDBMS Verbindung aufzunehmen und das SQL-Schema der Datenbank abzurufen. Sie können dann Connector Xpress verwenden, um Zuordnungen aus diesen Teilen des systemeigenen Schemas einzurichten, die relevant für Identitätsverwaltung und Bereitstellung sind. Eine Zuordnung beschreibt, wie die Bereitstellungsebene ein Element des systemeigenen Schemas darstellt.

Connector Xpress generiert Metadaten, die einem dynamischen Connector die Laufzeitzuordnungen zu einem Zielsystem beschreiben.

Die Ausgabe von Connector Xpress ist ein Metadatendokument, das produziert wird, wenn Sie Ihre Zuordnungen fertig stellen. Die Metadaten sind eine XML-Datei, die die Struktur Ihres Connector für CA IAM CS beschreibt.

Sie beschreibt die Bereitstellungsserver-Klassen und -Attribute und wie sie zum systemeigenen Schema zugeordnet werden.

Die Metadaten werden verwendet, um dynamische Endpunkttypen auf einem oder mehreren Bereitstellungsservern zu erstellen.

Hinweis: Für weitere Informationen zur Verwendung von Connector Xpress finden Sie im *Connector Xpress-Handbuch* im *CA Identity Manager-Bookshelf*.

Zusätzliche Komponenten

CA Identity Manager schließt einige zusätzliche Komponenten ein, die die CA Identity Manager-Funktionalität unterstützen. Einige dieser Komponenten werden mit CA Identity Manager installiert und einige müssen separat installiert werden.

WorkPoint-Workflow

WorkPoint-Workflow-Engine und WorkPoint Designer werden automatisch installiert, wenn Sie CA Identity Manager installieren.

Diese Komponenten ermöglichen Ihnen, eine CA Identity Manager-Aufgabe unter der Workflow-Steuerung zu platzieren und vorhandene Workflow-Prozessdefinitionen zu ändern oder neue Definitionen zu erstellen.

Hinweis: Weitere Informationen zu Workflows finden Sie im *Administrationshandbuch*.

Bereitstellungs-Manager

Der CA Identity Manager-Bereitstellungsmanager verwaltet den Bereitstellungsserver durch eine grafische Benutzeroberfläche. Diese wird für administrative Aufgaben wie die Verwaltung von Bereitstellungsserver-Optionen verwendet. In einigen Fällen können Sie auch den Bereitstellungsmanager verwenden, um gewisse Endpunktattribute zu verwalten, die Sie nicht in der CA Identity Manager-Benutzerkonsole verwalten können.

Der Bereitstellungsmanager wird als Teil der CA Identity Manager-Verwaltungstools installiert.

Hinweis: Diese Anwendung läuft nur unter Windows-Systemen.

Weitere Informationen zum Bereitstellungsmanager finden Sie im *Bereitstellungs-Referenzhandbuch*.

Berichtsserver

CA Identity Manager stellt Berichte bereit, die Sie verwenden können, um den Status von einer CA Identity Manager-Umgebung zu überwachen. Um die im Lieferumfang von CA Identity Manager enthaltenen Berichte zu verwenden, installieren Sie den Berichtsserver, der Teil von CA Identity Manager ist.

Der Berichtsserver basiert auf BusinessObjects Enterprise XI. Wenn Sie über einen bereits vorhandenen BusinessObjects-Server verfügen, können Sie diesen anstelle des Berichtsservers verwenden, um CA Identity Manager-Berichte zu generieren.

Hinweis: Installationsanweisungen finden Sie im *Installationshandbuch*.

Beispiel-CA Identity Manager-Installationen

Mit CA Identity Manager können Sie Benutzeridentitäten und ihren Zugriff auf Anwendungen und Konten auf Endpunktsystemen steuern. Basierend auf der benötigten Funktionalität wählen Sie aus, welche CA Identity Manager-Komponenten zu installieren sind.

In allen CA Identity Manager-Installationen wird der CA Identity Manager Server auf einem Anwendungsserver installiert. Sie verwenden das CA Identity Manager-Installationsprogramm, um die anderen Komponenten zu installieren, die Sie benötigen.

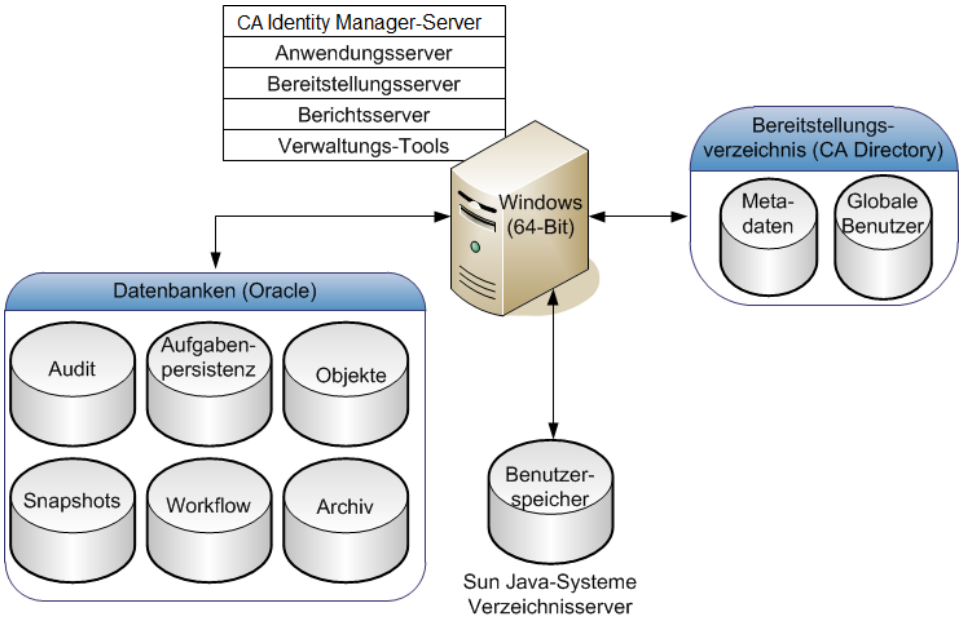
Die folgenden Abschnitte veranschaulichen einige Beispiele für CA Identity Manager-Implementierungen auf allgemeiner Ebene.

Installation mit Bereitstellungskomponenten

CA Identity Manager-Bereitstellung ermöglicht es Ihnen, eine Umgebung zu erstellen, die mit einem Bereitstellungsserver zur Bereitstellung von Konten für verschiedene Endpunktsysteme verbunden ist. Sie können Bereitstellungsrollen Benutzern zuweisen, die Sie durch CA Identity Manager erstellen. Bereitstellungsrollen sind Rollen mit Kontovorlagen, die Konten definieren, die Benutzer auf Endpunktsystemen erhalten können. Konten bieten Benutzern Zugriff auf zusätzliche Ressourcen, wie ein E-Mail-Konto.

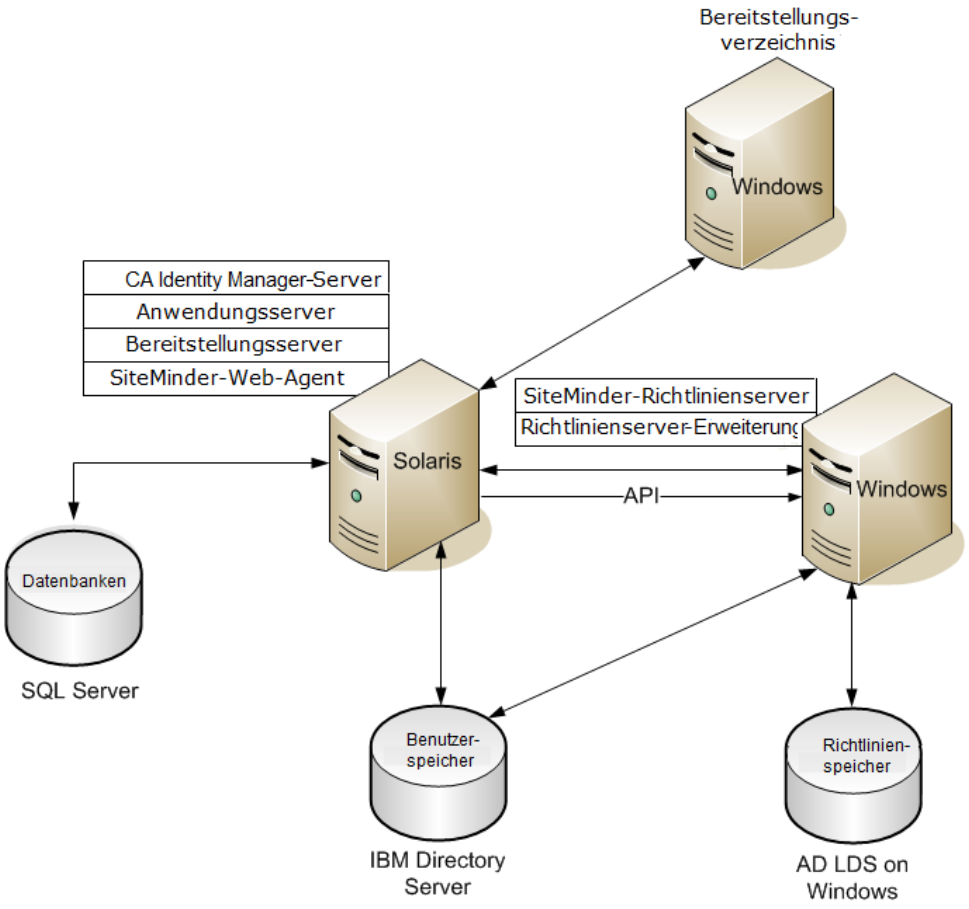
Wenn Sie einem Benutzer eine Bereitstellungsrolle zuweisen, bekommt dieser Benutzer die von den Kontovorlagen in der Rolle definierten Konten. Kontovorlagen definieren auch, wie Benutzerattribute Konten zugeordnet werden. Die Konten werden in verwalteten, von den Kontovorlagen definierten Endpunkten erstellt.

Die folgende Abbildung enthält ein Beispiel für eine CA Identity Manager-Installation mit Bereitstellung:



Installation mit SiteMinder-Richtlinienserver

Ein SiteMinder-Richtlinienserver bietet erweiterte Authentifizierung und Schutz für Ihre CA Identity Manager-Umgebung. Die folgende Abbildung ist ein Beispiel für eine CA Identity Manager-Installation mit einem SiteMinder-Richtlinienserver:



Eine CA Identity Manager-Implementierung, die SiteMinder einschließt, schließt alle Komponenten von der grundlegenden Installation oder der Installation mit Bereitstellung ein, plus diese zusätzlichen Komponenten:

SiteMinder-Web-Agent

Wird zusammen mit dem SiteMinder-Richtlinienserver zum Schutz der Benutzerkonsole verwendet. Der Web-Agent wird auf dem System mit dem CA Identity Manager-Server installiert.

SiteMinder-Richtlinienserver

Bietet erweiterte Authentifizierung und Autorisierung für CA Identity Manager und andere Funktionalität wie Kennwortservices und Single Sign-On.

Erweiterungen für SiteMinder-Richtlinienserver

Ermöglichen einem SiteMinder-Richtlinienserver, CA Identity Manager zu unterstützen. Installieren Sie die Erweiterungen auf jedem SiteMinder-Richtlinienserver Ihrer CA Identity Manager-Implementierung.

SiteMinder-Richtlinienspeicher

Speichert Informationen, dass SiteMinder Zugriff auf Webressourcen verwalten muss.

Wenn CA Identity Manager in SiteMinder integriert ist, schließt der Richtlinienspeicher auch Informationen über CA Identity Manager-Verzeichnisse und Umgebungen ein, sodass SiteMinder erweiterte Authentifizierung angeben kann.

Hinweis: Die Komponenten werden als Beispiele auf unterschiedlichen Plattformen installiert. Allerdings können Sie andere Plattformen wählen. Die CA Identity Manager-Datenbanken befinden sich auf Microsoft SQL Server und der Benutzerspeicher auf einem IBM-Verzeichnisserver. Der SiteMinder-Richtlinienspeicher ist auf AD LDS unter Windows gespeichert.

Kapitel 4: Planen der Implementierung

Um eine CA Identity Manager-Implementierung zu planen, legen Sie fest, wie CA Identity Manager Benutzer verwaltet und welche Funktionalität Sie benötigen, um Ihre Geschäftsziele zu erfüllen. Einige zu berücksichtigende Fragen sind:

- Wie verwalte ich Benutzer?
- Benötige ich Kontobereitstellung?
- Was sind meine benutzerdefinierten Geschäftsanforderungen und sollte ich sie mithilfe von Workflow implementieren?

Anhand der von Ihnen getroffenen Entscheidungen können Sie die beste Art und Weise bestimmen, wie Sie CA Identity Manager für Ihre Umgebung implementieren.

Dieses Kapitel enthält folgende Themen:

Entscheiden, was verwaltet werden soll

Wenn Sie entscheiden, was Sie verwalten wollen, hilft dies bei der Entscheidung, welche Komponenten Sie installieren wollen. Mit CA Identity Manager können Sie Folgendes verwalten:

- Benutzeridentitäten
- Zugriff auf Konten auf Endpunktsystemen

Benutzeridentitäten

Benutzeridentitäten stellen die Personen dar, die ein Unternehmen verwalten muss, wie Mitarbeiter, Unternehmer, Zulieferer und andere.

Um Benutzeridentitäten zu verwalten, müssen Sie nur den CA Identity Manager-Server und die Verwaltungstools installieren.

Konfigurieren der Unterstützung für die Benutzerverwaltung

In CA Identity Manager verwalten Sie Benutzer mit Admin-Rollen, die die CA Identity Manager-Aufgaben festlegen, die von Administratoren ausgeführt werden können.

Hinweis: Bevor Sie die Benutzerverwaltung in CA Identity Manager implementieren, müssen Sie entscheiden, welche Funktionalität Sie benötigen. Außerdem müssen Sie einen Plan entwickeln (siehe Seite 59), in welchen Phasen diese Funktionalität implementiert werden soll.

Um die Unterstützung für die Benutzerverwaltung zu konfigurieren, führen Sie die folgenden allgemeinen Schritte aus:

1. Installieren Sie den CA Identity Manager-Server und die Verwaltungstools.

   Wenn Sie Konten zu verwalteten Benutzern benötigen, müssen Sie auch die Unterstützung für die Bereitstellung (siehe Seite 45) installieren.

   Hinweis: Weitere Informationen dazu finden Sie im *Installationshandbuch*.

2. Erstellen Sie Folgendes in der CA Identity Manager-Management-Konsole:

   - **CA Identity Manager-Verzeichnis**

     Beschreibt einen Benutzerspeicher für CA Identity Manager. Folgende Funktionen sind enthalten:

     - Ein Zeiger zu einem Benutzerspeicher, in dem verwaltete Objekte wie Benutzer, Gruppen und Organisationen gespeichert werden.
     - Metadaten, die beschreiben, wie verwaltete Objekte im Verzeichnis gespeichert und in CA Identity Manager dargestellt werden.

   - **CA Identity Manager-Umgebung**

     Gibt einen Verwaltungs-Namespace an, mit dem CA Identity Manager-Administratoren Objekte wie Benutzer, Gruppen und Organisationen mit einem Satz von zugeordneten Rollen und Aufgaben verwalten können. Die CA Identity Manager-Umgebung steuert die Verwaltung und die grafische Darstellung eines Verzeichnisses.

   Weitere Informationen zu CA Identity Manager-Verzeichnissen und -Umgebungen finden Sie im *Konfigurationshandbuch*.

3. Ändern Sie die Standard-Admin-Rollen und -Aufgaben, um diese Ihren Geschäftsanforderungen anzupassen.

   Zu den typischen Rollenänderungen zählen das Hinzufügen oder Entfernen von Standardaufgaben aus vorhandenen Admin-Rollen oder das Erstellen neuer Admin-Rollen auf Basis der Standardrollen.

Zu den typischen Aufgabenänderungen gehört das Anpassen der Registerkarten zu den Standardbenutzerprofilen, um nur die Informationen einzuschließen, die Sie verwalten möchten. (Die Standardprofilregisterkarten schließen alle Attribute ein, die für Benutzer definiert werden.)

Weitere Informationen zum Ändern der Standard-Admin-Rollen und -Aufgaben finden Sie im *Benutzerkonsolendesign-Handbuch*.

4. Weisen Sie die Admin-Rollen Benutzern zu, die Benutzerverwaltungsaufgaben ausführen.

Bereitstellen von Konten anderer Anwendungen

Die Entscheidung, die Bereitstellung zu implementieren, hängt von der Informationsart ab, die Sie verwalten müssen. Wenn Sie ein zentrales Benutzerverzeichnis verwenden und keine Benutzerkonten in anderen Systemen verwalten möchten, brauchen Sie keine Bereitstellung. Wenn Sie Benutzerkonten über eine Vielzahl von Systemen verwalten möchten, sollten Sie die Bereitstellungsunterstützung implementieren.

Bereitstellungsfunktionen werden durch den Bereitstellungsserver angegeben, der mit CA Identity Manager integriert wird. Der Bereitstellungsserver bietet folgende Funktionen für die Kontobereitstellung:

- Endpunktverwaltung
- Kontosynchronisierung
- Kontovorlagen
- Funktionen zum Durchsuchen und Korrelieren

Hinweis: Die Bereitstellungsinformationen werden in einem Bereitstellungsverzeichnis gespeichert. Wenn CA Identity Manager Benutzer in einem anderen Typ von Verzeichnis verwaltet, schließt deren Bereitstellung einen CA Identity Manager-Benutzerspeicher und ein Bereitstellungsverzeichnis ein.

Endpunktverwaltung

Um Konten bereitzustellen, definieren und verwalten Sie Endpunkte in der CA Identity Manager-Benutzerkonsole. Ein *Endpunkt* ist ein System, für das Benutzer einen Zugriff benötigen. Beispiele für Endpunkte schließen Oracle-Datenbanken, UNIX-NIS-Server, Windows-Server und Microsoft Exchange-Server ein. Verwenden Sie *Kontovorlagen* (siehe Seite 46), um Konten zu erstellen und die Benutzermöglichkeiten in verwalteten Endpunkten zu bestimmen.

Hinweis: Sie können auch den Bereitstellungsmanager verwenden, um Endpunkte zu definieren und zu verwalten. Obwohl wir empfehlen, die Benutzerkonsole für die meisten Endpunkt-Verwaltungsaufgaben zu verwenden, gibt es einige Aufgaben, für die der Bereitstellungsmanager erforderlich ist. Dazu zählt die Verwaltung von bestimmten Endpunktattributen und die Verwaltung von Endpunktobjekten, die keine Konten sind. Weitere Informationen zum Bereitstellungsmanager finden Sie in der *Bereitstellungsreferenz*.

Kontosynchronisierung

Sie können Benutzerkonten über mehrere verwaltete Endpunkte synchronisieren. Wenn die Kontosynchronisierung aktiviert ist, wird eine Änderung an einem Benutzerprofil im Bereitstellungsserver an alle Endpunkte übertragen, wo dieser Benutzer ein Konto hat.

