CA Enterprise Log Manager

Implementierungshandbuch

r12.1 SP1

CA-Produktreferenzen

Dieses Dokument bezieht sich auf die folgenden Produkte von CA:

- CA Access Controll
- CA Audit
- CA ACF2™
- CA Directory
- CA Embedded Entitlements Manager (CA EEM)
- CA® Enterprise Log Manager
- CA Identity Manager
- CA IT Process Automation Manager (CA IT PAM)
- CA NSM
- CA Security Command Center (CA SCC)
- CA Service Desk
- CA SiteMinder®
- CA Spectrum®
- CA Top Secret®

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.

Änderungen in der Dokumentation

Seit der letzten Version dieser Dokumentation wurden folgende Aktualisierungen vorgenommen:

- Installationshinweise für ein System mit SAN-Laufwerken – In diesem neuen Abschnitt werden alternative Vorgehensweisen beschrieben, wie die Installation von CA Enterprise Log Manager auf einem SAN-Laufwerk verhindert werden kann, da in diesem Fall die Installation fehlschlagen würde.
- Standardportzuweisungen – Eine Beschreibung von Port 53, ein bekannter TCP-/UDP-Port für Domänennamen-Server (DNS), wurde diesem vorhandenen Thema hinzugefügt.
- Konfigurieren von nicht interaktiver Authentifizierung für die automatische Archivierung – Dieser Abschnitt wurde erweitert und enthält nun das häufige Szenario der Archivierung zwischen mehreren Sammelserver und einzelnen Berichtsserver. Für das Szenario mit einem Sammelserver, einem Berichtsserver, und einem Remote-Speicherserver zeigen Beispiele die Beziehung zwischen nicht interaktiver Authentifizierung und der entsprechenden automatischen Archivierung.
- Automatische Software-Updates ohne Online-Proxy – Dieser bereits vorhandene Abschnitt wurde aktualisiert. Es wird eine neue FTP-Seite beschrieben, die eine tar-Datei für jede CA Enterprise Log Manager-Version und alle Service Packs enthält. Sie können die Datei mit der Erweiterung "tar" herunterladen und auf einem Offline-Update-Proxy entpacken.
- Flussdiagramm zur Bereitstellung automatischer Software-Updates – Dieses neue Thema wurde hinzugefügt, um einen Querverweis zwischen Informationen zum Abrufen von Aktualisierungen in einer Offline-Umgebung und On-Demand-Aktualisierungen herzustellen.
- Der Anhang "Hinweise zu CA IT PAM" – Dieser Anhang enthielt Angaben zu Installationspfaden, die nicht für alle Szenarien gelten. Dies wurde korrigiert. Verschiedene Themen in diesem Abschnitt wurden abgeändert, um widerzuspiegeln, dass eine gemeinsame Verwendung des CA EEM-Servers von CA Enterprise Log Manager und CA IT PAM im FIPS-Modus nicht unterstützt wird.
- Durchführen eines Upgrades vorhandener CA Enterprise Log Manager-Server und Agenten – In diesem neuen Abschnitt wird der Vorgang beschrieben, wie ein Upgrade für sowohl Server als auch Agenten durchgeführt wird, um FIPS-Unterstützung zu erhalten, wie der FIPS-Modus aktiviert werden kann und wie der FIPS-Modus für Agenten über das Agenten-Dashboard überprüft werden kann.

- Hinzufügen eines neuen CA Enterprise Log Manager-Servers zu einer bereits vorhandenen Föderation, in der FIPS-Modus aktiviert ist – In diesem neuen Abschnitt werden die Prozesse beschrieben, über die Sie einer vorhandenen Föderation, bei der sowohl die lokalen als auch die CA EEM-Remote-Server im FIPS-Modus ausgeführt werden, hinzufügen können.
- Implementieren von benutzerdefinierten Zertifikaten – Dieses bereits vorhandene Thema wurde verändert und enthält nun die neue Dateinamenerweiterung ".cer" des Zertifikats.
- Hinzufügen des vertrauenswürdigen Root-Zertifikats zum CA Enterprise Log Manager-Verwaltungsserver – Dieses bereits vorhandene Thema wurde verändert und enthält nun die neue Dateinamenerweiterung ".cer" des Zertifikats.
- Hinzufügen des Zertifikats des vertrauenswürdigen Roots zu allen anderen CA Enterprise Log Manager-Servern – Dieses bereits vorhandene Thema wurde verändert und enthält nun die neue Dateinamenerweiterung ".cer" des Zertifikats.
- Hinzufügen eines allgemeinen Zertifikatsnamens zu einer Zugriffsrichtlinie – Dieses bereits vorhandene Thema wurde verändert und enthält nun die neue Dateinamenerweiterung ".cer" des Zertifikats.
- Bereitstellen neuer Zertifikate – Dieses bereits vorhandene Thema wurde verändert und enthält nun die neue Dateinamenerweiterung ".cer" des Zertifikats.
- Agenten und das Agentenzertifikat – Dieses bereits vorhandene Thema wurde verändert und enthält nun die neue Dateinamenerweiterung ".cer" des Zertifikats.
- Wiederherstellen eines CA EEM-Servers für die Verwendung mit CA Enterprise Log Manager – Dieses bereits vorhandene Thema wurde verändert und enthält nun die neue Dateinamenerweiterung ".cer" des Zertifikats.
- Sichern eines CA Enterprise Log Manager-Servers – Dieses bereits vorhandene Thema wurde verändert und enthält nun die neue Dateinamenerweiterung ".cer" des Zertifikats.
- Integration mit CA Audit r8 SP2 – Die Themen in diesem Abschnitt wurden entfernt, da CAELM4Audit nicht unter r12.1 SP1 und höher unterstützt wird.