Hinweis: Kontosynchronisierungseinstellungen werden auf der Registerkarte "Profil" für eine CA Identity Manager-Aufgabe angegeben. Weitere Informationen zum Konfigurieren von Admin-Aufgaben finden Sie im *Administrationshandbuch*.

Kontovorlagen

Mit Kontovorlagen wird definiert, wie ein Benutzer in einem verwalteten Endpunkt dargestellt wird. Beispiel: Eine Vorlage für ein Exchange-Konto kann das Format der E-Mail-Adresse eines Benutzers als <Anfangsbuchstabe des Vornamens><Nachname>@mycompany.com definieren.

Kontovorlagen bestimmen auch die Berechtigungen, die ein Benutzer innerhalb eines verwalteten Systems hat. Zum Beispiel kann über die Vorlage für ein Exchange-Konto zusätzlich zum Definieren des Formats einer E-Mail-Adresse auch die Postfachgröße eines Benutzers beschränkt werden.

Sie erstellen und verwalten Kontovorlagen in der Benutzerkonsole.

Funktionen zum Durchsuchen und Korrelieren

Die Funktionen zum Durchsuchen und Korrelieren vereinfachen die Endpunktverwaltung, indem Änderungen in verwalteten Systemen entdeckt und synchronisiert werden.

Die Funktion "Durchsuchen" findet Objekte, einschließlich Konten, in Endpunkten und speichert Referenzen zu diesen im Bereitstellungsverzeichnis. Sie können die Funktion "Durchsuchen" verwenden, um neue zu verwaltende Objekte zu ermitteln. Wenn Sie zum Beispiel Konten in einem LDAP-Verzeichnis bereitstellen und neue Organisationen in diesem Verzeichnis hinzugefügt werden, können Sie mit der Funktion "Durchsuchen" diese neuen Organisationen zur Verwendung in Kontovorlagen einführen.

Die Funktion "Korrelieren" ordnet ein Konto in einem verwalteten Endpunkt einem globalen Benutzer im Bereitstellungsverzeichnis zu. Wenn eine Änderung am Konto über den Endpunkt ausgeführt wird, kann die Funktion "Korrelieren" diese Änderungen mit dem globalen Benutzerkonto synchronisieren.

Hinweis: Weitere Informationen zur Funktionalität "Durchsuchen und Korrelieren" finden Sie im *Administrationshandbuch*.

Konfigurieren der Unterstützung für die Bereitstellung

Nachdem Sie beschlossen haben, die Bereitstellung zu implementieren, müssen Sie die folgenden allgemeinen Schritte ausführen.

1. Verwenden Sie das CA Identity Manager-Server-Installationsprogramm, um den CA Identity Manager-Server, den Bereitstellungsserver, die Bereitstellungsverzeichnis-Initialisierung und die Verwaltungstools zu installieren.

   Hinweis: Weitere Informationen zur Installation von CA Identity Manager-Komponenten finden Sie im *Installationshandbuch*.

2. Konfigurieren Sie den Bereitstellungsmanager für die Verbindung mit dem CA Identity Manager-Server.

3. Konfigurieren Sie die Bereitstellung in der CA Identity Manager-Management-Konsole:

   a. Aktivieren Sie die Bereitstellung.

   b. Konfigurieren Sie eine Umgebung für die Bereitstellung, indem Sie Folgendes ausführen:

      - Importieren von benutzerdefinierten Rollendefinitionen
      - Konfigurieren eines Inbound-Administrators
      - Verbinden der Umgebung mit dem Bereitstellungsserver

   Hinweis: Weitere Informationen finden Sie im *Konfigurationshandbuch*.

4. Erstellen Sie Endpunkte in der Benutzerkonsole.

   Dies erlaubt CA Identity Manager, den Endpunkt zu verwalten.

   Hinweis: Weitere Informationen zur Endpunktverwaltung finden Sie im *Administrationshandbuch*.

5. Durchsuchen und korrelieren Sie den Endpunkt.

   Wenn Sie einen Endpunkt durchsuchen, findet CA Identity Manager die Objekte im Endpunkt und speichert Instanzen davon im Bereitstellungsverzeichnis. Diese Aktion füllt das Bereitstellungsverzeichnis mit Konten und anderen im Endpunkt gefundenen Objekten auf.

   Wenn Sie Konten an einem Endpunkt korrelieren, ordnet CA Identity Manager jedem Konto einen globalen Benutzer im Bereitstellungsverzeichnis zu. Sie können wählen, ob die Korrelationsfunktion globale Benutzer erstellt, die nicht anwesend sind, oder ob sie Konten, die keinen passenden globalen Benutzer haben, dem globalen Benutzer [Standardbenutzer] zuordnet.

6. Erstellen und warten Sie Endpunkt-Benutzerkonten, indem Sie Kontovorlagen nutzen, die die Attribute enthalten, die zur Erstellung von Konten verwendet werden.

7. Ordnen Sie die Kontovorlagen den Bereitstellungsrollen zu.

   Wenn Sie Bereitstellungsrollen Benutzern zuweisen, erstellt CA Identity Manager Konten in den zugeordneten Endpunkten für diese Benutzer.

   Hinweis: Weitere Informationen zu Kontovorlagen und Bereitstellungsrollen finden Sie im *Administrationshandbuch*.

Bestimmen der Audit-Anforderungen

CA Identity Manager bietet Überprüfungsfunktionen, die Ihnen erlauben, Aktivitäten in einer CA Identity Manager-Umgebung zu überwachen.

Diese Informationen werden in einer Audit-Datenbank gespeichert. Umfang und Art der Informationen, die in der Audit-Datenbank gespeichert werden, sind konfigurierbar.

Audit-Daten lassen sich in der Benutzerkonsole durch die Aufgabe "Gesendete Aufgaben anzeigen" anzeigen. Diese Aufgabe erlaubt Administratoren das Suchen und Anzeigen von Aufgaben, die im System auftreten. Administratoren können Aufgabeninformationen auf höherer Ebene oder Aufgaben- und Ereignisdetails anzeigen.

Anmerkungen zum CA Identity Manager-Auditing

Audit-Daten stellen einen Verlaufsdatensatz der Vorgänge bereit, die in einer CA Identity Manager-Umgebung stattfinden. Zum Auditing von Daten in CA Identity Manager benötigen Sie Folgendes:

- Audit-Datenbank
- Auditeinstellungsdatei

Audit-Datenbank

Wenn Sie das CA Identity Manager-Installationsprogramm verwenden, konfiguriert CA Identity Manager eine Verbindung zu einer einzelnen Datenbank, der CA Identity Manager-Datenbank, und erstellt eine Datenquelle, um die Datenbanktabellen für das Auditing zu verbinden.

Hinweis: Die CA Identity Manager-Datenbank schließt auch Daten ein, die von anderen CA Identity Manager-Funktionen einschließlich Aufgabenpersistenz, Workflow und Berichterstellung verwendet werden. Für Skalierbarkeitszwecke können Sie eine neue, separate Instanz einer Datenbank für das Auditing erstellen.

Hinweis: Weitere Informationen zur Audit-Datenbank finden Sie im *Installationshandbuch*.

Auditeinstellungen

Sie konfigurieren Auditeinstellungen in einer Auditeinstellungsdatei. Eine Auditeinstellungsdatei bestimmt den Umfang und die Art der Informationen, die CA Identity Manager überprüft. Sie können eine Auditeinstellungsdatei für Folgendes konfigurieren:

- Aktivieren Sie die Überprüfung für eine CA Identity Manager-Umgebung.
- Aktivieren Sie die Überprüfung für einige oder alle von Admin-Aufgaben generierten CA Identity Manager-Ereignisse.
- Aufzeichnen von Ereignisinformationen bei bestimmten Status wie beim Abschließen oder Abbrechen eines Ereignisses
- Protokollieren Sie Informationen zu Attributen, die an einem Ereignis beteiligt sind. Sie können zum Beispiel Attribute protokollieren, die sich während eines ModifyUserEvent-Ereignisses ändern.
- Legen Sie die Auditebene für die Attributprotokollierung fest.

Hinweis: Weitere Informationen zur Audit-Konfiguration finden Sie im *Konfigurationshandbuch*.

Anmerkungen zu CA Audit

CA Audit ist ein Audit-Management-System, mit dem Sie sicherheitsbezogene Daten für Auditing, Berichterstellung, Compliance-Prüfung und Ereignisüberwachung erfassen und speichern können.

Zur Integration in CA Audit installieren Sie bei der CA Identity Manager-Serverinstallation auch die iRecorder-Komponente. Die iRecorder-Komponente ruft Ereignisse aus CA Identity Manager ab. Auf Grundlage der Richtlinien des CA Audit Policy Manager ignoriert iRecorder das Ereignis oder leitet es weiter zu CA Audit.

Festlegen der Benutzerspeicheranforderungen

Eine CA Identity Manager-Implementierung muss einen Benutzerspeicher einschließen, der die Benutzeridentitäten enthält, die CA Identity Manager verwaltet. Normalerweise ist dies ein vorhandener Benutzerspeicher, den ein Unternehmen verwendet, um Informationen über Benutzer wie Mitarbeiter und Kunden zu speichern.

Wenn Ihre Implementierung die Bereitstellung einschließt, benötigt CA Identity Manager auch ein Bereitstellungsverzeichnis mit den globalen Benutzern, die Konten zugeordnet sind, die sich auf Endpunkten wie Microsoft Exchange, Active Directory und Oracle befinden.

Verwalten mehrerer Benutzerspeicher

Ein Unternehmen kann mehrere Benutzerspeicher verwalten. In jedem Benutzerspeicher erlaubt die Benutzeridentität Zugriff auf unterschiedliche Unternehmensressourcen. Sie können eine der folgenden Methoden verwenden, um mehrere Benutzerspeicher zu verwalten:

- Verwenden Sie CA Identity Manager, um das Bereitstellungsverzeichnis direkt zu verwalten, und verwenden Sie den Bereitstellungsserver, um die Benutzer und Konten in unterschiedlichen Benutzerspeichern indirekt zu verwalten.

  Dieser Ansatz ermöglicht Folgendes:

  - Zentrales Verwalten von Benutzern, die verschiedenen Unternehmensressourcen von einem Speicherort zugewiesen sind
  - Implementieren gemeinsamer Sicherheits- und Geschäftsregeln für alle Unternehmensressourcen Dies kann Folgendes einschließen:
    - Steuerung des rollenbasierten Zugriffs
    - Delegierte Verwaltung
    - Aufgaben und Fenster, die auf Basis des Typs der verwalteten Unternehmensidentitäten angepasst werden

- Identitätsrichtlinien für Regel-basierte Identitätsverwaltung
- Anpassung und Erweiterbarkeit

Hinweis: Weitere Informationen dazu finden Sie im *Administrationshandbuch*.

- Erstellen separater CA Identity Manager-Umgebungen zur Verwaltung jedes Benutzerspeichers

  Bei dieser Methode werden Informationen nicht zwischen Umgebungen freigegeben.

Auswählen der zu installierende Komponenten

Die folgende Tabelle listet die Komponenten auf, die installiert werden müssen, damit die gewünschte Funktionalität unterstützt wird.

Hinweis: Eine Anleitung zur Installation dieser Komponenten finden Sie im *Installationshandbuch*.

Aufgabe	Installieren dieser Komponenten
Verwalten von Benutzeridentitäten in einem vorhandenen Unternehmensbenutzerspeicher	■ CA Identity Manager-Server
Bereitstellen von Konten in Endpunktsystemen	■ Bereitstellungsserver ■ Bereitstellungsverzeichnis ■ Bereitstellungs-Manager ■ Connectors ■ Connector-Server **Hinweis**: Eine Anleitung zum Installieren des gewünschten Connectortyps finden Sie im zugehörigen *Connector-Handbuch*.

Aufgabe	Installieren dieser Komponenten
Implementieren Sie eine oder mehrere der folgenden Funktionen: ■ Erweiterte Authentifizierung ■ Erweiterte Kennwortrichtlinien ■ Unterschiedliche Konsolendesigns für unterschiedliche Sets von Benutzern ■ Konfigurieren der lokalen Voreinstellungen für Benutzer	■ SiteMinder-Richtlinienserver ■ Richtlinienspeicher ■ SiteMinder-Web-Agent ■ CA Identity Manager-Erweiterungen zum Richtlinienserver **Hinweis**: Anleitungen zum Installieren des SiteMinder-Richtlinienservers und des Richtlinienspeichers finden Sie im Installationshandbuch zum *CA SiteMinder Web Access Manager-Richtlinienserver* .Eine Anleitung zum Installieren des Web-Agenten finden Sie im *Installationshandbuch zum CA SiteMinder Web Access Manager-Web-Agent* .
Generieren von Berichten zu CA Identity Manager-Aktivitäten	Berichtsserver

Festlegen der Hardwarevoraussetzungen

Die Hardware, die Sie für eine CA Identity Manager-Installation benötigen, hängt von der Funktionalität, die Sie implementieren möchten, und der Größe Ihrer Bereitstellung ab.

Die folgenden Abschnitte beschreiben typische CA Identity Manager-Implementierungen und deren erforderliche Hardware.

Bereitstellungstypen

Bei der Planung der benötigten Hardware für eine CA Identity Manager-Bereitstellung müssen Sie die Funktionen berücksichtigen, die Sie implementieren möchten, und die Anfangsgröße der Bereitstellung. Verwenden Sie eine der folgenden Kategorien, um die Größe der Bereitstellung zu schätzen.

Hinweis: Der Bereitstellungstyp, den Sie auswählen, bestimmt die Größe der DxGrid-Datei, die vom Bereitstellungsverzeichnis verwendet wird. Sie geben den Bereitstellungstyp an, wenn Sie den CA Identity Manager-Server installieren.

Demonstration

Eine einzelne Serverbereitstellung für Demonstrationszwecke oder für grundlegende Tests in einer Entwicklungsumgebung. Eine Demonstrationsbereitstellung unterstützt bis zu 10.000 bereitgestellte Konten.

Hinweis: Dieser Implementierungstyp unterstützt keine Produktionsimplementierungen.

Grundlegend

Eine Hochverfügbarkeitsimplementierung, die für die meisten kleinen bis mittleren Implementierungen geeignet ist. Eine grundlegende Implementierung unterstützt bis zu 400.000 bereitgestellte Konten.

Dieser Implementierungstyp benötigt zwei Server für die Ausführung der CA Identity Manager-Anwendung und ihrer Komponenten und zwei Server für die Ausführung der CA Identity Manager-Datenbank und des Benutzerspeichers.

Mittel

Eine Hochverfügbarkeitsimplementierung, die für Implementierungen mittlerer Größe geeignet ist. Eine mittlere Bereitstellung unterstützt bis zu 600.000 bereitgestellte Konten.

Großbetrieb

Eine Hochverfügbarkeitsimplementierung, die zusätzliche Server-Cluster einschließt, um zusätzliche Benutzer und eine erhöhte Anzahl von Transaktionen zu bewältigen. Eine große Bereitstellung unterstützt mehr als 600.000 bereitgestellte Konten.

Hinweis: Weitere Informationen zu Hochverfügbarkeitsimplementierungen finden Sie im *Installationshandbuch*.

Zusätzliche Anforderungen für die Bereitstellung

Zusätzlich zu den für eine grundlegende CA Identity Manager-Implementierung benötigten Komponenten sind die folgenden Komponenten erforderlich, wenn CA Identity Manager die Bereitstellung mit einschließt:

- Bereitstellungsserver

  Kann auf dem gleichen Rechner wie der CA Identity Manager-Server installiert werden.

- Bereitstellungsverzeichnis-Initialisierung

  Wichtig! Die Bereitstellungsverzeichnis-Initialisierung muss auf CA Directory installiert werden.

- Bereitstellungs-Manager

  Kann auf jedem Windows-Rechner installiert werden, der Zugriff auf den Bereitstellungsserver hat.

Hinweis: In einer Entwicklungsumgebung können diese Komponenten auf einem Rechner installiert werden, der auch die grundlegenden Installationskomponenten einschließt.

Zusätzliche Anforderungen für die SiteMinder-Integration

Wenn CA Identity Manager SiteMinder integriert werden soll, muss die Implementierung die Komponenten der grundlegenden CA Identity Manager-Installation plus folgende zusätzliche Komponenten umfassen:

- **Richtlinienserver**

  Stellt Dienste für Richtlinienverwaltung, Authentifizierung, Autorisierung und Konten zur Verfügung.

  Der Richtlinienserver kann auf dem gleichen Rechner wie der CA Identity Manager-Server installiert werden, wenn der Richtlinienserver CA Identity Manager fest zugeordnet ist. Wenn der Richtlinienserver andere Anwendungen schützt, empfehlen wir, diesen auf einem getrennten Rechner zu installieren, um beste Leistung zu sichern.

- **Richtlinienspeicher**

  Enthält die alle Daten des Richtlinienservers. Sie können einen Richtlinienspeicher in einer unterstützten LDAP- oder relationalen Datenbank konfigurieren. In Hochverfügbarkeitsimplementierungen empfehlen wir, den Richtlinienspeicher auf einem getrennten Server zu installieren.

- **Erweiterungen zum Richtlinienserver**

  Ermöglichen einem SiteMinder-Richtlinienserver, CA Identity Manager zu unterstützen. Installieren Sie die Erweiterungen auf jedem SiteMinder-Richtlinienserver Ihrer CA Identity Manager-Implementierung.

- **SiteMinder-Web-Agent**

  Wird zusammen mit dem SiteMinder-Richtlinienserver zum Schutz der Benutzerkonsole verwendet. Wird auf dem System mit dem CA Identity Manager-Server installiert.

Auswählen einer Methode für den Benutzerimport

Wenn Sie Benutzer in einen vorhandenen Benutzerspeicher importieren müssen, sollte die Methode, die Sie auswählen, an Ihren Geschäftsanforderungen orientiert sein.

Die folgenden Abschnitte beschreiben Optionen für das Importieren von Benutzern.

Importieren von Benutzern in einen neuen Benutzerspeicher

Nachdem Sie beschlossen haben, wie Sie Benutzerdaten speichern möchten, müssen Sie möglicherweise Benutzer von einem Speicher in den anderen importieren. Je nach Ihrer Implementierung können Sie unterschiedliche Methoden verwenden, um Benutzer zu importieren.

Hinweis: Nachdem Sie Benutzer in einen neuen Benutzerspeicher importiert haben, können Sie Identitätsrichtlinien (siehe Seite 57) verwenden, um Änderungen auf importierte Benutzer anzuwenden.

Importieren von Benutzern über CA Identity Manager

CA Identity Manager bietet folgende Methoden zum Hinzufügen von Benutzern zu einem Benutzerspeicher, der diese verwaltet.

Methode	Funktionen	Beschränkungen
Massendatenlader	Ermöglicht es Ihnen, die Massendatenlader-Aufgabe in der Benutzerkonsole zu verwenden, um Feeder-Dateien hochzuladen, die zur gleichzeitigen Anpassung einer Vielzahl von verwalteten Objekten verwendet werden. Der Vorteil der Massendatenlader-Methode liegt darin, dass Sie den Bearbeitungsprozess von vielen verwalteten Objekten mithilfe einer Informationsdatei (Feeder-Datei) automatisieren können. Die Massendatenlader-Aufgabe kann darüber hinaus einem Workflow-Prozess zugeordnet werden.	Wenn Sie den Massendatenlader verwenden, sehen Sie möglicherweise Out-Of-Memory-Ausnahmen je nach der Zahl von Benutzern, die Sie importieren. Um dieses Problem zu lösen, vergrößern Sie die JVM-Speichereinstellungen.
Remote-Aufruf von Aufgaben über Webservices zur externen Ansteuerung von Aufgaben (TEWS)	Erlaubt die Ausführung von CA Identity Manager-Aufgaben, die für Webservices aktiviert werden, einschließlich der Aufgabe "Benutzer erstellen". Wenn die Aufgabe für die Benutzersynchronisierung konfiguriert ist, wird CA Identity Manager anwendbare Identitätsrichtlinien ausführen.	Leistungsmerkmale des Webservice-Modells sind möglicherweise nicht besonders gut für Hochdurchsatzanforderungen von Massenimportvorgängen geeignet.
IM API	■ Stellt benutzerbasierte APIs zur Verfügung, die direkt für das Erstellen von Benutzern über einen Java-Client aufgerufen werden können. ■ Bietet Kapazitäten für höchsten Durchsatz.	■ Umgeht Audit- und Sicherheitsmechanismen, die von Aufgabenserver bereitgestellt werden. ■ Unterstützt keine Ausführung von Identitätsrichtlinien.

Hinweis: Weitere Informationen zum Massendatenlader finden Sie im *Administrationshandbuch*. Weitere Informationen zu TEWS und zur IM API finden Sie im *Programmierhandbuch für Java*.

Ausführen von Identitätsrichtlinien auf importierten Benutzern

Eine *Identitätsrichtlinie* bezeichnet einen Satz von Geschäftsänderungen, die eintreten, wenn ein Benutzer eine bestimmte Bedingung oder Regel erfüllt. Zu diesen Änderungen zählen das Zuweisen oder Widerrufen von Rollen (einschließlich Bereitstellungsrollen für Benutzer im Bereitstellungsverzeichnis), das Zuweisen oder Widerrufen von Gruppenmitgliedschaften sowie das Aktualisieren von Attributen eines Benutzerprofils.

Sie können Identitätsrichtlinien verwenden, um Änderungen auf Benutzerkonten anzuwenden, nachdem diese in einen neuen Benutzerspeicher importiert wurden.

Dieser Abschnitt beschreibt Methoden für die Ausführung von Identitätsrichtlinien für importierte Benutzer in einem oder in zwei Schritten.

Einstufige Vorgehensweise

Sie können die folgenden Importmethoden verwenden, um in einem Schritt Identitätsrichtlinien auf Benutzern auszuführen, die Sie in einen neuen Benutzerspeicher importieren:

- Massendatenlader in der Benutzerkonsole
- Ausführen der Aufgabe "Benutzer erstellen" über TEWS
- Eingehende Synchronisierung

Zweistufige Vorgehensweise

Bei einer Vorgehensweise in zwei Schritten importieren Sie zuerst Benutzer und führen dann die Identitätsrichtlinien auf diesen Benutzern aus. Sie können diese Methode verwenden, wenn CA Identity Manager Benutzer im Bereitstellungsserver verwaltet. Diese Methode kann je nach Ihren Importanforderungen mehr Flexibilität bieten.

1. Verwenden Sie eines der Importtools für das Hinzufügen von Benutzern zum Bereitstellungsverzeichnis.
2. Rufen Sie für jeden importierten Benutzer über TWES die CA Identity Manager-Aufgabe "Benutzer synchronisieren" auf.

Importieren von Benutzern über den Bereitstellungsserver

Der Bereitstellungsserver bietet Optionen für den Massendatenimport, mit denen Benutzer dem Bereitstellungsverzeichnis hinzugefügt und dort verwaltet werden können. Die folgenden Tabellen beschreiben die Methoden, mit denen Benutzer in das Bereitstellungsverzeichnis importiert werden können.

Methode	Funktionen	Beschränkungen
Batch-Hilfsprogramm (etautil)	Eine Befehlszeilenschnittstellen, über die Sie Objekte im Bereitstellungsverzeichnis verwalten können.	■ Gegenwärtig nur für Windows-Systeme unterstützt.
Durchsuchen und Korrelieren	■ Entdeckt neue Objekte, die vom Bereitstellungsserver in einem bekannten Endpunkt verwalten werden können (einschließlich Benutzern) ■ Bietet Korrelationsfunktionen für Objektinstanzen, die im Endpunkt und auf dem Bereitstellungsserver vorhanden sind. Weitere Informationen dazu finden Sie unter Funktionen zum Durchsuchen und Korrelieren.	■ Standardmäßig stehen die Funktionen zum Durchsuchen und Korrelieren für gegenwärtig unterstützte Connectors zur Verfügung. Das kann auf benutzerdefinierte Connectors ausgedehnt werden. ■ Die Korrelationsoption kann sich bei großen Benutzerzahlen auf die Skalierbarkeit auswirken. Wenn Sie diese Importoption auswählen, müssen Sie die Implikationen auf Leistung und Skalierbarkeit prüfen.

Synchronisieren von globalen Benutzern mit dem CA Identity Manager-Benutzerspeicher

Nachdem Sie Benutzer in den Bereitstellungsserver importiert haben, können Sie die folgenden Methoden verwenden, um diese Benutzer dem CA Identity Manager-Benutzerspeicher hinzuzufügen:

- **Eingehende Synchronisierung**

  Die eingehende Synchronisierung hält die CA Identity Manager-Benutzer bei Änderungen im Bereitstellungsverzeichnis auf dem aktuellen Stand. Änderungen im Bereitstellungsverzeichnis schließen solche mit ein, die von Bereitstellungsmanager oder von Systemen mit Connectors zum Bereitstellungsserver gemacht wurden.

  Beachten Sie Folgendes, wenn Sie die eingehende Synchronisierung für den Import von Benutzern verwenden:

  - In der CA Identity Manager-Management-Konsole können Sie anpassen, wie die Attribute von der eingehenden Anfrage den Attributen in der CA Identity Manager-Aufgabe zugeordnet werden.

    Hinweis: Weitere Informationen finden Sie im *Administrationshandbuch*.

  - Überlegen Sie, welche Änderungen am Bereitstellungsserver zu einer Synchronisierung mit dem Benutzerspeicher des Unternehmens führen sollen. Das Synchronisieren einer Vielzahl von Änderungen kann Auswirkungen auf Leistung und Skalierbarkeit haben.

- **Bereitstellungsrollen und Kontovorlagen**

  Der Bereitstellungsserver kann Konten im CA Identity Manager-Benutzerspeicher mithilfe von Bereitstellungsrollen und Kontovorlagen verwalten. Dies erfordert, dass ein verwalteter Endpunkt, der auf den CA Identity Manager-Benutzerspeicher zeigt, erworben wurde und die entsprechenden Kontovorlagen und Rollen vorhanden sind. In diesem Fall kann globalen Benutzern, die mit einer der in Importieren von Benutzern über den Bereitstellungsserver beschriebenen Optionen erstellt wurde, eine Bereitstellungsrolle zugewiesen werden, mit der das Benutzerkonto im CA Identity Manager-Benutzerspeicher erstellt wird.

Entwickeln eines Bereitstellungsplans

Bei der Planung einer großen Implementierung sollten Sie CA Identity Manager-Funktionalität in Phasen bereitstellen. Mit der folgenden Bereitstellungsreihenfolge können Sie sofort spürbaren Nutzen aus CA Identity Manager ziehen, die Änderungsanforderungen der Implementierung im Laufe der Zeit prüfen und Ihre Umgebung sorgfältig auf optimale Leistung und Skalierbarkeit hin einrichten:

- Self-Service und Kennwortverwaltung
- Identitätsrichtlinien
- Workflow-Genehmigungen

- Delegierte Verwaltung für Benutzer, Gruppe und Organisationsobjekte
- Delegierte Verwaltung für Rollenverwaltung

Prüfen Sie nach jeder Bereitstellungsphase die Leistung, und nehmen Sie Anpassungen vor, bevor Sie zur nächsten Phase übergehen. Unter Optimieren von CA Identity Manager (siehe Seite 69) finden Sie weitere Informationen zu Leistung, Optimierung und Skalierbarkeit.

Bereitstellen von Self-Service und Kennwortverwaltung

Stellen Sie aus den folgenden Gründen Self-Service-Aufgaben und Kennwortverwaltung vor anderen CA Identity Manager-Funktionen bereit:

- Self-Service-Aufgaben und Kennwortverwaltung sind leicht bereitzustellen und sorgen schnell für großen Nutzen.
- Diese Funktionen sind unabhängig vom Modell der delegierten Verwaltung und können nach Bedarf neu konfiguriert werden, um auf veränderte Geschäftsanforderungen zu reagieren.
- Diese Funktionen generieren normalerweise das höchste Volumen an Aufgaben, die CA Identity Manager regelmäßig verarbeitet. Daher gibt es die Möglichkeit, die Skalierbarkeit Ihrer Implementierung zu testen, bevor Sie weitere Funktionen bereitstellen.

Führen Sie zur Bereitstellung von Self-Service-Aufgaben folgende Schritte aus:

1. Konfigurieren Sie die Aufgabe "Selbstregistrierung".

   Dies ist eine öffentliche Aufgabe, die standardmäßig während der Installation aktiviert ist. Um diese Aufgabe zu konfigurieren, können Sie bei Bedarf Felder zur Standardaufgabe "Selbstregistrierung" hinzufügen oder Felder aus dieser entfernen.

2. Stellen Sie die Rolle "Selbstverwaltung" bereit.

   Die Mitgliederregel für diese Rolle sollte so konfiguriert werden, dass sie sich auf alle Benutzer bezieht, oder die Rolle sollte eine Mitgliederregel enthalten, die neuen Benutzern automatisch diese Rolle zuweist. Zum Beispiel können Sie eine Mitgliederregel erstellen, die allen Vollzeitbeschäftigten die Selbstverwaltungsrolle zuweist. Wenn sich ein Benutzer selbst anmeldet, kann CA Identity Manager den Mitarbeitertyp auf "Vollzeit" festlegen (durch Verwendung eines Logical-Attribute-Handlers oder eines Geschäftsaufgaben-Handlers). Der Benutzer entspricht den Kriterien der Mitgliederregel und bekommt die Selbstverwaltungsrolle automatisch zugewiesen.

   Hinweis: Wenn Sie Mitgliederregeln für die Rolle "Selbstverwaltung" konfigurieren, dürfen Sie Administratoren nicht erlauben, Rollenmitglieder hinzuzufügen oder zu entfernen. Da die Rolle automatisch zugewiesen wird, gibt es keinen Bedarf an einem Administrator, der ausdrücklich die Rolle zuweist.

Führen Sie zur Bereitstellung von Kennwortverwaltungsfunktionen folgende Schritte aus:

1. Konfigurieren Sie öffentliche Kennwortverwaltungsaufgaben wie die Aufgabe "Kennwort vergessen".
2. Erstellen Sie Kennwortrichtlinien, die entscheiden, wie Kennwörter erstellt werden und wann sie ablaufen.
3. Stellen Sie die Rolle "Kennwort-Manager" bereit, die Rollenmitgliedern ermöglicht, Benutzerkennwörter zurückzusetzen.

Hinweis: Weitere Informationen zu Rollen, Aufgaben und Kennwortverwaltung finden Sie im *Administrationshandbuch*.

Bereitstellen von Identitätsrichtlinien

Eine Identitätsrichtlinie bezeichnet einen Satz von Geschäftsänderungen, die eintreten, wenn ein Benutzer eine bestimmte Bedingung oder Regel erfüllt. Sie können Identitätsrichtlinien verwenden, um geschäftsorientierte Berechtigungen anzugeben, bevor ein vollständiges Delegierungsmodell bereitgestellt wird. Zum Beispiel können Sie eine Identitätsrichtlinie erstellen, die allen Benutzern, deren Titel "Vertriebs-Manager" ist, die Bereitstellungsrolle "Vertriebs-Manager" zuweist und damit den Zugriff auf Vertriebsanwendungen gewährt. Wenn ein Vertriebsbeauftragter zum "Vertriebs-Manager" befördert wird, bekommt er automatisch Zugriff auf alle Systeme, die er für seinen Job benötigt, ohne dass er auf dazu auf einen Administrator warten muss.

Führen Sie zur Bereitstellung von Identitätsrichtlinien folgende Schritte aus:

1. Konfigurieren Sie Identitätsrichtlinien, die von Änderungen an Benutzerprofilattributen ausgelöst werden.
2. Konfigurieren Sie die Rolle "User Manager", um einer kleine Anzahl von Administratoren zu erlauben, mit Benutzeraufgaben wie "Benutzer erstellen" und "Benutzer ändern" Attribute zu ändern, die die Identitätsrichtlinien auslösen.

   Stellen Sie sicher, dass Sie die Bereichsregeln in den Mitgliederrichtlinien zu "User Manager" konfigurieren, um den Satz von Benutzern zu bestimmen, die Rollenmitglieder verwalten können.

Beachten Sie das Folgende, wenn Sie Identitätsrichtlinien bereitstellen:

- Erstellen Sie zuerst Identitätsrichtlinien, die Genehmigungen erteilen, die *keinen* Workflow benötigen. Dies ermöglicht es Ihnen, Identitätsrichtlinien bereitzustellen, ohne dass Sie Workflow-Prozesse, Genehmigungsformulare und Genehmigermodelle definieren müssen.
- Bevor Sie Identitätsrichtlinien erstellten, sollten Sie sich mit anderen CA Identity Manager-Methoden zur Implementierung von Geschäftsregeln vertraut machen, wie Datenvalidierungsregeln, logische Attribute, Business-Logic-Task-Handler und Workflow-Prozesse. So können Sie ermitteln, welche Methode die beste Lösung darstellt.

  Hinweis: Weitere Informationen zu diesen Methoden finden Sie im *Administrationshandbuch* und im *Programmierhandbuch für Java*.
- Identitätsrichtlinien sind eine effiziente Weise, Berechtigungen in CA Identity Manager zuzuweisen. Allerdings können sie spürbare Auswirkungen auf die Leistung (siehe Seite 85) haben.
- Bei der erstmaligen Bereitstellung von Benutzeraufgaben sollten Sie ggf. Beziehungsregisterkarten wie die "Rollen"-Registerkarten entfernen oder verstecken, auf denen die gleichen Berechtigungen wie für die Identitätsrichtlinien verwaltet werden. Dies senkt das Risiko von unbefugten Berechtigungen und verhindert potenzielle Leistungseinbußen durch falsch eingerichtete Rollen.

Hinweis: Weitere Informationen zu Identitätsrichtlinien finden Sie im *Administrationshandbuch*.

Bereitstellen von Workflow-Genehmigungen

Workflow-Genehmigungen können Ihrer CA Identity Manager-Implementierung eine zusätzliche Ebene der Sicherheit und Automatisierung hinzufügen.

Die Bereitstellung von Workflow-Genehmigungen erfordert die folgenden Aufgaben:

1. Entscheiden Sie, für welche Ereignisse oder Aufgaben Genehmigungen benötigt werden.
2. Definieren Sie für jeden Workflow-Vorgang einen Satz von Genehmigern, auch Teilnehmer genannt.

   Hinweis: Alle Teilnehmer werden dynamisch durch Teilnehmer-Resolver festgelegt. Um eine gute Leistung zu erhalten, müssen Sie die Anzahl der Teilnehmer auf dreißig Benutzer beschränken.
3. Konfigurieren Sie die Genehmigungsformulare.
4. Definieren Sie bei Bedarf benutzerdefinierte Workflow-Prozesse.

Umgebungsgenehmigung und Genehmigung für Workflow auf Aufgabenebene

CA Identity Manager unterstützt zwei Typen von Genehmigungen: Genehmigungen auf Umgebungsebene und Genehmigungen auf Aufgabenebene. Genehmigungen auf Umgebungsebene werden für alle Instanzen eines Ereignisses definiert, ungeachtet der Aufgaben, denen sie zugeordnet sind. Genehmigungen auf Aufgabenebene werden für ein bestimmtes Ereignis definiert, das einer bestimmten Aufgabe zugeordnet ist. Genehmigungen auf Aufgabenebene haben Vorrang vor Genehmigungen auf Umgebungsebene.

Die meisten Genehmigungen werden auf Umgebungsebene definiert, um sicherzustellen, dass bei einem Ereignis unabhängig von der zugeordneten Aufgabe die gleichen Workflow-Aktivitäten auftreten. In den folgenden Situationen sollten Sie jedoch Workflows auf Aufgabenebene implementieren:

- Sie haben spezialisierte Aufgaben, die bestimmte Geschäftsänderungen ausführen, die wiederum Ereignisse generieren, die keine Genehmigungen benötigen.
- Sie haben Änderungsaktionen, die durch Identitätsrichtlinien ausgelöst werden, die wiederum Ereignisse generieren, die keine Workflow-Genehmigung benötigen.
- Sie benötigen die Flexibilität, um bestimmten Workflow-Vorgängen aufgabenspezifische Änderungen zuzuordnen.

Genehmigungen auf Umgebungsebene können bei wachsendem Umfang der Transaktionen bedeutende Verarbeitungs- und Systemressourcen benötigen. Dies kann schließlich zu Leistungs- und Skalierbarkeitsproblemen führen. Mit Genehmigungen auf Aufgabenebene lassen sich diese Probleme ggf. reduzieren oder ganz beseitigen.

Bereitstellen einer delegierten Verwaltung für Benutzer, Gruppen und Organisationen

Bei der delegierten Verwaltung werden Benutzer und deren Berechtigungen verwaltet, indem verschiedene CA Identity Manager-Benutzer die Funktionen zum Ändern, Zuweisen und Verwenden einer Rolle ausführen.

Hinweis: Delegierungsmodelle müssen sorgfältig aufgebaut werden, um eine gute Leistung und Skalierbarkeit der CA Identity Manager-Implementierung sicherzustellen.

Delegierungen werden von Bereichsregeln durchgesetzt, die in Mitglieds- und Admin-Richtlinien für Admin-Rollen definiert werden. Eine Bereichsregel bestimmt die Objekte, bei denen ein Rollenmitglied die Rolle verwenden kann. Zum Beispiel kann eine Bereichsregel einem Benutzer-Manager ermöglichen, die Benutzer seiner Abteilung, aber nicht die von anderen Abteilungen zu verwalten.

Im Allgemeinen sollten Bereichsregeln die logische Struktur des Benutzerspeichers widerspiegeln. Beispiel: In einem hierarchischen LDAP-Benutzerspeicher können Bereiche für Organisationen definiert werden. In einer relationalen Datenbank können Bereiche mithilfe von Attributen wie der Abteilungs-ID definiert werden.