Weitere Informationen:

Flussdiagramm zur Bereitstellung automatischer Software-Updates (siehe Seite 177)
Szenario: Verwendung von CA EEM auf CA Enterprise Log Manager zur Authentifizierung von CA IT PAM (siehe Seite 274)
Bereiten Sie die Implementierung der CA IT PAM-Authentifizierung auf freigegebenem CA EEM vor (siehe Seite 275)
Kopieren einer XML-Datei auf den CA Enterprise Log Manager-Verwaltungsserver (siehe Seite 276)
Kopieren des Zertifikats auf den CA IT PAM-Server (siehe Seite 278)
Festlegen von Kennwörtern für die vordefinierten CA IT PAM-Benutzerkonten (siehe Seite 278)
Installieren der CA IT PAM-Domäne (siehe Seite 280)
Implementierungsprozess der CA IT PAM-Authentifizierung (siehe Seite 274)
Registrieren von CA IT PAM mit freigegebenem CA EEM (siehe Seite 276)
Wiederherstellen eines CA EEM-Servers für die Verwendung mit CA Enterprise Log Manager (siehe Seite 286)
Sichern eines CA Enterprise Log Manager-Servers (siehe Seite 287)
Hinzufügen eines neuen CA Enterprise Log Manager-Servers zu einer bereits vorhandenen Föderation, in der FIPS-Modus aktiviert ist (siehe Seite 94)

Inhalt

Kapitel 3: Installieren von CA Enterprise Log Manager 71

Anhang A: Aspekte für CA Audit-Benutzer 223

Anhang B: Aspekte für CA Access Control-Benutzer 249

Kapitel 1: Einführung

Dieses Kapitel enthält folgende Themen:

Über dieses Handbuch

In diesem *CA Enterprise Log Manager-Implementierungshandbuch* finden Sie Anleitungen zur Planung, Installation und Konfiguration von CA Enterprise Log Manager, so dass Sie Ereignisprotokolle von Ereignisquellen in Ihrem Netzwerk empfangen können. Das Handbuch ist so aufgebaut, dass bei den einzelnen Aufgaben zunächst der Ablauf und die Ziele beschrieben werden. Auf die Abläufe folgen in der Regel relevante Konzepte und dann Verfahren zum Erreichen der Ziele.

Das *CA Enterprise Log Manager-Implementierungshandbuch* richtet sich an Systemadministratoren, die für die Installation, Konfiguration und Wartung einer Lösung zur Protokollerfassung, für die Erstellung von Benutzern und die Festlegung bzw. Zuweisung von Benutzerrollen sowie für Zugriff auf und Wartung von Sicherungsdaten verantwortlich sind.

Ferner enthält dieses Handbuch Informationen zu den folgenden Aufgaben:

- Konfigurieren eines Connectors oder Adapters zum Erfassen von Ereignisdaten
- Konfigurieren von Services zur Steuerung von Berichterstellung, Datenaufbewahrung, Sicherung und Archivierung
- Konfigurieren einer Föderation (Verbunds) von CA Enterprise Log Manager-Servern
- Konfigurieren von automatischen Software-Updates zum Abrufen von Inhalts-, Konfigurations- und Betriebssystemaktualisierungen

Übersicht über den Inhalt des Handbuchs:

Abschnitt	Description
Planen der Umgebung	Beschreibt die Planung von Bereichen wie Protokollerfassung, Agenten, Föderation (Verbund), Benutzer- und Zugriffsverwaltung, automatische Software-Updates und Disaster Recovery
Installieren von CA Enterprise Log Manager	Stellt Arbeitsblätter mit erforderlichen Informationen und detaillierte Anleitungen für die Installation von CA Enterprise