Beachten Sie bei der Bereitstellung einer delegierten Verwaltung für Benutzer, Gruppen und Organisationen Folgendes:

- Beschränken Sie bei benutzerbezogenen Aufgaben den Zugriff auf Beziehungsregisterkarten wie die Registerkarten "Admin-Rollen" und "Bereitstellungsrollen". Diese Beziehungsregisterkarten sind bei Standardbenutzeraufgaben wie "Benutzer erstellen" und "Benutzer ändern" enthalten. Sie sollten diese aus den Standardaufgaben entfernen und nur bei spezialisierten Aufgaben verwenden, die einer kleinen Anzahl von Admin-Rollen zugeordnet sind.
- CA Identity Manager wertet jede Bereichsregel dynamisch aus; Bereichsinformationen werden nicht zwischengespeichert. Erstellen Sie Bereichsregeln, die einfache Verzeichnisabfragen enthalten, um eine gute Leistung zu sichern.
- Werten Sie die Leistung von Bereichsregeln aus, indem Sie ermitteln, wie lange CA Identity Manager benötigt, um die Objekte zurückzugeben, die ein Administrator verwalten kann.

Bereitstellen einer delegierten Verwaltung von Rollen

Die delegierte Verwaltung von Rollen weist die wichtigsten Berechtigungen in CA Identity Manager zu und kann große Auswirkungen (siehe Seite 70) auf die Leistung haben. Aus diesen Gründen sollten Sie eine delegierte Verwaltung von Rollen erst bereitstellen, nachdem Sie alle anderen Funktionen bereitgestellt haben.

Bei der Bereitstellung einer delegierten Verwaltung von Rollen ist Folgendes zu beachten:

- Beschränken Sie die Anzahl der Admin-Rollen, Admin-Rollen-Mitglieder und Admin-Rollen-Administratoren, um die Umgebung zu schützen und eine gute Leistung sicherzustellen.
- Führen Sie nach der Bereitstellung einer delegierten Verwaltung von Rollen Leistungs- und Skalierbarkeitstests durch. Optimieren Sie bei Bedarf die Umgebung.

Kapitel 5: Integrieren von SiteMinder

Dieses Kapitel enthält folgende Themen:

SiteMinder und CA Identity Manager

Bei Integration von CA Identity Manager und CA SiteMinder kann CA SiteMinder die CA Identity Manager-Umgebung um die folgenden Funktionen ergänzen:

Erweiterte Authentifizierung

CA Identity Manager beinhaltet standardmäßig eine systemeigene Authentifizierung für CA Identity Manager-Umgebungen. CA Identity Manager-Administratoren müssen einen gültigen Benutzernamen und ein Kennwort eingeben, um sich an einer CA Identity Manager-Umgebung anzumelden. CA Identity Manager authentifiziert den Namen und das Kennwort mithilfe des Benutzerspeichers, den CA Identity Manager verwaltet.

Wenn CA Identity Manager mit CA SiteMinder integriert ist, verwendet CA Identity Manager die grundlegende CA SiteMinder-Authentifizierung, um die Umgebung zu schützen. Beim Erstellen einer CA Identity Manager-Umgebung werden in CA SiteMinder eine Richtliniendomäne und ein Authentifizierungsschema erstellt, um diese Umgebung zu schützen.

Ist CA Identity Manager mit CA SiteMinder integriert, können Sie auch die SiteMinder-Authentifizierung verwenden, um die Management-Konsole zu schützen.

Zugriffsrollen und -aufgaben

Zugriffsrollen ermöglichen CA Identity Manager-Administratoren, Berechtigungen in Anwendungen zuzuweisen, die von CA SiteMinder geschützt werden. Diese Zugriffsrollen stellen eine einzelne Aktion dar, die ein Benutzer in einer Geschäftsanwendung ausführen kann, wie beispielsweise eine Bestellung in einer Finanzanwendung zu generieren.

Verzeichniszuordnung

Ein Administrator muss möglicherweise Benutzer verwalten, deren Profile in einem anderen als dem für die Authentifizierung des Administrators verwendeten Benutzerspeicher enthalten sind. Bei der Anmeldung an der CA Identity Manager-Umgebung wird der Administrator mithilfe eines Verzeichnisses authentifiziert, und ein anderes Verzeichnis berechtigt den Administrator, Benutzer zu verwalten.

Bei Integration von CA Identity Manager und CA SiteMinder können Sie eine CA Identity Manager-Umgebung so konfigurieren, dass unterschiedliche Verzeichnisse für Authentifizierung und Autorisierung verwendet werden.

Designs für unterschiedliche Benutzergruppen

Ein Design ändert das Erscheinungsbild der Benutzerkonsole. Bei Integration von CA Identity Manager und CA SiteMinder können Sie festlegen, dass unterschiedlichen Benutzergruppen unterschiedliche Designs angezeigt werden. Um diese Änderung durchzuführen, verwenden Sie zum Zuordnen eines Designs zu einer Benutzergruppe eine SiteMinder-Antwort. Die Antwort ist mit einer Regel in einer Richtlinie verknüpft, die einem Satz von Benutzern zugeordnet ist. Wenn die Regel ausgelöst wird, wird wiederum die Antwort ausgelöst, um an CA Identity Manager Informationen zum Design weiterzugeben, mit dem die Benutzerkonsole erstellt werden soll.

Hinweis: Weitere Informationen finden Sie im *Handbuch zum Benutzerkonsolendesign*.

Gebietsschemavoreinstellungen für eine lokalisierte Umgebung

Bei Integration von CA Identity Manager und CA SiteMinder können Sie mithilfe des HTTP-Headers "Imlanguage" Gebietsschemavoreinstellungen für einen Benutzer definieren. Sie legen diesen Header am SiteMinder-Richtlinienserver innerhalb einer SiteMinder-Antwort fest und geben ein Benutzerattribut als Wert des Headers an. Dieser Imlanguage-Header dient als Gebietsschemavoreinstellung höchster Priorität für einen Benutzer.

Hinweis: Weitere Informationen finden Sie im *Handbuch zum Benutzerkonsolendesign*.

Weitere Informationen:

Installation mit SiteMinder-Richtlinienserver (siehe Seite 41)

Authentifizierung - SiteMinder

CA Identity Manager schließt die folgenden Konsolen ein, die geschützt werden sollten:

Benutzerkonsole

Ermöglicht CA Identity Manager-Administratoren, Aufgaben in einer CA Identity Manager-Umgebung auszuführen.

Verwaltungskonsole

Ermöglicht CA Identity Manager-Administratoren, ein CA Identity Manager-Verzeichnis, ein Bereitstellungsverzeichnis und eine CA Identity Manager-Umgebung zu erstellen und zu konfigurieren.

CA Identity Manager schließt die systemeigene Authentifizierung ein, die die Benutzerkonsole standardmäßig schützt. Die Management-Konsole wird nicht standardmäßig geschützt, aber Sie können CA Identity Manager so konfigurieren, dass sie geschützt wird. CA SiteMinder kann auch zum Schützen der Management-Konsole verwendet werden.

Um andere Typen der Authentifizierung für die Benutzerkonsole zu konfigurieren wie Zertifikat oder Schlüsselauthentifizierung, muss SiteMinder in CA Identity Manager integriert werden.

Hinweis: Weitere Informationen finden Sie im *Konfigurationshandbuch*.

Kapitel 6: Optimieren von CA Identity Manager

Dieses Kapitel enthält folgende Themen:

CA Identity Manager-Leistung

Die CA Identity Manager-Leistung hängt von der individuellen Leistung der unterschiedlichen Funktionen und Komponenten ab.

Sie können die folgende Funktionalität in einer CA Identity Manager-Umgebung optimieren:

- Rollen
- Aufgaben
- Gruppenmitgliedschaft und Verwaltung
- Identitätsrichtlinien

Für zusätzliche Leistungsgewinne können Sie auch die folgenden Komponenten anpassen:

- Benutzerspeicher
- Bereitstellungskomponenten
- Laufzeitkomponenten, einschließlich der Datenbanken wie der Aufgabenpersistenz-Datenbank, und Anwendungsservereinstellungen

Um beste Leistung sicherzustellen, können Sie die CA Identity Manager-Funktionalität mithilfe der Richtlinien in den folgenden Abschnitten konfigurieren. Messen Sie dann die Leistung und passen Sie bei Bedarf die Komponenten an. Da die Komponenten zusammenarbeiten, müssen Sie die Schritte ggf. mehrere Male durchführen, bevor Sie die optimalen Einstellungen für Ihre Umgebung gefunden haben.

Optimierung von Rollen

CA Identity Manager enthält drei Typen von Rollen:

- Admin-Rollen

  Bestimmen die Berechtigungen, die ein Benutzer in der Benutzerkonsole hat.

  Wenn sich ein Benutzer in einer CA Identity Manager-Umgebung anmeldet, hat das Konto des Benutzers eine oder mehrere Admin-Rollen. Jede Admin-Rolle enthält Aufgaben, wie "Benutzer erstellen", die vom Benutzer in der CA Identity Manager-Umgebung ausgeführt werden können. Die Admin-Rollen, die ein Benutzer hat, bestimmen die Darstellung der Benutzerkonsole. Daher sehen Benutzer nur die Aufgaben, die ihren Rollen zugeordnet sind.

- Bereitstellungsrollen

  Geben Benutzern Konten in verwalteten Endpunkten wie einem E-Mail-System.

- Zugriffsrollen

  Bieten eine zusätzliche Möglichkeit, Berechtigungen in CA Identity Manager anzugeben.

Rollen schließen Richtlinien ein, die Folgendes bestimmen:

- Wer die Rolle verwenden kann (nur für Admin- und Zugriffsrollen) und wo sie diese verwenden können.
- Wer Rollenmitglieder und Administratoren verwalten kann.
- Wer die Rollendefinition ändern kann.

Die Überprüfung von Rollen und den ihnen zugeordneten Berechtigungen können eine spürbare Auswirkungen auf die CA Identity Manager-Leistung haben.

Auswirkung der Rollenprüfung bei der Anmeldung auf die Leistung

Wenn ein CA Identity Manager-Benutzer versucht, sich bei der Benutzerkonsole anzumelden, werden folgende Aktionen durchgeführt:

1. CA Identity Manager fordert den Benutzer auf, Anmeldeinformationen wie Benutzername und Kennwort einzugeben.
2. Die Anmeldeinformationen des Benutzers werden mithilfe von einer der folgenden Methoden authentifiziert:
   - Systemeigene CA Identity Manager-Authentifizierung
   - SiteMinder-Authentifizierung, wenn die CA Identity Manager-Implementierung SiteMinder enthält

3. CA Identity Manager wertet jede Mitgliederrichtlinie für jede Admin-Rolle in der Umgebung aus, um zu entscheiden, welche Admin-Rollen für den Benutzer gelten.

   Hinweis: Diese Auswertung wird für einen bestimmten Benutzer nur einmal ausgeführt. Nach der Anfangsauswertung speichert CA Identity Manager die Ergebnisse. CA Identity Manager verwendet die zwischengespeicherten Informationen so lange, bis eine Änderung an dem Benutzer oder dem Satz von Mitgliederrichtlinien vorgenommen wird. In diesem Fall aktualisiert CA Identity Manager die Informationen im Zwischenspeicher.

4. Die CA Identity Manager-Benutzerkonsole zeigt die Kategorien an, die der Benutzer auf Basis seiner Rollen anzeigen kann.

Dieser Prozess wird für jeden Benutzer ausgeführt, der sich bei der Benutzerkonsole anmeldet. Wenn eine CA Identity Manager-Umgebung eine Vielzahl von Rollen oder ineffiziente Mitgliederrichtlinien enthält, kann sich die Prüfung der Rollenmitgliedschaft merklich auf die Leistung auswirken. In diesem Fall wird der Begrüßungsbildschirm, den Benutzer bei der Anmeldung an der Benutzerkonsole sehen, nur sehr langsam angezeigt.

Hinweis: CA Identity Manager muss keine Mitgliederrichtlinien auswerten, wenn ein Benutzer auf eine öffentliche Aufgabe zugreift, um ein vergessenes Kennwort selbst zu registrieren oder anzufordern. In diesen Fällen benötigt CA Identity Manager eine Liste der Rollen des Benutzers, da keine vollständige Benutzerkonsole angezeigt wird.

Rollenobjekte und Leistung

Um jede Rolle zu unterstützen, erstellt CA Identity Manager in Abhängigkeit von der Rollenkonfiguration eine Anzahl von Objekten im CA Identity Manager-Objektspeicher (siehe Seite 33).

CA Identity Manager erstellt ein Basisobjekt für jede Rolle. Zusätzlich zum Basisobjekt erstellt CA Identity Manager ein Objekt für jede Richtlinie.

Eine Vielzahl von Rollenobjekten kann sich auf die Leistung beim Durchsuchen des Objektspeichers und bei der Richtlinienauswertung auswirken.

Objektspeicher-Leistung

CA Identity Manager speichert Informationen, um Benutzer und Berechtigungen in einem Objektspeicher verwalten zu können. Eine Vielzahl von Rollenobjekten im Objektspeicher kann folgende Probleme verursachen:

- Die Suche nach verwalteten Objekten über CA Identity Manager-Aufgabenfenster dauert länger.

  Um die Auswirkung auf die Suchen zu reduzieren, können Sie die für die Suche verwendeten Attribute indizieren (siehe Seite 90).

- Rollenverwaltungsaufgaben werden langsamer ausgeführt.

  Zu den Rollenverwaltungsaufgaben, die von einem großen Objektspeicher betroffen sind, gehören folgende:

  - Die Aufgabe "Admin-Rolle erstellen" ist langsam, weil CA Identity Manager bestätigen muss, dass der Rollenname im Objektspeicher eindeutig ist.
  - Die Aufgabe "Admin-Rolle löschen" muss alle Objekte entfernen, die zur Unterstützung der Rolle erstellt wurden, und der Objektzwischenspeicher muss aktualisiert werden.

- CA Identity Manager benötigt viel Zeit, um Rollenrichtlinien auszuwerten.

CA Identity Manager speichert Informationen im Objektspeicher zwischen, um die Leistung zu verbessern.

Optimieren der Rollenrichtlinienauswertung

Für jede Admin-Rolle können Sie drei Typen von Richtlinien erstellen:

- Mitgliederrichtlinien

  Definieren Mitgliederregeln, mit denen die Benutzer bestimmt werden, die die Rolle erhalten, und Bereichsregeln, mit denen die Objekte bestimmt werden, die Rollenmitglieder verwalten können.

- Admin-Richtlinien

  Definieren Admin-Regeln, Bereichsregeln und Administratorrechte für eine Rolle.

- Eigentümerrichtlinien

  Legen fest, wer eine Rolle ändern kann.

Um die Leistung bei der Auswertung der CA Identity Manager-Rollenrichtlinien zu optimieren, berücksichtigen Sie Folgendes:

- Beschränken Sie die Anzahl von Admin-Rollen in einer CA Identity Manager-Umgebung.
- Befolgen Sie die Richtlinien für das Erstellen von Richtlinienregeln (siehe Seite 73).
- Passen Sie den Benutzerspeicher an.
- Passen Sie den Richtlinienspeicher an, wenn SiteMinder in CA Identity Manager integriert ist.

Richtlinien für das Erstellen von Richtlinienregeln

Einer der Schlüsselfaktoren beim Bestimmen der umfassenden Leistung von Rollenrichtlinienauswertungen ist der Zeitumfang, der benötigt wird, um einzelne Richtlinienregeln auszuwerten. Um die Dauer der Richtlinienregelauswertung zu verbessern, müssen Sie beim Erstellen der Richtlinie Folgendes beachten:

- Beschränken Sie wenn möglich die Anzahl der Richtlinienobjekte, die CA Identity Manager erstellt, und die Anzahl der Suchen im Benutzerspeicher, die CA Identity Manager ausführt, indem Sie Richtlinienregeln mit komplexen Ausdrücken erstellen.

  Eine einzelne Regel mit einem komplexen Ausdruck ist effizienter als mehrere Regeln mit einfachen Ausdrücken.

- Wählen Sie wenn möglich den effizientesten und am besten skalierbaren Richtlinienregeltyp aus.
- Aktivieren Sie die Option für die Auswertung von Richtlinienregeln im Arbeitsspeicher.

  Die Option für die Auswertung im Arbeitsspeicher reduziert deutlich die Richtlinienauswertungsdauer, indem Informationen über einen auszuwertenden Benutzer aus dem Benutzerspeicher abgerufen werden und eine Repräsentation dieses Benutzers im Arbeitsspeicher abgelegt wird. CA Identity Manager verwendet die Repräsentation im Arbeitsspeicher, um die Attributwerte in Bezug auf die Richtlinienregeln zu vergleichen.

  Hinweis: Weitere Informationen zur Option für die Auswertung im Arbeitsspeicher finden Sie im *Konfigurationshandbuch*.

- Passen Sie den Benutzerspeicher an.
- Passen Sie den Richtlinienspeicher an, wenn SiteMinder in Ihrer CA Identity Manager-Implementierung integriert ist.

Beschränken Sie Richtlinienobjekte und Suchen im Benutzerspeicher.

Jede Regel in einer Rollenrichtlinie benötigt einen Satz von Objekten im Objektspeicher. Wenn CA Identity Manager eine Regel auswertet, lädt es diese Objekte und führt alle erforderlichen Suchen im Benutzerspeicher aus.

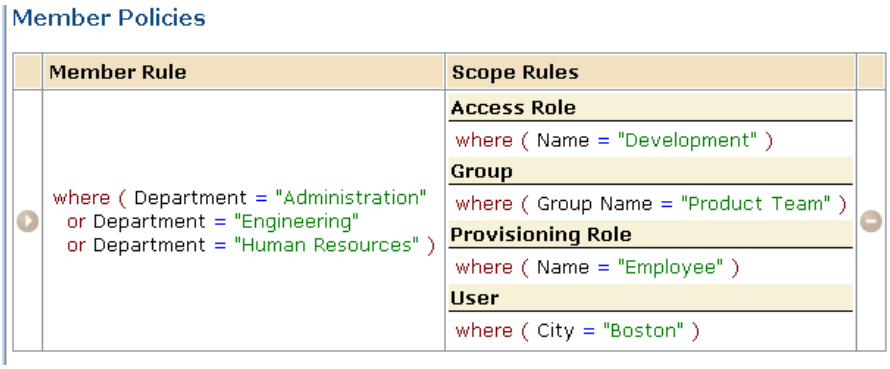
Das folgende Beispiel zeigt eine Mitgliederrichtlinie, die drei Mitgliederregeln umfasst. Jede Regel umfasst vier Bereichsregeln.

In diesem Beispiel erstellt CA Identity Manager die Objekte und führt die in der folgenden Tabelle beschriebenen Benutzerspeichersuchen aus, wenn die Mitgliederrichtlinie ausgewertet und angewendet wird.

Regel	Richtlinienobjekte	Potenzielle Benutzerspeichersuchen
■ Mitgliederregel: where (Department = "Administration") ■ Benutzerbereich: City = "Boston" ■ Gruppenbereich: Group Name = "Product Team" ■ Bereitstellungsrollenbereich: Name = "Employee" ■ Zugriffsaufgabenbereich:Name = "Development"	5	5 (eine für jedes Regeldefinitionsobjekt)
■ Mitgliederregel: where (Department = "Engineering") ■ Benutzerbereich: City = "Boston" ■ Gruppenbereich: Group Name = "Product Team" ■ Bereitstellungsrollenbereich: Name = "Employee" ■ Zugriffsaufgabenbereich:Name = "Development"	5	5
■ Mitgliederregel: where (Department = "Human Resources") ■ Benutzerbereich: City = "Boston" ■ Gruppenbereich: Group Name = "Product Team" ■ Bereitstellungsrollenbereich: Name = "Employee" ■ Zugriffsaufgabenbereich:Name = "Development"	5	5

In diesem Beispiel erstellt CA Identity Manager 15 Objekte und führt 15 Verzeichnissuchen aus, um Mitgliedschaft und Bereich zu bestimmen.

Um die Anzahl von Richtlinienobjekten und Benutzerspeichersuchen zu beschränken, die CA Identity Manager ausführt, werden die Regeln in komplexen Ausdrücken kombiniert. Das folgende Beispiel gibt die gleichen Berechtigungen aus dem ersten Beispiel in nur einer Mitgliederregel an.



In diesem Beispiel erstellt CA Identity Manager nur zehn Richtlinienobjekte und führt nur fünf Benutzerspeichersuchen aus.

Regel	Richtlinienobjekte	Potenzielle Benutzerspeichersuchen
■ Mitgliederregel: where (Department = "Administration") OR where (Department = "Engineering") OR where (Department = "Human Resources") ■ Benutzerbereich: City = "Boston" ■ Gruppenbereich: Group Name = "Product Team" ■ Bereitstellungsrollenbereich: Name = "Employee" ■ Zugriffsaufgabenbereich:Name = "Development"	5	5

Auswählen von skalierbaren Richtlinienregeltypen

Zusätzlich zur Anzahl der Richtlinienregeln kann sich auch der Typ der Richtlinienregel auf die Leistung auswirken. Normalerweise basiert die Erstellung der Richtlinienregeln darauf, wie der Benutzerspeicher strukturiert ist und wie Berechtigungen ermittelt werden. Zum Beispiel können Sie Richtlinienregeln auf Basis der Gruppenmitgliedschaft, der Organisation oder der Benutzerattribute erstellen. Wenn es allerdings verschiedene Möglichkeiten gibt, Richtlinienregeln zu erstellen, müssen Sie die Leistungsrichtlinien in der folgenden Tabelle berücksichtigen, bevor Sie entscheiden, welcher Typ von Regel verwendet werden soll.

Hinweis: Die Richtlinienregeltypen in der folgenden Tabelle werden in Reihenfolge der Leistung aufgelistet, beginnend mit dem effizientesten Regeltyp.

Richtlinienregeltyp	Leistungshinweise
Organisation	■ Beste Gesamtleistung ■ Benötigt keine Suche in LDAP-Verzeichnissen. CA Identity Manager verwendet in der Richtlinienregel den DN des Benutzers, der bewertet wird, und den DN der Organisation.
Rolle	■ CA Identity Manager speichert Rollenobjektinformationen und frühere Auswertungen im Zwischenspeicher des Objektspeichers. ■ In den meisten Fällen ist die Leistung so gut wie die Organisationsrichtlinienregeln es erlauben.
Benutzerattribut	■ Bietet die beste Suchleistung des Benutzerspeichers und ist am wenigsten von großen Benutzerumfängen betroffen. ■ Ermöglicht es Ihnen, die Auswertung im Arbeitsspeicher auszuführen und so bedeutende Leistungsgewinne zu erzielen.
Gruppenmitgliedschaft	■ Leistung hängt von Gruppengröße und Benutzerspeichertyp ab.

Aufgaben-Optimierungen

In CA Identity Manager hängen die Aufgaben, die ein Benutzer in der Benutzerkonsole sieht, von den Berechtigungen dieses Benutzers ab. Um Aufgaben anzuzeigen und auszuführen, muss CA Identity Manager mehrere Sicherheitsprüfungen ausführen, die spürbare Auswirkungen auf die Leistung haben können, wenn sie auf alle Benutzer in einer CA Identity Manager-Umgebung angewendet werden.

CA Identity Manager führt Sicherheitsprüfungen aus, wenn die folgenden Aktionen stattfinden:

- Benutzer meldet sich bei der Benutzerkonsole an

  In diesem Fall muss CA Identity Manager die Rollen des Benutzers auswerten, um zu entscheiden, auf welche Aufgaben dieser Benutzer in der Benutzerkonsole zugreifen kann.

- Benutzer startet eine Aufgabe

  Wenn eine Aufgabe gestartet wird, muss CA Identity Manager entscheiden, welche Objekte dieser Benutzer mit dieser Aufgabe verwalten darf.

- Benutzer greift auf eine Beziehungsregisterkarte zu

  Eine Beziehungsregisterkarte ist eine Registerkarte, auf der ein Benutzer eine Eins-zu-Viele-Beziehung zwischen dem Thema der Aufgabe und einem Satz von Berechtigungen anzeigen oder verwalten kann. Ein Beispiel für eine Beziehungsregisterkarte ist die Registerkarte "Admin-Rollen", auf der die Rollen angezeigt werden, die ein Benutzer hat.

- Benutzer fügt Objekte auf einer Beziehungsregisterkarte hinzu

  Beispiel: CA Identity Manager führt zusätzliche Sicherheitsprüfungen aus, wenn ein Benutzer einem anderen Benutzer über die Registerkarte "Admin-Rollen" zusätzliche Rollen hinzufügt.

Die Aufgabenleistung wird von folgenden Faktoren beeinflusst:

- Vom Aufgabenbereich, der entscheidet, wo ein Administrator eine Aufgabe verwenden kann.
- Von den Beziehungsregisterkarten, auf denen die Beziehung eines Objekts zu anderen Objekten angezeigt wird

Aufgabenbereichs-Auswertung und Leistung

Wenn ein Administrator eine Admin-Aufgabe verwendet, die eine Suche nach einem verwalteten Objekt wie Benutzer, Gruppe, Organisation, Aufgabe oder Rolle enthält, prüft CA Identity Manager Aufgabenbereichsregeln und wendet diese an. Diese Regeln können sich merklich auf die Dauer auswirken, die CA Identity Manager benötigt, um die Liste von Objekten anzuzeigen, die für die Aufgabe ausgewählt werden können.

Hinweis: Im Gegensatz zu Richtlinienauswertungen von Mitgliedern, Admins und Eigentümern werden Informationen zu Bereichsregelauswertungen nicht in einem Zwischenspeicher abgelegt.

Der Aufgabenbereich wird durch Folgendes bestimmt:

- Der Typ des Objekts, das die Aufgabe verwaltet.
- Bereichsregeln, die auf die Admin-Rolle angewendet werden, die die Aufgabe enthält. Bereichsregeln werden in Mitglieder-, Eigentümer- und Admin-Richtlinien definiert.
- Benutzerdefinierte Suchkriterien.

Nehmen Sie zum Beispiel die Aufgabe "Benutzer ändern", die in der Rolle "User Manager" enthalten ist. Die Rolle "User Manager" hat eine Mitgliederrichtlinie mit einer Bereichsregel, die Benutzer-Managern erlaubt, Benutzer in der Organisation "Employees" zu verwalten. Ein Administrator öffnet die Aufgabe "Benutzer ändern" und gibt die Suchkriterien ein: Der Nachname beginnt mit A. In diesem Fall umfasst der Bereich für die Aufgabe "Benutzer ändern" alle Benutzer in der Organisation "Employees", deren Nachname mit A beginnt.

Wiedergabe von Beziehungsregisterkarten in CA Identity Manager

Eine Beziehungsregisterkarte erlaubt Benutzern, die Beziehung anzuzeigen und zu verwalten, die zwischen dem Subjekt einer Aufgabe und einem Satz von Berechtigungen besteht. Zum Beispiel zeigt die Registerkarte "Bereitstellungsrollen" die Bereitstellungsrollen an, die ein Benutzer hat.

Um die Objekte zu bestimmen, die auf einer Beziehungsregisterkarte angezeigt werden, führt CA Identity Manager zahlreiche Sicherheitsprüfungen aus, die sich merklich auf die Leistung auswirken können.

Das folgende Beispiel zeigt die Schritte, die CA Identity Manager ausführt, um die Registerkarte "Bereitstellungsrollen" wiederzugeben:

1. Ein Administrator klickt in der Aufgabe "Benutzer ändern" auf die Registerkarte "Bereitstellungsrollen".
2. CA Identity Manager ruft die Bereitstellungsrollen ab, bei denen der ausgewählte Benutzer Mitglied ist.
3. Wenn die Registerkarte so konfiguriert ist, dass sie die Verwaltung von Rollenadministratoren erlaubt, führt CA Identity Manager einen zweiten Aufruf durch, um die Liste der Bereitstellungsrollen abzurufen, bei denen der ausgewählte Benutzer Administrator ist.
4. CA Identity Manager wertet jede Bereitstellungsrolle des Benutzers aus um festzustellen, ob der Administrator, der die Aufgabe initiiert hat, die Mitgliedschaft für diese Rolle verwalten kann.

   Wenn der Administrator Rollenmitglieder verwalten kann, zeigt CA Identity Manager in der Rollenliste der Registerkarte in der Spalte "Mitgliedschaft" für diese Rolle ein aktiviertes Kontrollkästchen an.
5. CA Identity Manager wertet jede Bereitstellungsrolle des Benutzers aus um festzustellen, ob der Administrator, der die Aufgabe initiiert hat, die administrativen Rechte für diese Rolle verwalten kann.

   Wenn der Administrator administrative Rechte verwalten kann, zeigt CA Identity Manager in der Rollenliste der Registerkarte in der Spalte "Administrator" für diese Rolle ein aktiviertes Kontrollkästchen an.

   CA Identity Manager muss die Schritte 2–5 ausführen, um die aktuellen Bereitstellungsrollen des Benutzers anzuzeigen. Wenn der Administrator eine neue Bereitstellungsrolle zuweisen muss, sind die folgenden zusätzlichen Schritte erforderlich.
6. Der Administrator klickt auf die Schaltfläche "Hinzufügen", um die neu zuzuweisenden Bereitstellungsrollen zu suchen.
7. CA Identity Manager zeigt ein Suchfenster an, über das der Administrator die hinzuzufügende Rolle suchen kann.
8. Der Administrator gibt einen Suchfilter ein, um die hinzuzufügende Rolle zu finden.

9. CA Identity Manager gibt die Liste von Bereitstellungsrollen zurück, die folgende Kriterien erfüllen:
   - Die Rollen stimmen mit dem vom Administrator eingegebenen Suchfilter überein.
   - Der Administrator kann die Mitgliedschaft für die Rollen verwalten.
   - Der Benutzer gehärt zu dem administrativen Bereich des Administrators für die Rollen.
   - Der Benutzer hat die Bereitstellungsrollen noch nicht.
10. CA Identity Manager wiederholt Schritt 9, um die Rollen zu bestimmen, bei denen der Administrator Administratorrechte verwalten kann.

Beziehungsregisterkarten und Leistung

Aufgrund der Anzahl an Sicherheitsprüfungen, die CA Identity Manager ausführt, kann sich die Wiedergabe der Beziehungsregisterkarte merklich auf die Leistung auswirken. Die Faktoren, die die Leistung bestimmen, variieren je nach Registerkartentyp.

Bei Beziehungsregisterkarten von Rollen können sich die folgenden Faktoren auf die Leistung auswirken:

- Anzahl von Rollen, bei denen das Subjekt der Aufgabe ein Mitglied ist
- Anzahl von Rollen, bei denen das Subjekt der Aufgabe ein Administrator ist
- Gesamtanzahl von Objekten im System, bei denen CA Identity Manager die Rollen des Subjekts berechnen muss
- Anzahl von Mitglieds-/Admin-Richtlinien pro Rolle
- Komplexität der Mitglieds-/Admin-Richtlinienbereichsregeln
- Die Möglichkeit, zwischengespeicherte Autorisierungen zu verwalten, damit die Aufgabenaufrufer die Auswirkung der Sicherheitsdurchsetzung beschränken

Um Gruppenmitgliedschaft und Administratorrechte auf Gruppenbeziehungsregisterkarten zu bestimmen, muss CA Identity Manager alle Gruppen im Benutzerspeicher suchen. Die Leistung dieser Suchen hängt von den folgenden Faktoren ab:

- Anzahl von Gruppenobjekten im Benutzerspeicher
- Anzahl von Mitgliedern in einer Gruppe
- Leistung von Datenbank oder Verzeichnis, wo sich der Benutzerspeicher befindet

Prozessverarbeitung und Leistung

Admin-Aufgaben beinhalten Ereignisse. Hierbei handelt es sich um Aktionen, die von CA Identity Manager zum Abschließen von Aufgaben ausgeführt werden. Eine Aufgabe kann mehrere Ereignisse umfassen. So kann beispielsweise die Aufgabe "Benutzer erstellen" Ereignisse für das Erstellen des Benutzerprofils, das Hinzufügen des Benutzers zu einer Gruppe und das Zuweisen von Rollen beinhalten.

Wenn CA Identity Manager eine Aufgabe verarbeitet, verarbeitet es jedes der Aufgabe zugeordnete Ereignis. Während der Ereignisverarbeitung speichert CA Identity Manager jedes Ereignis vier Mal. Dies erlaubt CA Identity Manager, prozessinterne Aktionen im Fall eines unerwarteten Herunterfahrens des Systems zu erhalten.

Wenn CA Identity Manager gleichzeitig mehrere Ereignisse verarbeitet, werden die Ereignisse einer Warteschlange hinzugefügt. Wenn das erste Ereignis die erste Phase seines Lebenszyklus abgeschlossen hat, wird es gespeichert und dann zurück zum Ende der Warteschlange verschoben, um auf den Start der zweiten Phase zu warten. CA Identity Manager stellt dann die erste Verarbeitungsphase für das nächste in der Warteschlange befindliche Ereignis fertig und verschiebt es dann wieder an das Ende der Warteschlange. Der Prozess wird fortgesetzt, bis für alle Ereignisse in der Warteschlange die erste Verarbeitungsphase abgeschlossen ist. Dann fängt für das erste Ereignis in der Warteschlange die zweite Verarbeitungsphase an. Dies wird fortgesetzt, bis alle Ereignisse in der Warteschlange alle vier Verarbeitungsphasen durchlaufen haben.

Unter normalen Lastbedingungen wirkt sich dieses Verhalten nicht auf die Leistung aus. Wenn das System allerdings eine Vielzahl von Aufgaben und Ereignissen verarbeitet, wie z. B. während der Massendatenladung einer großen Benutzermenge, muss jedes Ereignis und jede Aufgabe länger in der Warteschlange verbleiben und hat daher eine längere Abschlusszeit.

Um Probleme mit der Leistung unter Belastungszuständen zu verhindern, berücksichtigen Sie die folgenden Aktionen:

- Nutzen Sie auf der Registerkarte "Profil" der Aufgabe die Einstellung "Aufgabenpriorität".

  Die Einstellung "Aufgabenpriorität" ermöglicht es Ihnen, die Priorität einer Aufgabe auf "Hoch", "Mittel" oder "Niedrig" festzulegen.

  Die Priorität von Aufgaben, die sofort verarbeitet werden müssen, sollte auf "Hoch" gesetzt werden. Aufgaben, die in eine Massendatenlast einbezogen sind, sollten auf "Niedrig" gesetzt werden.

Wenn eine Aufgabenpriorität festgelegt wird, werden die der Aufgabe zugeordneten Ereignisse mit anderen Aufgaben verarbeitet, die die gleiche Priorität haben. Wenn zum Beispiel die Priorität der Aufgabe "Benutzer ändern" auf "Hoch" gesetzt wurde, und ein Administrator ändert ein Benutzerprofil, dann verarbeitet CA Identity Manager diese Aufgabe vor Aufgaben, deren Priorität "Mittel" oder "Niedrig" ist. Wenn es weitere Aufgaben mit der Priorität "Hoch" gibt, führt CA Identity Manager die erste Verarbeitungsphase für das erste Ereignis mit hoher Priorität aus und verschiebt dieses Ereignis dann an das Ende der Liste mit den Ereignissen hoher Priorität.

- Installieren eines separaten, dedizierten CA Identity Manager-Servers zur Verarbeitung von Vorgängen mit Massendatenlasten

Richtlinien für die Optimierung von Aufgaben

Die Standardaufgaben, die CA Identity Manager bei der Erstellung einer CA Identity Manager-Umgebung bereitstellt, werden so konfiguriert, dass sie eine breite Palette an Verwaltungsanwendungsfällen unterstützen. Die meisten CA Identity Manager-Implementierungen benötigen nicht alles von der in den Standardaufgaben bereitgestellten Funktionalität. Nachdem Sie eine CA Identity Manager-Umgebung erstellt haben, ändern Sie diese Aufgaben, um sie spezifischen Administrationsanforderungen anzupassen.

Die folgenden Schritte stellen Richtlinien für das Ändern von Aufgaben dar:

- **Erstellen von spezialisierten Benutzerverwaltungsaufgaben**

  Der Standardaufgaben "Benutzer erstellen", "Benutzer ändern" und "Benutzer anzeigen" stellen die volle administrative Funktionalität bereit. In den meisten Implementierungen benötigt nur eine kleine Anzahl von Administratoren alle verfügbaren Funktionen.

  Erstellen Sie neue Aufgaben, die nur die erforderlichen Funktionen enthalten. Beispiel: Wenn die meisten Benutzerverwaltungsaufgaben nur die Profil- und Gruppenverwaltung betreffen, erstellen Sie eine neue Aufgabe "Benutzer ändern", die nur die Registerkarten "Profil" und "Gruppe" enthält. Entfernen Sie die Registerkarten "Admin-Rollen", "Zugriffsrollen" und "Bereitstellungsrollen", die in der Standardaufgabe von "Benutzer ändern" verfügbar sind.

  Nicht verwendete Registerkarten können bedeutenden Overhead verursachen, wenn sie in häufig eingesetzten Aufgaben belassen werden. Dies ist insbesondere der Fall, wenn ein TEWS-Client (Client für Webservice zur externen Ansteuerung von Aufgaben) verwendet wird, bei dem diese Registerkarten versehentlich durch die Registerkarte "Java-Klasse" aktiviert werden können, die mit CA Identity Manager bereitgestellt wird.

  Die spezialisierten Aufgaben, die Sie erstellen, sollten zu dem Modell für delegierte Verwaltung (siehe Seite 64) passen, das Sie für Ihre Umgebung definiert haben.

- **Deaktivieren von "Administratoren verwalten" auf Beziehungsregisterkarten**

  Standardmäßig bieten alle Beziehungsregisterkarten die Möglichkeit, administrative Rechte für das Objekt zu verwalten, das die Registerkarte verwaltet, wie Rollen und Gruppen. In den meisten Implementierungen muss Administratoren diese Funktionalität nicht bereitgestellt werden.