Abschnitt	Description
	Log Manager sowie die Überprüfung der Installation bereit
Grundlagen zur Benutzer- und Zugriffskonfiguration	Bietet Anleitungen zur Bestimmung eines Benutzerspeichers und zum Erstellen eines anfänglichen administrativen Benutzers für die Konfiguration der anderen Benutzer und Zugriffsinformationen
Konfigurieren von Services	Bietet Anleitungen zum Konfigurieren von Services wie globale und lokale Filter, Ereignisprotokollspeicher, Berichtsserver und Optionen für automatische Software-Updates
Konfigurieren der Ereigniserfassung	Bietet Konzepte und Anleitungen für die Verwendung oder Konfiguration der Komponenten für die Ereignisverfeinerungs-Bibliothek, etwa der Zuordnungs- und Analysedateien und der CA-Adapter
Erstellen von Föderationen	Beschreibt unterschiedliche Arten von Föderationen (Verbunden) und bietet Anleitungen zum Erstellen von Verbundbeziehungen zwischen CA Enterprise Log Manager-Servern sowie zum Anzeigen eines Föderationsdiagramms
Arbeiten mit der Ereignisverfeinerungs-Bibliothek	Bietet Übersichtsinformationen zur Arbeit mit Nachrichtenanalyse- und Datenzuordnungsdateien
Aspekte für CA Audit-Benutzer	Beschreibt die möglichen Interaktionen zwischen CA Enterprise Log Manager und CA Audit, die Konfiguration von iRecordern und Richtlinien sowie den Import von Daten aus einer CA Audit-Collector-Datenbank
Aspekte für CA Access Control-Benutzer	Beschreibt die Integration mit CA Access Control, die Änderung von CA Audit-Richtlinien zum Senden von Ereignissen an CA Enterprise Log Manager, die Konfiguration eines CA Access Control-iRecorders zum Senden von Ereignissen an CA Enterprise Log Manager sowie den Import von CA Access Control-Ereignissen aus einer CA Audit-Collector-Datenbank
Hinweise zu CA IT PAM	Beschreibt den Installationsprozess für CA IT PAM, durch den die Authentifizierung von der EEM-Komponente auf dem CA Enterprise Log Manager-Verwaltungsserver ausgeführt wird.
Disaster Recovery	Beschreibt Verfahren zur Sicherung, Wiederherstellung und zum Austausch von Daten mit dem Ziel, die Wiederherstellung Ihrer Protokollverwaltungslösung im Notfall zu gewährleisten
CA Enterprise Log Manager und Virtualisierung	Beschreibt das Verfahren zum Erstellen und Konfigurieren eines virtuellen Rechners für einen CA Enterprise Log Manager-Server

Hinweis: Genaue Informationen zur Betriebssystemunterstützung und zu den Systemanforderungen finden Sie in den *Versionshinweisen*. Eine Übersicht über CA Enterprise Log Manager und ein einfaches Verwendungsszenario finden Sie im *Übersichtshandbuch*. Genaue Informationen zur Verwendung und Wartung des Produkts finden Sie im *Administrationshandbuch.* Informationen zur Verwendung aller Seiten in CA Enterprise Log Manager finden Sie in der Online-Hilfe.

Kapitel 2: Planen der Umgebung

Dieses Kapitel enthält folgende Themen:

Serverplanung

Zunächst müssen Sie bei der Planung Ihrer Umgebung entscheiden, wie viele CA Enterprise Log Manager-Server benötigt werden und welche Rollen die einzelnen Server übernehmen sollen. Es gibt folgende Rollen:

- Verwaltungsserver

  Auf diesem Server werden vordefinierte und benutzerdefinierte Inhalte und Konfigurationen gespeichert. Ferner werden über diesen Server Benutzer authentifiziert und Zugriff auf Funktionen gewährt.

- Quellserver

  Dieser Server empfängt Ereignisprotokolle von den Agenten und verfeinert Ereignisse.

- Berichtsserver

  Auf diesem Server werden Abfragen zu erfassten Ereignissen, spontane Abfragen und Berichte sowie geplante Alarme und Berichte verarbeitet.

- Wiederherstellungspunkt

  Dieser Server empfängt wiederhergestellte Ereignisprotokolldatenbanken zur Überprüfung alter Ereignisse.

Der erste installierte Server ist der Verwaltungsserver. Dieser Server kann auch andere Rollen übernehmen. Pro CA Enterprise Log Manager-Netzwerk kann nur ein Verwaltungsserver vorhanden sein. Jedes CA Enterprise Log Manager-Netzwerk muss über einen Verwaltungsserver verfügen.

Architekturvarianten:

- System mit einem Server, in dem der Verwaltungsserver auch alle anderen Rollen übernimmt
- System mit zwei Servern, in dem der Verwaltungsserver alle Rollen mit Ausnahme der des Quellservers übernimmt. Die Erfassung wird auf einem eigens dafür eingerichteten Server durchgeführt.

- System mit mehreren Servern, in dem jedem Server eine bestimmte Rolle zugewiesen ist.

Genaue Informationen zu Serverrollen und Architekturen finden Sie im Folgenden.

Serverrollen

Ein CA Enterprise Log Manager-System kann einen oder mehrere Server aufweisen. Indem Sie verschiedenen Servern unterschiedliche Rollen zuweisen, können Sie die Leistung optimieren. Es ist jedoch auch möglich, dass ein Server verschiedene oder sogar alle Rollen übernimmt. Wenn Sie überlegen, welche Rollen Sie den einzelnen installierten Servern zuweisen möchten, bedenken Sie, welche Verarbeitungslast jede Rolle in Bezug auf andere relevante Faktoren in der Umgebung mit sich bringt.

- Verwaltungsserver

  Die Rolle des Verwaltungsservers wird standardmäßig vom ersten installierten CA Enterprise Log Manager-Server übernommen. Der Verwaltungsserver führt folgende Hauptfunktionen aus:

  - Er fungiert als allgemeines Repository für alle Server, die auf diesem Server registriert werden. Insbesondere werden auf diesem Server Anwendungsbenutzer, Anwendungsgruppen (Rollen), Richtlinien, Kalender und Anwendungsobjekte gespeichert.
  - Falls Sie den Benutzerspeicher als internen Speicher konfigurieren, werden zudem globale Benutzer, globale Gruppen und Kennwortrichtlinien hier gespeichert. Falls der konfigurierte Benutzerspeicher auf einen externen Benutzerspeicher verweist, werden die Informationen zum globalen Benutzerkonto und zur globalen Gruppe aus dem referenzierten Benutzerspeicher geladen.
  - Er verarbeitet Benutzerrechte anhand einer schnellen, mit dem Speicher verknüpften Datei. Er authentifiziert Benutzer anhand der Benutzer- und Gruppenkonfiguration. Er autorisiert Benutzer für den Zugriff auf verschiedene Abschnitte der Benutzeroberfläche anhand von Richtlinien und Kalendern.
  - Er empfängt alle über automatische Software-Updates heruntergeladenen Inhalts- und Konfigurationsaktualisierungen.

  Ein CA Enterprise Log Manager-Servernetzwerk kann nur einen aktiven Verwaltungsserver aufweisen, es kann jedoch ein (inaktiver) Failover-Verwaltungsserver vorhanden sein. Falls Sie mehrere CA Enterprise Log Manager-Netzwerke erstellen, muss jedes über seinen eigenen aktiven Verwaltungsserver verfügen.

- Sammelserver

  In einem System mit einem Server fungiert der Verwaltungsserver auch als Sammelserver. In einem System mit zwei oder mehreren Servern sollte ein eigener Sammelserver vorhanden sein. Ein Sammelserver führt folgende Funktionen aus:

  – Er unterstützt die Konfiguration von Connectors.

  – Er empfängt die von den Connectors auf den Agenten eingehenden Ereignisprotokolle.

  – Er bereitet die eingehenden Ereignisprotokolle auf, indem die Daten aller Nachrichten analysiert und in das ELM-Schemadefinitionsformat übertragen werden, das eine einheitliche Darstellung von Ereignisdaten aus unterschiedlichen Ereignisquellen ermöglicht.

  – Er fügt Ereignisprotokolle in die Online-Datenbank ein und komprimiert die Online-Datenbank in eine Standby-Datenbank, wenn die festgelegte Größe erreicht ist.

  – Er archiviert die Standby-Datenbank automatisch anhand des festgelegten Zeitplans auf dem zugehörigen Berichtsserver.

    Wichtig! Wenn Sie getrennte Server für die Erfassung und die Berichterstellung verwenden, müssen Sie eine nicht interaktive Authentifizierung und eine stündliche, automatische Archivierung vom Sammelserver zum Berichtsserver konfigurieren.

  Ziehen Sie das von den Ereignisquellen produzierte Ereignisvolumen in Betracht, wenn Sie überlegen, ob Server eigens für die Ereigniserfassung und -verfeinerung eingerichtet werden sollen. Bedenken Sie zudem, wie viele Sammelserver Daten automatisch auf einem einzelnen Berichtsserver archivieren.