  Um den zusätzlichen Overhead zu beseitigen, der auftritt, wenn CA Identity Manager administrative Rechte auswertet, können Sie ggf. die Option "Administratoren verwalten" auf folgenden Registerkarten deaktivieren:

  - Admin-Rollen
  - Bereitstellungsrollen
  - Zugriffsrollen
  - Gruppen

  Um Benutzern zu ermöglichen, administrative Rechte auf bestimmten Registerkarten zu verwalten, können Sie Kopien der Standardregisterkarten erstellen, die Option "Administratoren verwalten" aktivieren und die Option "Mitglieder verwalten" deaktivieren. Fügen Sie die neuen Registerkarten spezialisierten Aufgaben hinzu, die nur von den Administratoren verwendet werden, die sie benötigen.

- **Aktivieren von bereichsbezogenen Suchen auf Rollenbeziehungs-Registerkarten**

  Sie können jede Rollenregisterkarte so konfigurieren, dass Suchen enthalten sind, bei denen Administratoren Kriterien angeben, nach denen einem Benutzer neue Rollen zugewiesen werden. Rollensuchen beschränken die Anzahl von Mitglieds- und Admin-Richtlinienregeln, die CA Identity Manager bewerten muss, um zu entscheiden, welche Rollen ein Administrator einem Benutzer zuweisen kann.

- **Einstellen von Aufgabensynchronisierungsoptionen**

  Für jede CA Identity Manager-Aufgabe können Sie eine Benutzer-Synchronisierungsoption angeben, die Benutzer mit Identitätsrichtlinien synchronisiert, und eine Bereitstellungskonto-Synchronisierungsoption, die Benutzer mit bereitgestellten Konten synchronisiert. Die Optionen ermöglichen Ihnen, Benutzer nach Abschluss einer Aufgabe oder eines Ereignisses zu synchronisieren.

  Um Auswertungs- und Verarbeitungszeit zu vermeiden, legen Sie die Synchronisierung so fest, dass sie stattfindet, wenn eine Aufgabe und nicht wenn Ereignisse abgeschlossen werden.

Richtlinien für die Optimierung von Gruppenmitgliedern/Administratoren

Um die Suchleistung nach Gruppenmitgliedern und Administratoren zu verbessern, berücksichtigen Sie Folgendes:

- Definieren Sie bekannte Attribute in der Verzeichniskonfigurationsdatei (directory.xml), mit denen in CA Identity Manager die Benutzerspeicherstruktur und die Inhalte beschrieben werden.

  Ein bekanntes Attribut ist ein Attribut, das eine Sonderbedeutung in CA Identity Manager hat.

  Um Gruppenmitglieder\Administrator-Suchen zu verbessern, definieren Sie die folgenden bekannten Attribute für das Benutzerobjekt:

  %MEMBER_OF%

  Identifiziert ein Attribut des Benutzerobjekts, das eine Liste von Gruppen speichert, in denen Benutzer Mitglied ist.

  Wenn definiert, kann dieses Attribut CA Identity Manager davon abhalten, alle Mitglieder aller Gruppen im Benutzerspeicher zu durchsuchen. Gruppensuchen können sich bei sehr großen Gruppen merklich auf die Leistung auswirken.

  %ADMINISTRATOR_OF%

  Identifiziert ein Attribut des Benutzerobjekts, das eine Liste von Gruppen speichert, bei denen der Benutzer ein Administrator ist.

  Wie das %MEMBER_OF%-Attribut können mit diesem bekannten Attribut lange Gruppensuchen vermieden werden.

- Angeben des Gruppentyps in der Verzeichniskonfigurationsdatei

  CA Identity Manager unterstützt drei Typen von Gruppen: Standardgruppen, verschachtelte Gruppen und dynamische Gruppen.

  Wenn Sie das Gruppenobjekt in der Verzeichniskonfigurationsdatei definieren, können Sie den Gruppentyp angeben, den der Benutzerspeicher unterstützt. Wenn Ihre Implementierung keine verschachtelten oder dynamischen Gruppen unterstützt, legen Sie das Gruppentypattribut folgendermaßen fest:

  GroupType = NONE

  Die Einstellung NONE gibt die Unterstützung für Standardgruppen an.

  Die Standardeinstellung für den Gruppentyp ist ALL, die sich aber auf die Leistung auswirken kann.

  Hinweis: Weitere Informationen zu bekannten Attributen und Gruppentypen in der Verzeichniskonfigurationsdatei finden Sie im *Konfigurationshandbuch*.

- Festlegen der Zwischenspeicherindizes des Bereitstellungsverzeichnisses zur Verbesserung der GlobalGroup-Leistung

  Bei CA Identity Manager-Implementierungen, die über eine Kombination aus Benutzerspeicher und Bereitstellungsverzeichnis verfügen, kann die GlobalGroup-Mitgliedschaft für die Auswertung der Richtlinienregel von Rollen und der Identitätsrichtlinien optimiert werden.

  Um diese Optimierung zu aktivieren, indizieren Sie die folgenden Attribute, die der Bereitstellungsserver verwendet, um die Gruppenmitgliedschaft im Zwischenspeicher des Bereitstellungsverzeichnisses aufzulösen:

  eTID

  Eindeutiges Objekt-ID-Attribut. Für Gruppenmitgliedschaftssuchen ist der Wert ein bestimmter Benutzer oder eine an der Suche beteiligte Gruppe.

  eTPID

  Übergeordnete ID des Objekts, die für die Suche nach Mitgliedschaftsbeziehungen verwendet wird.

  eTCID

  Untergeordnete ID des Objekts, die für die Suche nach Mitgliedschaftsbeziehungen verwendet wird.

  Fügen Sie zusätzlich die folgenden Hash-Eingaben hinzu:

  eTSuperiorClass

  Typ des übergeordneten Objekts in einer Mitgliedschaftssuche

  eTSubordinateClass

  Typ des untergeordneten Objekts in einer Mitgliedschaftssuche

  Hinweis: Weitere Informationen zum Zwischenspeicher für das Bereitstellungsverzeichnis finden Sie im *Installationshandbuch*.

Optimierung der Identitätsrichtlinien

Eine *Identitätsrichtlinie* bezeichnet einen Satz von Geschäftsänderungen, die eintreten, wenn ein Benutzer eine bestimmte Bedingung oder Regel erfüllt. Zu diesen Änderungen zählen das Zuweisen oder Widerrufen von Rollen, das Zuweisen oder Widerrufen von Gruppenmitgliedschaften sowie das Aktualisieren von Attributen eines Benutzerprofils.

CA Identity Manager wertet Identitätsrichtlinien aus, wenn die Benutzersynchronisierung stattfindet.

Die Identitätsrichtlinienleistung wird von folgenden Aspekten beeinflusst:

- Konfiguration der Identitätsrichtlinien
- Häufigkeit der Benutzersynchronisierung

Synchronisieren von Benutzern und Identitätsrichtlinien

Beim Verwenden von Identitätsrichtlinien sollten Sie damit vertraut sein, wie CA Identity Manager die Richtlinien auswertet und für Benutzer anwendet. Ohne genaue Kenntnisse der Benutzersynchronisierung konfigurieren Sie möglicherweise Identitätsrichtliniensätze, die zu unerwarteten Ergebnissen führen.

Das folgende Verfahren erläutert, wie CA Identity Manager Identitätsrichtlinien auswertet und sie anwendet:

1. Der Benutzersynchronisierungsdurchlauf beginnt:
   - **Automatisch**: Sie können Aufgaben von CA Identity Manager so konfigurieren, dass sie die Benutzersynchronisierung automatisch auslösen
   - **Manuell**: Mit Hilfe der Aufgabe "Benutzer synchronisieren" in der Benutzerkonsole können Sie einen Benutzer synchronisieren.
2. CA Identity Manager ermittelt die Identitätsrichtlinien, die für einen Benutzer gelten.
3. CA Identity Manager vergleicht die Identitätsrichtlinien, die für einen Benutzer gelten, mit der Liste der Richtlinien, die bereits für diesen Benutzer übernommen wurden.

   Hinweis: Die Liste der Richtlinien, die bereits für einen Benutzer übernommen wurden, sind im bekannten Attribut %IDENTITY_POLICY% im Benutzerprofil gespeichert. Informationen über das Konfigurieren dieses Attributs finden Sie im *Konfigurationshandbuch*.

   - Falls eine Identitätsrichtlinie in der Liste der anwendbaren Richtlinien aufgeführt wird *und* diese Richtlinie zuvor *nicht* für den Benutzer übernommen wurde, fügt CA Identity Manager sie zu einer Zuweisungsliste hinzu.
   - Falls eine Identitätsrichtlinie in der Liste der anwendbaren Richtlinien aufgeführt wird, diese Richtlinie bereits für den Benutzer übernommen wurde und die Einstellung "Einmal übernehmen" deaktiviert ist, fügt CA Identity Manager sie zur Liste der Richtlinien, die erneut zugewiesen werden, hinzu.
   - Wenn eine Identitätsrichtlinie nicht in der Liste der anwendbaren Richtlinien enthalten ist und die Richtlinie für den Benutzer übernommen wurde, stimmt der Benutzer nicht mehr mit der Richtlinienbedingung überein. CA Identity Manager fügt diese Richtlinien zu einer Liste der Richtlinien, deren Zuweisung aufgehoben wird, hinzu.

4. Nachdem CA Identity Manager alle Richtlinien eines Benutzers ausgewertet hat, werden diese in der folgenden Reihenfolge übernommen:

   a. Identitätsrichtlinien aus der Liste der Richtlinien, deren Zuweisung aufgehoben wird

   b. Identitätsrichtlinien aus der Liste der Richtlinien, die zugewiesen werden

   c. Identitätsrichtlinien aus der Liste der Richtlinien, die neu zugewiesen werden

5. Nachdem die Identitätsrichtlinien übernommen wurden, wertet CA Identity Manager die Richtlinien erneut aus, um festzustellen, ob infolge der Änderungen, die während des ersten Synchronisierungsdurchlaufs (Schritte 2-4) vorgenommen wurden, weitere Änderungen erforderlich sind.

   Dadurch soll sichergestellt werden, dass die durch die Anwendung von Identitätsrichtlinien vorgenommenen Änderungen nicht andere Identitätsrichtlinien auslösen.

6. CA Identity Manager wertet weiterhin Identitätsrichtlinien aus und übernimmt sie, bis der Benutzer mit allen anwendbaren Richtlinien synchronisiert ist oder bis CA Identity Manager die höchste Rekursionsebene erreicht, die in der Management-Konsole definiert ist.

   Zum Beispiel ändert eine Identitätsrichtlinie möglicherweise die Abteilung eines Benutzers, wenn diesem eine Rolle zugewiesen wird. Die neue Abteilung löst eine andere Identitätsrichtlinie aus. Falls die Rekursionsebene jedoch auf 1 eingestellt ist, wird die nächste Änderung erst durchgeführt, nachdem der Benutzer wieder synchronisiert wurde.

   Weitere Informationen über das Einstellen der Rekursionsebene finden Sie in der Online-Hilfe zur Management-Konsole.

Entwerfen von effizienten Identitätsrichtlinien

Verwenden Sie die folgenden Richtlinien, wenn Sie Identitätsrichtlinien erstellen:

- **Beschränken der Anzahl von Richtlinienobjekten**

  CA Identity Manager erstellt Objekte im Objektspeicher, die Identitätsrichtlinien unterstützen. Um die Anzahl von Objekten im Objektspeicher zu reduzieren, erstellen Sie Identitätsrichtlinien mit komplexen Ausdrücken.
  Eine ähnliche Vorgehensweise wird für Rollenrichtlinien (siehe Seite 74) empfohlen.

- **Beschränken der Iterationen von Identitätsrichtliniensätzen**

  Sie können die Rekursionsebene für eine Identitätsrichtlinie konfigurieren. Diese gibt an, wie viele Male CA Identity Manager bei der Benutzersynchronisierung Identitätsrichtlinien auswertet und anwendet, bestimmt. Zum Beispiel ändert eine Identitätsrichtlinie möglicherweise die Abteilung eines Benutzers, wenn diesem eine Rolle zugewiesen wird. Die neue Abteilung löst eine andere Identitätsrichtlinie aus. Falls die Rekursionsebene jedoch auf 1 eingestellt ist, wird die nächste Änderung erst durchgeführt, nachdem der Benutzer wieder synchronisiert wurde.

  Mit dem Festlegen der Rekursionsebene wird eingeschränkt, wie viele Male CA Identity Manager Identitätsrichtlinien auswerten muss.

- **Beschränken der Abhängigkeiten zwischen Identitätsrichtlinienregeln**

  Sie können eine Identitätsrichtlinie erstellen, bei der die Änderungsaktion (Aktion zu "Richtlinie anwenden" oder Aktion zu "Richtlinie entfernen") einer Richtlinie in der Identitätsrichtlinienbedingung einer anderen Richtlinie wie folgt verwendet wird.

Identitätsrichtlinienbedingung	Aktion zu "Richtlinie anwenden"	Aktion zu "Richtlinie entfernen"
where (Jobcode = "100")	Zum Mitglied von (Bereitstellungsrolle "Account Manager") machen	Mitglied von (Bereitstellungsrolle "Account Manager") entfernen
Als Mitglieder von (Bereitstellungsrolle "Account Manager")	Zum Mitglied von (Gruppe "Account Manager") machen	Mitglied von (Gruppe "Account Manager") entfernen

Wenn CA Identity Manager diesen Richtlinientyp auswertet, müssen die Änderungen mindestens zweimal ausgewertet und angewendet werden um sicherzustellen, dass beiden Bedingungen entsprochen wird. Die Rekursionsebene, die für eine ganze CA Identity Manager-Umgebung festgelegt wird, muss größer sein als 1. Dies führt zu weiteren Auswertungen für jeden Identitätsrichtliniensatz.

Beschränken der Aufgaben, die eine Benutzersynchronisierung auslösen

Identitätsrichtlinien werden während des Benutzersynchronisierungsprozesses ausgewertet und angewandt. Sie können die automatische Synchronisierung durch das Angeben einer der folgenden Benutzersynchronisierungsoptionen für eine Aufgabe konfigurieren:

Bei Abschluss der Aufgabe

CA Identity Manager startet den Benutzersynchronisierungsdurchlauf nach Abschluss aller Ereignisse.

Bei jedem Ereignis

CA Identity Manager startet den Prozess der Benutzersynchronisierung, wenn jedes Ereignis in einer Aufgabe abgeschlossen ist.

Beschränken Sie für eine optimale Leistung die Anzahl der Aufgaben, die eine automatische Benutzersynchronisierung auslösen.

Berücksichtigen Sie beim Konfigurieren der Benutzersynchronisierung Folgendes:

- **Deaktivieren der Benutzersynchronisierung für Kennwortaufgaben**

  In den meisten Fällen werden Kennwörter nicht in Identitätsrichtlinienbedingungen verwendet.

- **Deaktivieren der Benutzersynchronisierung für die Aufgabe "Benutzer synchronisieren"**

  Da die Aufgabe "Benutzer synchronisieren" Identitätsrichtlinienauswertungen auslöst, führt CA Identity Manager die Auswertungen erneut aus, wenn die Benutzersynchronisierungsoption für diese Aufgabe aktiviert wird.

- **Erstellen von spezialisierten Aufgaben**

  Erstellen Sie, wenn möglich, Aufgaben, die Änderungen ausführen, durch die Identitätsrichtlinienbedingungen ausgelöset werden, und aktivieren Sie dann die Benutzersynchronisierung nur für diese Aufgaben.

Optimieren der Auswertung der Identitätsrichtlinienregel

Sie können die Auswertungszeit für Identitätsrichtlinienbedingungen verkürzen, die Benutzerattribute enthalten, indem Sie die Option für die Auswertung im Arbeitsspeicher aktivieren. Wenn die Option für die Auswertung im Arbeitsspeicher aktiviert ist, ruft CA Identity Manager Informationen über einen zu bewertenden Benutzer aus dem Benutzerspeicher ab und speichert eine Repräsentation dieses Benutzers im Arbeitsspeicher. CA Identity Manager verwendet die Repräsentation im Arbeitsspeicher, um die Attributwerte in Bezug auf die Richtlinienbedingungen zu vergleichen. Dadurch wird die Anzahl der Aufrufe beschränkt, die CA Identity Manager direkt im Benutzerspeicher durchführt.

Hinweis: Weitere Informationen zur Option für die Auswertung im Arbeitsspeicher finden Sie im *Konfigurationshandbuch*.

Optimieren des Benutzerspeichers

Die Optimierung des Benutzerspeichers betrifft eine Anzahl von Schritten, einschließlich der Folgenden:

- Optimieren der Struktur des Benutzerspeichers
- Abstimmen der zugrunde liegenden Speicher
- Implementieren von Lastenausgleich und Replikation

Diese Schritte hängen vom Typ von Benutzerspeicher ab, den Sie verwenden. Weitere Informationen zur Optimierung in diesen Bereichen finden Sie in der Dokumentation zu der Datenbank oder dem Verzeichnis, das den Benutzerspeicher enthält.

Zusätzlich zu den allgemeinen Optimierungsaspekten gelten die folgenden Optimierungsüberlegungen speziell für CA Identity Manager:

- **Messen der Suchleistung im Benutzerspeicher**

  Für eine optimale Leistung sollten CA Identity Manager-Richtlinienauswertungssuchen innerhalb von 10 bis 20 Millisekunden abgeschlossen sein.

  Um sicherzustellen, dass CA Identity Manager konsistent diese Suchen in der empfohlenen Zeit abschließen kann, sollte die Suchleistung unter verschiedenen Belastungszuständen getestet werden.

  Sie können diese Messung auch verwenden, um zu entscheiden, wann ein Benutzerspeicher seine physischen Limits erreicht und zusätzliche Server für den Lastenausgleich erforderlich sind.

- **Index-Attribute**

  Indizieren Sie jedes Attribut, das in einer Rollen- oder Identitätsrichtlinie verwendet wird. Das Indexieren von Attribute kann zu bedeutenden Leistungsverbesserungen führen.

  Hinweis: Weitere Informationen zum Indexieren von Attributen finden Sie in der Dokumentation zu dem LDAP-Verzeichnis oder der relationalen Datenbank, wo sich der Benutzerspeicher befindet.

- **Zwischenspeichern von LDAP-Binds**

  In CA Identity Manager werden alle Verzeichnis-LDAP-Binds von dem Proxy-Benutzer ausgeführt, der im CA Identity Manager-Verzeichnisobjekt definiert ist. Bei jeder Verbindung werden immer die gleichen LDAP-Binds für diesen Benutzer verwendet.

  Wenn Sie ein LDAP-Verzeichnis als Benutzerspeicher verwenden, konfigurieren Sie das Verzeichnis so, dass LDAP-Binds (oder Sitzungen) zwischengespeichert werden, wenn dies vom Verzeichnis unterstützt wird.