- Berichtsserver

  In einem System mit einem oder zwei Servern fungiert der Verwaltungsserver auch als Berichtsserver. In einem System mit vielen Servern sollten Sie mindestens einen Server eigens als Berichtsserver einrichten. Ein Berichtsserver führt folgende Funktionen aus:

  - Da die nicht interaktive Authentifizierung und automatische Archivierung konfiguriert ist, empfängt er neue Datenbanken mit aufbereiteten Ereignissen der Sammelserver.
  - Er verarbeitet spontane Befehle, Abfragen und Berichte.
  - Er verarbeitet geplante Alarme und Berichte.
  - Er unterstützt Assistenten für die Erstellung individueller Abfragen und Berichte.
  - Wenn nicht interaktive Authentifizierung und automatische Archivierung vom Berichtsserver auf einen Remote-Speicherserver konfiguriert wird, werden alte Datenbanken auf einen Remote-Speicherserver verschoben.

  Falls auf einem Server mit vielen spontanen Aktivitäten viele komplexe Berichte und Alarme erzeugt werden sollen, sollten Sie einen eigenen Server für die Berichterstellung einrichten.

- Remote-Speicherserver

  Ein Remote-Speicherserver, bei dem es sich nicht um einen CA Enterprise Log Manager-Server handelt, führt folgende Funktion aus:

  - Er empfängt in festgelegten Intervallen stark komprimierte, automatisch archivierte Datenbanken von den Berichtsservern, bevor diese aufgrund ihres Alters oder aufgrund mangelnden Speicherplatzes gelöscht werden. Wenn Sie die automatische Archivierung einrichten, müssen Sie die Datenbanken nicht manuell verschieben.
  - Er dient als lokaler Speicher für Offline-Datenbanken. Sie können diese Datenbanken wahlweise auch für die langfristige Speicherung an einen externen Speicherort verschieben bzw. kopieren. Offline-Datenbanken werden in der Regel gemäß den behördlich vorgeschriebenen Fristen aufbewahrt.

  Remote-Speicherserver gehören nie zu einer CA Enterprise Log Manager-Föderation. Sie sollten allerdings in die Planung Ihrer Architektur einbezogen werden.

- Wiederherstellungspunktserver

  Berichtsserver fungieren in der Regel als Wiederherstellungspunktserver für die Datenbanken, die früher auf ihnen gespeichert waren. Falls Sie über ein großes Netzwerk verfügen, sollten Sie einen eigenen CA Enterprise Log Manager-Server für diese Rolle einrichten. Ein Wiederherstellungspunktserver führt folgende Funktionen aus:

  - Er dient für die Überprüfung der Protokolle alter Ereignisse.
  - Er empfängt wiederhergestellte Datenbanken von einem Remote-Speicherserver, auf dem alle Offline-Datenbanken gespeichert sind. Sie können das Hilfsprogramm "restore-ca-elm.sh" dazu verwenden, Datenbanken zum Wiederherstellungspunkt zu verschieben, wenn Sie zuerst die nicht interaktive Authentifizierung vom Speicherserver zum Wiederherstellungspunkt konfigurieren.
  - Er katalogisiert den Archivkatalog neu und fügt die wiederhergestellten Datenbanken zu seinen Datensätzen hinzu.
  - Er bewahrt Datensätze über verschiedene konfigurierte Zeiträume hinweg auf, je nach Wiederherstellungsmethode.

  Der Vorteil eines eigenen Wiederherstellungspunkts ist, dass dieser Server aus der Föderation ausgeschlossen werden kann, so dass föderierte Berichte keine alten, wiederhergestellten Daten enthalten. Alle auf dem Wiederherstellungspunktserver erstellten Berichte enthalten nur Ereignisdaten aus den wiederhergestellten Datenbanken.

Wenn Sie einem Server eine bestimmte Rolle zuweisen, bedeutet dies nicht, dass auf diesem Server keine Funktionen anderer Rollen ausgeführt werden können. Nehmen Sie als Beispiel eine Umgebung mit dedizierten Sammelservern und einem Berichtsserver. Sie können in dieser Umgebung einen Alarm planen, mit dem der Sammelserver auf einen bestimmten Umstand hin überprüft wird, über den Sie unbedingt so bald wie möglich unterrichtet werden müssen.

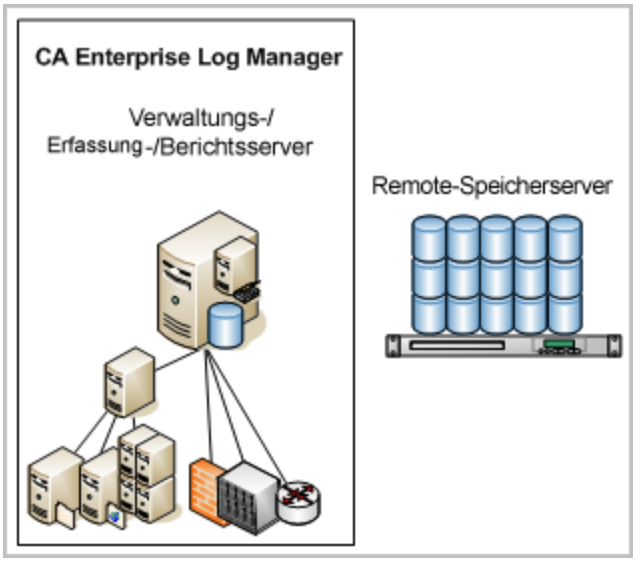
Beispiel: Netzwerkarchitekturen

Die einfachste CA Enterprise Log Manager-Architektur ist ein System mit einem Server, in dem ein CA Enterprise Log Manager-Server alle Rollen übernimmt:

- Die CA Enterprise Log Manager-Verwaltungs-, -Quell- und -Berichtsserver übernehmen die Konfigurations-/Inhaltsverwaltung, Ereigniserfassung und -verfeinerung sowie Abfragen und Berichte.

  Hinweis: Ein Remote-Server, bei dem es sich nicht um einen CA Enterprise Log Manager-Server handelt, speichert archivierte Ereignisprotokolldatenbanken.

Diese Konfiguration eignet sich für Systeme wie etwa Testsysteme mit geringem Ereignisvolumen und wenigen geplanten Berichten.

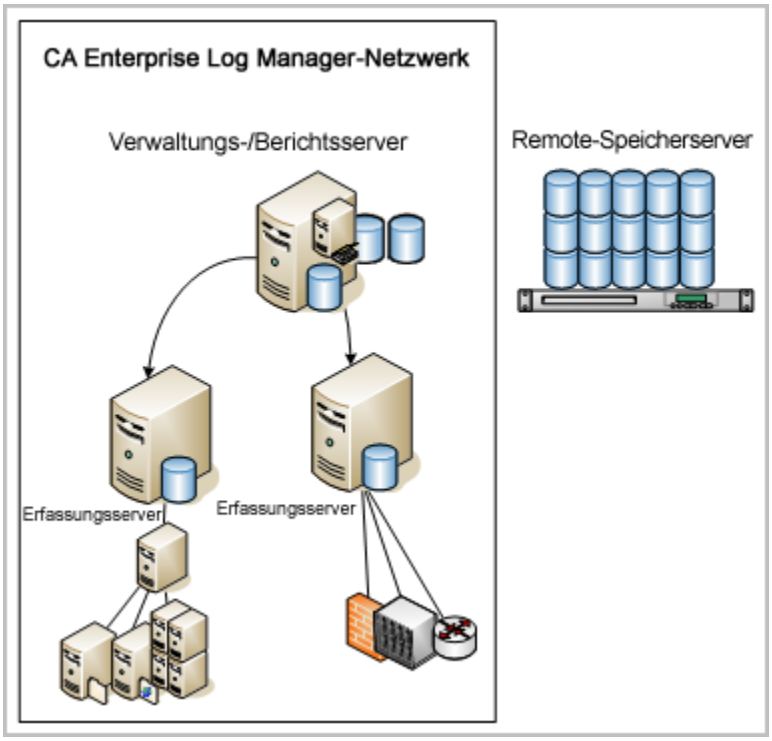


Auf diese einfachste Architektur folgt ein System mit mehreren Servern, in dem der erste installierte CA Enterprise Log Manager-Server die meisten Rollen übernimmt:

- Der CA Enterprise Log Manager-Verwaltungs- und -Berichtsserver übernimmt die Konfigurations-/Inhaltsverwaltung sowie Abfragen und Berichte.
- Die (agentenlosen) CA Enterprise Log Manager-Quellserver für Protokolldateien übernehmen die Ereigniserfassung und -verfeinerung.

Hinweis: Ein Remote-Server, bei dem es sich nicht um einen CA Enterprise Log Manager-Server handelt, wird für die Speicherung archivierter Ereignisprotokolldatenbanken eingerichtet.

Diese Architektur eignet sich für ein Netzwerk mit mittlerem Ereignisvolumen. Die Pfeile zeigen an, dass über die Verwaltungsfunktionen des Verwaltungs-/Berichtsservers die für alle Server geltenden globalen Einstellungen verwaltet werden. Sobald mehrere Quellserver vorhanden sind, wird diese Architektur "Hub-and-Spoke" genannt.