- **Aktivieren von Zwischenspeichern für Benutzerspeicher**

  Wenn CA Identity Manager die Richtlinienentscheidungen für einen Benutzer auswertet, werden diese Informationen in einem Autorisierungszwischenspeicher abgelegt. Wenn die Zwischenspeichung der Informationen abläuft, wertet CA Identity Manager erneut alle Richtlinien für diesen Benutzer aus.

  Um die Leistung von Benutzerspeichersuchen in nachfolgenden Richtlinienregelauswertungen zu verbessern, erlauben Sie dem Benutzerspeicher eine Zwischenspeicherung der gesuchten Daten, wenn dies vom Benutzerspeicher unterstützt wird.

  CA Directory enthält einen Zwischenspeicher, dxCache genannt, bei dem es sich um eine Datenbankimplementierung im Arbeitsspeicher handelt, die eine gleichzeitige Suche in allen Zwischenspeichern erlaubt.

  Hinweis: Weitere Informationen zu CA Directory finden Sie im *CA Directory-Administrator-Handbuch*.

Optimieren von Bereitstellungskomponenten

Wenn eine CA Identity Manager-Implementierung die Bereitstellung mit einschließt, verwenden Sie die folgenden Optimierungen, um die beste Leistung zu erzielen:

- Optimieren der Verbindung zwischen CA Identity Manager-Server und Bereitstellungsserver

  Die Kommunikation zwischen CA Identity Manager und dem Bereitstellungsserver erfolgt mithilfe der Java IAM (JIAM) API. Um die Kommunikationsleistung zu verbessern, konfigurieren Sie Folgendes:

  - JIAM-Sitzungspool für mehrere Verbindungen zum Bereitstellungsserver

    Hinweis: CA empfiehlt, den Anfangssitzungswert auf 8 und die größtmöglichen Sitzungen auf 128 einzustellen.

  - JIAM-Zwischenspeicher für aus dem Bereitstellungsserver abgerufene Objekte

  Hinweis: Weitere Informationen zu den JIAM-Konfigurationseinstellungen finden Sie im *Administrationshandbuch*.

- Einstellen der Kontosynchronisierung auf das Ende einer Aufgabe (siehe Seite 82) und nicht auf das Ende jedes Ereignisses
- Optimieren des Bereitstellungsservers

  Hinweis: Weitere Informationen dazu finden Sie im *Administrationshandbuch* und im *Installationshandbuch*.

Optimieren der Laufzeitkomponenten

Geschäftsänderungen werden in CA Identity Manager über Aufgaben durchgeführt. Eine Aufgabe enthält ein oder mehrere Ereignisse, die für Aktivitäten stehen, die CA Identity Manager ausführt, um die Aufgabe zu vervollständigen. Zum Beispiel kann die Aufgabe "Benutzer erstellen" die Ereignisse CreateUserEvent und AddToGroupEvent enthalten.

CA Identity Manager enthält die folgenden Komponenten, die zur Laufzeit Aufgaben und Ereignisse verarbeiten:

- CA Identity Manager-Datenbanken, die CA Identity Manager-Funktionalität unterstützen
- JMS-Meldungen, die für die Verarbeitung von Ereignissen verantwortlich sind

Optimieren von CA Identity Manager-Datenbanken

Bei der Ausführung einer Aufgabe verwendet CA Identity Manager die folgenden Datenbanken:

- Aufgabenpersistenz

  Verwaltet Informationen zu CA Identity Manager-Aufgaben und -Ereignissen über die Zeit. Dies erlaubt CA Identity Manager, bei Systemfehlern den letzten bekannten Status von Ereignissen und Aufgaben wiederherzustellen.

  Hinweis: Diese Datenbank hat die größten Auswirkungen auf die CA Identity Manager-Leistung, da die Aufgabe und deren Ereignisse in der Datenbank gespeichert und von dort bei Zustandsübergängen abgerufen werden.

- Audit

  Stellt einen Verlaufsdatensatz von Vorgängen zur Verfügung, die in einer CA Identity Manager-Umgebung stattfinden.

- Workflow

  Speichert Workflow-Prozessdefinitionen, Jobs, Skripte und andere Daten, die von der Workflow-Engine benötigt werden.

- Berichterstellung

  Speichert Snapshot-Daten, die den aktuellen Zustand von Objekten in CA Identity Manager zum Zeitpunkt des Snapshots widerspiegeln.

CA Identity Manager kommuniziert mit jeder Datenbank über einen JDBC-Verbindungspool. Sie erstellen und konfigurieren einen JDBC-Verbindungspool in dem Anwendungsserver, der CA Identity Manager hostet. Wenn Sie den JDBC-Verbindungspool konfigurieren, müssen Sie Folgendes beachten:

- Die Anzahl von Aufgaben, die gleichzeitig ausgeführt werden können.
- Weitere Laufzeitkomponenten, wenn Sie die JDBC-Verbindungspoolgröße konfigurieren. Jede Laufzeitkomponente funktioniert zusammen mit den anderen Laufzeitkomponenten.

  Hinweis: CA empfiehlt, den Anfangswert für den Verbindungspool auf 128 festzulegen.

- Für die Aufgabenpersistenz-Datenbank muss die Anzahl von Datenbankverbindungen im Pool jeder der ausführenden Aufgaben die Möglichkeit geben, während der gesamten Ausführungszeit Aufgaben- und Ereignisdaten abzurufen und zu aktualisieren.

- Die Aufgabenpersistenz-Datenbank verwendet vorbereitete Anweisungen. Stellen Sie sicher, dass der Zwischenspeicher für vorbereitete Anweisungen für die Datenbank konfiguriert wird, die Sie zum Speichern der Aufgabenpersistenzdaten verwenden.

  Hinweis: Weitere Informationen zum Konfigurieren des Zwischenspeichers für vorbereitete Anweisungen finden Sie in der Dokumentation zu der Datenbank, die Sie für die Aufgabenpersistenz verwenden.

JMS-Einstellungen

Eine CA Identity Manager-Aufgabe enthält Ereignisse. Das sind Aktionen, die CA Identity Manager ausführt, um eine Aufgabe abzuschließen.

Während des Lebenszyklus eines Ereignisses, durchläuft das Ereignis folgende Zustände:

- BEGIN
- APPROVED
- EXECUTING
- COMPLETED
- INVALID

Workflow-gesteuerte Ereignisse können auch folgende Zustände aufweisen:

- PENDING
- REJECTED

CA Identity Manager verwendet JMS-Meldungen, um diese Zustandsübergänge zu steuern.

Steuern von JMS Message Drive Event-Zustandsübergängen

CA Identity Manager verwendet JMS-Meldungen, um die Zustandsübergänge eines Ereignisses zu steuern. Das folgende Verfahren beschreibt die erforderlichen Schritte:

1. Ein Benutzer sendet eine Aufgabe.
2. Die Aufgabe generiert ein oder mehrere Ereignisse.
3. Wenn ein Ereignis zur Ausführung bereit ist, ändert CA Identity Manager den Status des Ereignisses in BEGIN, und das Ereignis verbleibt in der Aufgabenpersistenz-Datenbank.
4. CA Identity Manager erstellt eine JMS-Meldung, die die Ereignis-ID enthält, und sendet diese Meldung an die Events Message Queue.
5. Bei Erhalt der Meldung startet JMS dann eine Instanz der Event Message Driven Bean, die eine Implementierung des Ereignis-Controllers ist.

6. Der Ereignis-Controller verwendet die Ereignis-ID aus der Meldung, um das Ereignis aus der Aufgabenpersistenz-Datenbank abzurufen, und führt dann die Aktionen für den aktuellen Zustand des Ereignisses aus.
7. Nach Abschluss dieses Zustands wird für das Ereignis der nächste Zustand festgelegt, der in der Aufgabenpersistenz-Datenbank verbleibt, und eine neue JMS-Meldung wird für das Bearbeiten des nächsten Zustands gesendet.

   Dieser Zyklus dauert fort, bis der Zustandsautomat des Ereignisses beendet ist.

JMS-Meldungen und Leistung

Für jedes Ereignis gibt es drei bis fünf Zustände, die JMS-Meldungen für Zustandsübergange benötigen:

- BEGIN
- PENDING (nur bei Workflow-Steuerung)
- APPROVED oder REJECTED
- EXECUTING
- COMPLETED oder INVALID

Um ein einzelnes Ereignis zu bearbeiten, finden die folgenden Aktionen statt:

- Drei bis fünf Beiträge zur Events Message Queue
- Drei bis fünf Aufrufe der Message Driven Bean
- Sechs bis zehn Verbindungen zur Aufgabenpersistenz-Datenbank (eine Lese-Aktion und eine Schreib-Aktion pro Zustand)

Diese Aktionen können sich auf die Zeitdauer auswirken, die CA Identity Manager benötigt, um eine Aufgabe zu bearbeiten.

Um bei Zustandsübergängen beste Leistung zu sichern, müssen Sie die JMS-Ressourcen auf dem Anwendungsserver optimieren, der CA Identity Manager hostet, sodass angemessene JMS-Ressourcen verfügbar sind.

Optimieren von JMS-Einstellungen

Die folgenden JMS-Optimierungsparameter für Anwendungsserver definieren Warteschlangenverbindungen (Queue Connections) und Message Driven Bean-Instanzenpools.

- **Optimieren von WebSphere JMS**

  WebSphere stellt für Queue Connection Factories zwei Parameter bereit, die Sie konfigurieren können, um die Leistung zu verbessern. Verwenden Sie die WebSphere-Management-Konsole, um die folgenden Eigenschaften festzulegen:

  - Unter "Resources" finden Sie die folgenden Queue Connection Factories: "iam-im-neteQCF" und "iam-im-wpConnectionFactory".
  - Bearbeiten Sie für beide die Verbindungspooleigenschaften, indem Sie den Wert für die maximalen Verbindungen auf 128 festlegen.

- **Optimieren von WebLogic**

  In WebLogic-Anwendungsservern erhalten Queue Connection Factories je nach JMS Thread Pool-Größe vom JMS Thread Pool des Servers oder dem Standardausführungspool Threads zur Handhabung von Verbindungen. Wenn die JMS Thread Pool-Größe 0 ist, verwendet WebLogic die Threads im Ausführungspool.

  Wir empfehlen, dass Sie die Anzahl der JMS Thread Pool-Threads auf die maximale Bean Pool-Größe für die CA Identity Manager Event Message Driven Bean einstellen, die standardmäßig 128 beträgt.

  Sie verwenden die WebLogic-Serverkonsole, um die JMS Thread Pool-Größe in den JMS Services-Eigenschaften für die Domäne und den Server festzulegen, auf dem CA Identity Manager installiert ist.

  Die CA Identity Manager Event Message Driven Bean-Poolgröße wird durch das Ändern der Einstellung "max-beans-in-free-pool" in der Deskriptordatei an folgendem Speicherort festgelegt:

  WebLogic_home\domain\applications\iam_im.ear\identityminder_ejb.jar\META-INF\weblogic-ejb-jar.xml

```
<weblogic-enterprise-bean>
        <ejb-name>SubscriberMessageEJB</ejb-name>
        <message-driven-descriptor>
            <pool>
                <max-beans-in-free-pool>128</max-beans-in-free-pool>
                <initial-beans-in-free-pool>16</initial-beans-in-free-pool>
            </pool>
            <destination-jndi-name>com.netegrity.ims.msg.queue</destination-
jndi-name>
        </message-driven-descriptor>
    </weblogic-enterprise-bean>
```

- **Optimieren von JBoss**

  Über JBoss-Anwendungsservern erhalten Queue Connection Factories Verbindungs-Threads von der Standard JMS Pool-Session-Factory des Servers. Standardmäßig wird die maximale Anzahl von Threads auf 15 festgelegt.

  Wir empfehlen, diesen Wert einzustellen, um mit dem Wert für die maximale Größe des Standard Message Bean Container übereinzustimmen.

  Die JMS Session Pool-Section-Factory wird über das MaximumSize-Element des JMSContainerInvoker in der folgenden Datei festgelegt:

  jboss_home\server\default\conf\standardjboss.xml

```
<invoker-proxy-binding>
         <name>message-driven-bean</name>
         ….
         <proxy-factory-config>

<JMSProviderAdapterJNDI>DefaultJMSProvider</JMSProviderAdapterJNDI>

<ServerSessionPoolFactoryJNDI>StdJMSPool</ServerSessionPoolFactoryJNDI>
            <MaximumSize>128</MaximumSize>
            <MaxMessages>1</MaxMessages>
            ….
         </proxy-factory-config>
     </invoker-proxy-binding>
```

  Die Poolgröße für eine CA Identity Manager Event Message Driven Bean wird durch das Ändern des Wertes für die maximale Größe in der folgenden Deskriptordatei festgelegt:

  jboss_home\server\default\conf\standardjboss.xml

```
<container-configuration>
         <container-name>Standard Message Driven Bean</container-name>
         <call-logging>false</call-logging>
         <invoker-proxy-binding-name>message-driven-bean</invoker-proxy-
binding-name>
        ……
         <container-pool-conf>
            <MaximumSize>128</MaximumSize>
         </container-pool-conf>
   </container-configuration>
```

Optimieren der JBoss 5-Leistung

In einer Standardinstallation von JBoss 5 wird der JBoss-Hot Deployment-Scanner alle 5 Sekunden ausgeführt, was sich auf die JBoss-Leistung auswirkt. Sie können diese Funktion deaktivieren, wenn sie nicht benötigt wird, oder ändern, wie häufig der Scanner ausgeführt werden soll.

Deaktivieren oder Ändern von Hot Deployment

1. Bearbeiten Sie die Datei "hdscanner-jboss-beans.xml" in diesem Speicherort:

   Einzelner Knoten: *jboss_home*/server/default/deploy

   Cluster: *jboss_home*/server/all/deploy

2. Um diese Funktion zu deaktivieren, fügen Sie die folgende Zeile im HDScanner-Bean hinzu:
   `<attribute name="ScanEnabled">False</attribute>`
3. Um die Scan-Häufigkeit zu ändern, vergrößern Sie den "scanPeriod"-Attributwert auf über 5000 (Millisekunden).

Hinweis: Weitere Details dazu finden Sie unter http://community.jboss.org/wiki/JBossASTuningSlimming.

Handhaben des Fehlers "Ungenügender Speicherplatz"

Die Ausnahme "Ungenügender Speicherplatz" wird möglicherweise angezeigt, wenn die Java-Heap-Größe zu klein ist. Wir empfehlen eine Anfangsgröße von 1024.

Kapitel 7: Erstellen eines Disaster-Recovery-Plans

Dieses Kapitel enthält folgende Themen:

Dienstausfall durch einen Notfall

Im Fall eines Systemausfalls können Benutzer den Zugriff auf Dienste verlieren, die für ihre Jobs kritisch sind. Dadurch können diese Benutzer keine Dienste für anderen Benutzer mehr bereitstellen.

Die Dringlichkeit, mit der der Zugriff auf Dienste wiederhergestellt werden soll, hängt von der eigentlichen Verwendung von CA Identity Manager ab. In einigen Organisationen benötigen Benutzer ununterbrochenen Zugriff auf Dienste, die von CA Identity Manager bereitgestellt werden, während andere Benutzer Systemwiederherstellung innerhalb eines Tages benötigen. In jedem Fall empfehlen wir, dass Sie Vorbereitungen treffen, um Ihre CA Identity Manager-Implementierung vor einem Ereignis zu schützen, das den teilweisen oder vollständigen Ausfall Ihrer Systeme verursacht.

Durch das Konfigurieren einer redundanten Architektur für CA Identity Manager können Sie Benutzern garantieren, dass Dienste hochverfügbar sind. Wenn eine primäre Komponente fehlschlägt, fährt die alternative Komponente fort, den gleichen Dienst bereitzustellen. Außerdem können Sie routinemäßig kritische Systeme und Software sichern, sodass Sie ein System oder Daten wiederherstellen können, die vollkommen verloren gehen.

Dieses Dokument gibt allgemeine Planungsrichtlinien für diese Szenarien an. Wir empfehlen, dass Sie diese Richtlinien verwenden, um bestimmte Disaster-Recovery-Vorgänge zu entwickeln, die den Anforderungen Ihrer Organisation entsprechen.

Planen für Disaster Recovery

Um einen wirksamen Disaster-Recovery-Plan zu entwickeln, setzen Sie die folgenden Phasen um, die in diesem Kapitel ausführlich behandelt werden.

✓	Phase
	1. Definieren der Disaster-Recovery-Anforderungen (siehe Seite 101) Analysieren Sie basierend auf Ihrem organisatorischen Bedarf, welche Arten von Notfällen auftreten können und wie schnell Sie die Dienste wiederherstellen müssen.
	2. Entwerfen einer redundanten Architektur (siehe Seite 102) Entwerfen Sie entsprechend Ihren Anforderungen eine Architektur mit redundanten Komponenten an einem Remote-Standort.
	3. Entwickeln von Sicherungsplänen (siehe Seite 104) Um Ihre Installation zu schützen, entwickeln Sie Pläne für das Sichern von Komponenten.
	4. Entwickeln von Wiederherstellungsverfahren (siehe Seite 105) Entwickeln Sie Verfahren, um verlorene Komponenten wiederherzustellen.
	5. Dokumentieren des Wiederherstellungsplans (siehe Seite 109) Dokumentieren Sie Ihre Pläne, damit Sie CA Identity Manager im Notfall wiederherstellen können.
	6. Testen des Wiederherstellungsplans (siehe Seite 109) Überprüfen Sie basierend auf Ihren Disaster-Recovery-Vorgängen, dass Sie Ihre CA Identity Manager-Implementierung wiederherstellen können, wie sie vor dem Notfall vorhanden war.
	7. Durchführen von Disaster-Recovery-Schulungen (siehe Seite 111) Stellen Sie abschließend sicher, dass die für die Wiederherstellung des Systems verantwortlichen Mitarbeiter dafür geschult sind

Definieren der Disaster-Recovery-Anforderungen

Das Folgende sind einige allgemeine Richtlinien, die für das Definieren von Anforderungen für einen Disaster-Recovery-Plan berücksichtigt werden sollten:

1. Stellen Sie ein Team mit den folgenden Kenntnissen zusammen:
   - Kenntnisse von der Architektur und den Systemen, die CA Identity Manager unterstützen
   - Kenntnisse darüber, wie man die von CA Identity Manager verwendeten relationalen Datenbanken und LDAP-Benutzerspeicher sichert
2. Identifizieren Sie potenzielle Notfallszenarien, einschließlich teilweisen oder vollständigen Verlust von Systemen an einem oder mehr Standorten.
3. Listen Sie die Systeme auf, deren Verfügbarkeit kritisch ist, um Ihre Installation zu unterstützen.
4. Definieren Sie die annehmbare größtmögliche Ausfallzeit für jedes dieser Systeme.

   Zum Beispiel können Systeme, die einen alternativen Server unterstützen, eine geringere Priorität für die Wiederherstellung haben.