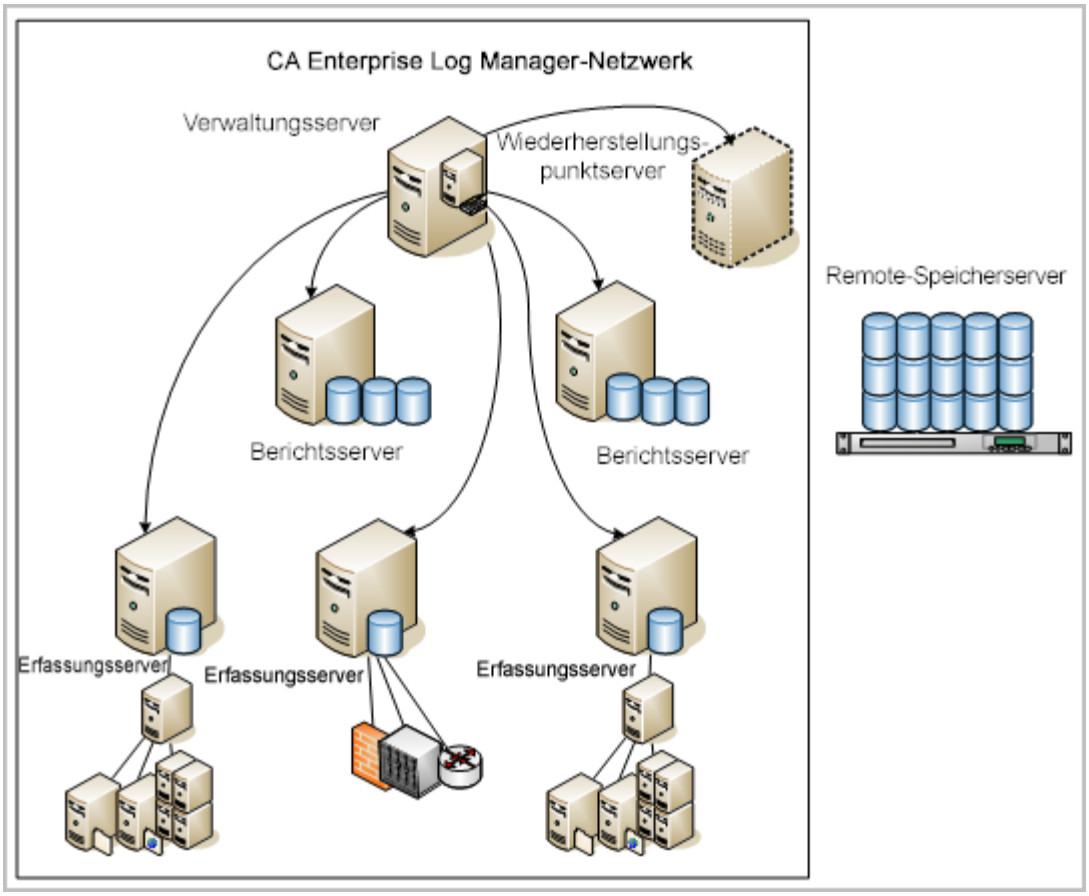


In einem großen Netzwerk mit hohem Ereignisvolumen, vielen komplexen geplanten Berichten und Alarmen und fortwährender individueller Anpassung können ein oder mehrere CA Enterprise Log Manager-Server spezifische Rollen übernehmen:

- Der CA Enterprise Log Manager-Verwaltungsserver übernimmt die Konfigurations- und Inhaltsverwaltung.
- Der CA Enterprise Log Manager-Berichtsserver verarbeitet Abfragen und Berichte.
- Die (agentenlosen) CA Enterprise Log Manager-Quellserver für Protokolldateien übernehmen die Ereigniserfassung und -verfeinerung.
- Wahlweise wird die Überprüfung von Ereignissen aus wiederhergestellten Archivdatenbanken von einem CA Enterprise Log Manager-Wiederherstellungspunktserver übernommen.

Hinweis: Ein Remote-Server, bei dem es sich nicht um einen CA Enterprise Log Manager-Server handelt, wird für die Speicherung archivierter Ereignisprotokolldatenbanken eingerichtet.

Dieses Setup ist ideal für große Netzwerke. Die Pfeile zeigen an, dass der Verwaltungsserver die für alle Server geltenden globalen Einstellungen verwaltet.