Entwerfen einer redundanten Architektur

Um vor dem Ausfall einer kritischen Komponente zu schützen, erwägen Sie die folgenden Schutzaktionen mit alternativen Komponenten (Server und Verzeichnisse) und redundanten Datenbanken an Remote-Speicherorten.

Konfigurieren Sie Redundanz für CA Identity Manager mithilfe des *Installationshandbuchs* .Berücksichtigen Sie die folgenden Komponenten:

- Redundante CA Identity Manager-Anwendungsserverknoten als Teil eines Clusters
- Ein Richtlinienserver-Cluster sorgt für Failover (wenn Sie CA SiteMinder verwenden, um CA Identity Manager zu schützen)
- Alternative Bereitstellungsserver, Bereitstellungsverzeichnisse und Connector-Server. Wenn eine primäre Komponente ausfällt, schaltet das System auf die alternative Komponente um.

Konfigurieren Sie Redundanz für Datenbanken, einschließlich der Folgenden:

- Eine der Laufzeitdatenbanken, die Teil von CA Identity Manager sind, wie die Workflow- oder Audit-Datenbank.

  Weitere Informationen finden Sie in der Dokumentation zur ORACLE oder Microsoft SQL Server.
- Die BusinessObjects-Datenbank, wenn Sie den Berichtsserver verwenden.

  Rufen Sie die Dokumentation zu BusinessObjects Enterprise, Version 2 und Version 2 SP 4 über die SAP-Dokumentationswebseite ab.

Alternative CA Identity Manager-Server

Die Angabe von redundanten Anwendungsserverknoten für den CA Identity Manager-Server bietet Skalierbarkeits- und Leistungsvorteile sowie Disaster Recovery, wenn einzelne Server ausfallen. Die gebräuchlichste Methode, für Failover für einen Anwendungsserver zur sorgen, ist das Erstellen eines Clusters. Die Vorgänge für das Erstellen des Clusters werden im Cluster-Abschnitt des *Installationshandbuchs* abgedeckt.

Hinweis: Für CA Identity Manager r12.0 und höhere Versionen ist ein Anwendungsserver-Cluster die einzige gültige Methode, um eine Mehrfachknotenbereitstellung zu implementieren. CA Identity Manager-Umgebungen benötigen die Cluster-Architektur nach Industriestandard J2EE, welcher JMS-Warteschlangen als Backbone verwendet. Dadurch ist die einzige gültige Methode für die Verwendung von mehreren Knoten in einer CA Identity Manager-Konfiguration ein Anwendungsserver-Cluster.

Weitere Details zu dieser Änderung finden Sie in TechDoc 545594.

Alternative Bereitstellungskomponenten

Einige Bereitstellungskomponenten haben die Option einer alternativen Komponente, um Hochverfügbarkeit zu bieten. Die alternative Komponente sollte sich für den höchsten Schutz an einem Remote-Standort befinden.

Konfigurationsdetails zu alternativen Servern und Verzeichnissen finden Sie im Kapitel über Hochverfügbarkeitsbereitstellungen im *Installationshandbuch*.

Bereitstellungsverzeichnisse an mehreren Standorten

Sie können primäre und alternative Bereitstellungsverzeichnisse mit den alternativen Verzeichnissen an einem Remote-Speicherort erstellen. CA Directory empfiehlt, dass Sie drei Bereitstellungsverzeichnisse, ein primäres und zwei alternative Verzeichnisse, installieren.

Bereitstellungsserver an mehreren Standorten

Um vor Ausfall des primären Bereitstellungsservers zu schützen, können Sie einen alternativen Bereitstellungsserver konfigurieren. Der Unterschied zwischen primären und alternativen Bereitstellungsservern ist, dass die Primärserverinstallation die Bereitstellungsverzeichnis-Containereinträge ausfüllt. Wenn Sie den Primärserver deinstallieren, werden auch diese Einträge entfernt. Abgesehen von Installation und Deinstallation funktionieren primäre und alternative Server in der gleichen Weise.

Connector-Server an mehreren Standorten

Für den Java- oder C++-Connector-Server können Sie mehrere Connector-Server konfigurieren, um den gleichen Endpunkt oder Endpunkttyp zu bedienen.

Für jeden Connector-Server, den Sie konfigurieren, sollten Sie einen alternativen Connector-Server an einem Remote-Standort konfigurieren, der die gleichen Endpunkte verarbeitet. Wenn der Connector-Server fehlschlägt, übernimmt der alternative Server sofort die Kommunikation mit den Endpunkten.

Redundante Datenbanken

Die unterstützte Datenbanksoftware, Microsoft SQL Server und Oracle, bietet die Möglichkeit, redundante Datenbanken anzugeben. Wenn die Hauptdatenbank ausfällt, ist die redundante Datenbank sofort verfügbar. Die redundante Datenbank sollte sich an einem Remote-Standort befindet, falls der ganze Standort betroffen ist.

Entwickeln von Sicherungsplänen

Um vor dem Ausfall von einem oder allen Systemen zu schützen, verwenden Sie externe Standortspeicherung für alle Daten, die Sie sichern, sowie einen Sicherungszeitplan, der Ihren Anforderungen für die größtmögliche Ausfallzeit entspricht. Die Sicherungs- und Wiederherstellungsverfahren verwenden unterschiedliche Anwendungen, deshalb sollten sie für die Wiederherstellung des ganzen CA Identity Manager-Systems koordiniert werden.

Nehmen Sie die folgenden Komponenten in Ihre Sicherungspläne auf:

Komponente	Beschreibung	Sicherungsmethode
CA Identity Manager-Benutzerspeicher	Ein LDAP-Benutzerverzeichnis oder eine relationale Datenbank, die die Datensätze für CA Identity Manager-Benutzer enthält	Informationen finden Sie in der Dokumentation, die mit Ihrer Datenbank oder LDAP-Software geliefert wurde.
CA Identity Manager-Datenbanken	Die Datenbanken für Aufgabenpersistenz, Workflow, Überwachung, Objektspeicher, Berichterstellung und Aufgabenpersistenz-Archiv Workflow, Aufgabenpersistenz und Überwachung haben die höchste Häufigkeit von Änderungen, und Sicherungen sollten dementsprechend geplant werden.	Informationen finden Sie in der Dokumentation, die mit Ihrer Datenbank-Software geliefert wurde.
SiteMinder-Richtlinienspeicher	Ein LDAP-Benutzerverzeichnis oder eine relationale Datenbank mit Objekten für den SiteMinder-Richtlinienserver, wenn Sie SiteMinder verwenden	Informationen finden Sie in der Dokumentation, die mit Ihrer Datenbank oder LDAP-Software geliefert wurde.
Bereitstellungsverzeichnis	Ein LDAP-Benutzerverzeichnis, das die Datensätze für Bereitstellungsbenutzer und Bereitstellungsobjekte enthält	Informationen finden Sie in der CA Directory-Dokumentation.
Anwendungsserver-JMS-Persistenzspeicher	Die Speicher, die für CA Identity Manager-Aufgabenereignis-Verarbeitungsmeldungen verwendet werden	Informationen finden Sie in der Anwendungsserver-Dokumentation.
Berichtsdatenbanken	Snapshot-Datenbank BusinessObjects-Datenbank	Informationen finden Sie in der Dokumentation, die mit Ihrer Datenbank-Software geliefert wurde.
Benutzerdefinierte Berichte	Benutzerdefinierte Berichte und zugehörige XML-Dateien	Rufen Sie die Dokumentation zu BusinessObjects Enterprise, Version 2 und Version 2 SP 4 über die SAP-Dokumentationswebseite ab.

Schließen Sie die folgenden Komponenten mithilfe eines Dateisystemsicherungsprogramms in Ihre Sicherungspläne ein:

Komponente	Beschreibung
Webserver-Komponenten	Konfiguration von bereitgestellten Webserver-Komponenten, wie Anwendungsserver-Plug-ins und SiteMinder-Web-Agenten. Ein Webserver-Frontend ist erforderlich, wenn Sie Lastenausgleich verwenden oder wenn Sie SiteMinder verwenden, um den Zugriff auf die Benutzerkonsole zu schützen.
XML-Datendateien	Alle CA Identity Manager-Verzeichnisse und Umgebungsdateien, die verwendet werden, um CA Identity Manager-Objektspeicher-Objekte zu erstellen, zu verwalten und zu archivieren.
CA Identity Manager-Anpassungskomponenten	Dateien befinden sich in den folgenden iam_im.ear-Ordnern: ■ Config ■ User_console.war WEB-INF\web.xml
Skripte und Programme	TEWS-Skripte, Programme, Programmausgänge
Connector Xpress-Komponenten	Benutzerdefinierte Connectors Connector Xpress-Projektdateien
Disaster-Recovery-Dokumentation	Sobald Sie Ihre eigene Dokumentation für Disaster Recovery erstellen, sichern Sie sie regelmäßig, falls die Anweisungen sich ändern.

Entwickeln von Wiederherstellungsverfahren

Die Verfahren zur Wiederherstellung hängen von der Sicherungsmethode ab. Die Wiederherstellung für ein ausgefallenes System hängt von den Umständen ab. Allerdings besteht in vielen Fällen die Wiederherstellungsmethode in der Neuinstallation der Software. Ausführliche Informationen finden Sie im Kapitel über Hochverfügbarkeitsbereitstellungen im *Installationshandbuchs*.

Wiederherstellen des CA Identity Manager-Benutzerspeichers

Informationen zum Wiederherstellen des CA Identity Manager-Benutzerspeichers finden Sie in der Dokumentation, die mit Ihrer Datenbank oder LDAP-Software geliefert wurde. Überprüfen Sie, dass der Datenspeicher aus der Sicherung intakt ist, einschließlich des Zugriffs auf alle Benutzerspeicher.

Wiederherstellen der CA Identity Manager-Datenbanken

Informationen zum Wiederherstellen der CA Identity Manager-Datenbanken finden Sie in der Dokumentation, die mit Ihrer Datenbank geliefert wurde. Überprüfen Sie, dass der Datenspeicher aus der Sicherung intakt ist, einschließlich des Zugriffs auf alle Datenbanken.

Wiederherstellen des SiteMinder-Richtlinienspeichers

Informationen zum Wiederherstellen des SiteMinder-Richtlinienspeichers finden Sie in der Dokumentation, die mit Ihrer Datenbank oder LDAP-Software geliefert wurde. Überprüfen Sie, dass der Datenspeicher aus der Sicherung intakt ist, einschließlich des Zugriffs auf alle Benutzerspeicher.

Wiederherstellen des CA Identity Manager-Servers

Wenn ein Cluster-Knoten für einen CA Identity Manager-Server ausfällt, führen Sie die folgenden Schritte aus:

1. Verwenden Sie den dokumentierten Standardvorgang, um einen Knoten hinzuzufügen.

   Weitere Informationen dazu finden Sie im *Installationshandbuch* der Cluster-Installation.

2. Aktualisieren Sie die Verbindung zum Bereitstellungsserver.

   Ausführliche Informationen finden Sie im Abschnitt zum Bereitstellungs-Failover im Kapitel über Hochverfügbarkeitsbereitstellungen des *Installationshandbuchs*.

Wiederherstellen von Bereitstellungsserver und -verzeichnis

Sie können einen ausgefallenen Bereitstellungsserver durch die Installierung eines alternativen Servers wiederherstellen. Wenn alle Systeme ausgefallen sind, stellen Sie die während des Systemausfalls verloren geganenen Daten wieder her.

Führen Sie die folgenden Schritte aus:

1. Kopieren Sie benutzerdefinierte Schemadateien in das CA Directory-Verzeichnis "config\schema".
2. Installieren Sie das neue Bereitstellungsverzeichnis.

   Die Datenspeicher sind leer.
3. Stellen Sie die Daten vom Sicherungsspeicherort wieder her.
4. Verwenden Sie das Bereitstellungsserver-Installationsprogramm, und geben Sie die Details für das neu wiederhergestellte Bereitstellungsverzeichnis an.

   Die Domäneninformationen sollten bereits vorhanden sein.
5. Stellen Sie ggf. den benutzerdefinierten Connector und Konfigurationsdateien aus der Sicherung wieder her.

Hinweis: Weitere Informationen finden Sie in der Dokumentation zu CA Directory.

Wiederherstellen des Connector-Servers

Wenn ein Connector-Server ausfällt, führen Sie die folgenden Schritte aus:

1. Verwenden Sie das Connector-Server-Installationsprogramm, um einen neuen Connector-Server zu installieren

   Registrieren Sie ihn während Installation bei dem Bereitstellungsserver.
2. Entfernen Sie die Registrierung des ausgefallenen Connector-Servers mithilfe von "csfconfig" oder Connector Xpress.

Wiederherstellen eines Berichtsservers

Wenn der Berichtsserver ausfällt, finden Sie die entsprechenden Verfahren in der BusinessObjects-Dokumentation. Rufen Sie die Dokumentation zu BusinessObjects Enterprise, Version 2 und Version 2 SP 4 über die SAP-Dokumentationswebseite ab.

Wiederherstellen von Admin-Aufgaben

Wenn eine Admin-Aufgabe zum Zeitpunkt des Systemausfalls bearbeitet wurde, kann sie unter den folgenden Bedingungen wieder hergestellt werden.

- Eine Admin-Aufgabe, die im Status "Ausstehend" mit Warten auf Genehmigungen war, ist weiterhin verfügbar, wenn die Speicher, die die Statusinformationen verwalten, noch vorhanden sind. Die Speicher schließen die Aufgabenpersistenz-Datenbank ein, den JMS-Speicher, der die Aufgaben- und Ereignis-JMS-Meldungen enthält, und die Workflow-Datenbank ein.
- Aufgaben mit Status "In Bearbeitung" (jeder andere Status als "Ausstehend") sind abhängig von weiteren Bedingungen.

  Eine Aufgabe in diesem Status erfordert das Senden einer neuen JMS-Meldung zur CA Identity Manager-Ereignismeldungs-Warteschlange, um weiter bearbeitet zu werden. Ausfälle, die auftreten, bevor dieses Ereignis an die Warteschlange gesendet wurde, verhindern, dass die Aufgabe nach der Wiederherstellung fortgesetzt wird.

  In dieser Situation sind zwei Optionen möglich, um die Aufgabe wiederherzustellen:

  - Wenn die Aufgabe in der Aufgabe "Gesendete Aufgaben anzeigen" im fehlgeschlagenen Status vorhanden ist, wechseln Sie zur Seite "Aufgabendetails" und verwenden die Option "Aufgabe erneut senden", um die Aufgabe erneut zu übermitteln.
  - Senden Sie eine neue Aufgabe mit den gleichen Änderungen.

Dokumentieren des Wiederherstellungsplans

Basierend auf den Richtlinien in diesem Kapitel empfehlen wir, dass Sie eine spezielle Disaster-Recovery-Dokumentation entwickeln, die sich auf Ihre Organisation bezieht.

Erwägen Sie folgende Vorgehensweise:

1. Identifizieren Sie die Namen und Standorte von Systemen in Ihrer Architektur und alternativen Komponenten für jedes System.

   Listen Sie für jedes System die installierte Software auf, wie das jeweilige installierte JDK, das Reparatur-Release eines Anwendungsservers und die Größe des installierten Speichers. Diese Details sind notwendig für ein System, das Sie komplett wieder aufbauen möchten.

2. Schreiben Sie Verfahren auf, um jede Komponente wiederherzustellen, oder im Bedarfsfall für die Wiederherstellung eines vollständigen Systems.

3. Identifizieren Sie eine Methode, um Benutzernamen und Kennwörter für Systeme und CA Identity Manager-Benutzeroberflächen zu finden oder zurückzusetzen, wenn diese nur ein oder zwei Mitarbeiter kennen.

4. Schützen Sie Ihre Disaster-Recovery-Dokumentation vor Verlust, indem Sie eine Sicherungskopie erstellen, die Sie an einem bekannten externen Standort speichern.

Testen des Wiederherstellungsplans

Um dabei zu helfen, eine erfolgreiche Wiederherstellung nach einem Systemausfall zu gewährleisten, können Sie einen simulierten Notfall planen, wo gewisse Systeme nicht verfügbar sind. Ziehen Sie die folgenden Tests in Erwägung, die in den nachfolgenden Abschnitten beschrieben werden.

1. Testen Sie den Failover-Prozess.

2. Testen Sie die Wiederherstellung von Systemen.

Testen des Failover-Prozesses

Alle Server oder Verzeichnisse sollten einen alternativen Server oder ein Verzeichnis an einem Remote-Standort haben, einschließlich dieser Komponenten:

- CA Identity Manager-Server
- Bereitstellungsserver
- Bereitstellungsverzeichnisse
- C++ und Java-Connector-Server
- Berichtsserver
- Richtlinienserver

Halten Sie jede Komponente manuell an und überprüfen Sie, dass alle Vorgänge weiterhin mithilfe der alternativen Komponente funktionieren. Zum Beispiel könnten Sie den folgenden Test des Bereitstellungsservers ausführen:

1. Halten Sie auf einem System mit dem primären Bereitstellungsserver die Bereitstellungsserverdienste im Dialogfeld der Windows-Dienste an.

   Der primäre Bereitstellungsserver wird angehalten.

2. Führen Sie in der Benutzerkonsole folgende Aktionen aus:

   a. Weisen Sie einem Benutzer eine Bereitstellungsrolle zu.

   b. Überprüfen Sie, dass die Endpunkt-Benutzerkonten für diesen Benutzer erstellt werden.

      Die Konten, die erstellt werden, hängen von dem alternativen Bereitstellungsserver ab, der die Kommunikation mit dem CA Identity Manager-Server verarbeitet.

Dieser Vorgang ist ein Beispiel für einen Test. Entwickeln Sie für jede Komponente, die Sie anhalten, ähnliche Tests, um zu überprüfen, dass die alternative Komponente verwendet wird.

Testen der Wiederherstellungsverfahren

Führen Sie entsprechend Ihrer Disaster-Recovery-Dokumentation einen Test für jeder kritische Komponente aus, um zu bestätigen, dass Sie das ausgefallene System wiederherstellen können.

Durchführen von Disaster-Recovery-Schulungen

Sobald Sie glauben, dass die Wiederherstellungsvorgänge zuverlässig sind, stellen Sie sicher, dass die Mitarbeiter, die die Wiederherstellung implementieren müssen, dazu in der Lage sind. Ihre Organisation kann ggf. andere Schritte benötigen, aber das Folgende sind einige allgemeine Richtlinien:

1. Machen Sie den Speicherort der Wiederherstellungsdokumentation öffentlich bekannt.
2. Führen Sie einen Probelauf zur Übung durch.
3. Integrieren Sie Feedback von der Übung, um sicherzustellen, dass die endgültigen Disaster-Recovery-Vorgänge ausreichend sind.

Hinweis: Sie können auch die Übung als eine Chance verwenden, Wiederherstellungskoordinatoren einschließlich einer Person als der Wiederherstellungskoordinator und einer zweiten Person als alternativen Koordinator zuzuweisen. Diese Mitarbeiter sollten beauftragt werden, sich an einem dokumentierten Ort zu treffen, um den Disaster-Recovery-Plan umzusetzen.