Planen der Ereigniserfassung

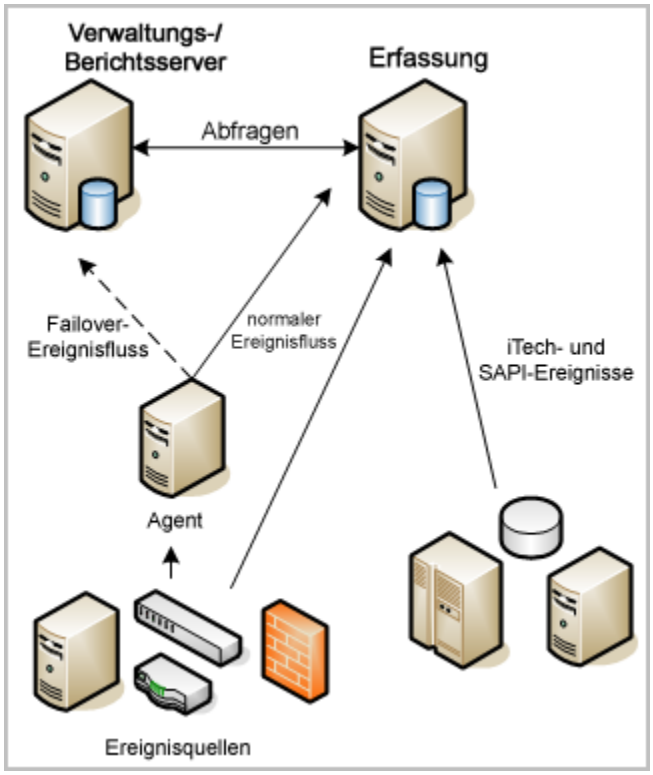
Die Planung der Protokollerfassung für Ihr Netzwerk basiert auf der Anzahl der Ereignisse pro Sekunde (EpS), die zur Speicherung verarbeitet werden müssen, und auf der erforderlichen Online-Aufbewahrungszeit der Daten. (*Online* bedeutet in diesem Fall "sofort durchsuchbar".) In der Regel werden die Daten 30 bis 90 Tage lang online aufbewahrt.

Jedes Netzwerk hat sein eigenes Ereignisvolumen, je nachdem, wie viele Geräte und welche Gerätetypen verwendet werden und in welchem Umfang Netzwerkgeräte und -anwendungen wie etwa Firewalls an die Ereignisinformationsanforderungen des Unternehmens angepasst sind. So erzeugen beispielsweise manche Firewalls je nach Konfiguration große Mengen überflüssiger Ereignisse.

Planen Sie Ihre Ereigniserfassung möglichst so, dass das gesamte Ereignisvolumen gleichmäßig auf alle CA Enterprise Log Manager-Server verteilt wird, so dass jeder Server nur eine normale konstante Arbeitslast verarbeiten muss. Damit bei den in Unternehmen üblichen Ereignisvolumen eine optimale Leistung erzielt werden kann, empfiehlt sich die Installation von mindestens zwei föderierten CA Enterprise Log Manager-Servern:

- Ein CA Enterprise Log Manager-Berichtsserver für die Verarbeitung von Abfragen, Berichten und Alarmen, die Alarmverwaltung, die Verwaltung von automatischen Software-Updates sowie die Benutzerauthentifizierung und -autorisierung
- Mindestens ein spezifisch für die Maximierung von Datenbankeinfügungen konfigurierter (agentenloser) CA Enterprise Log Manager-Quellserver für Protokolldateien

Die folgende Abbildung zeigt ein einfaches Beispiel für ein solches föderiertes CA Enterprise Log Manager-Netzwerk. Zwei CA Enterprise Log Manager-Server (einer für Berichte und einer für die Erfassung) verarbeiten den von verschiedenen Ereignisquellen stammenden Ereignisstrom. Beide Server können Daten für Abfragen, Berichte und Alarme untereinander austauschen.



Der (agentenlose) *Quellserver für Protokolldateien* ist hauptsächlich zuständig für die eingehenden Ereignisprotokolldaten und die Einfügung in die Datenbank. Bei diesem Server wird eine kurze Datenaufbewahrungszeit von maximal 24 Stunden verwendet. Die gespeicherten Ereignisprotokolle werden über ein automatisiertes Skript täglich oder je nach Ereignisvolumen auch öfter auf den Berichtsserver verschoben. Die Föderation und die Verwendung föderierter Abfragen zwischen den beiden Servern gewährleistet, dass Sie präzise Berichte aus den Ereignisprotokollen auf *beiden* Servern erhalten.

Der *Berichts*server hat mehrere Funktionen:

- Verarbeitung von Abfragen und Berichten
- Planung und Verwaltung von Alarmen
- Verschieben archivierter Dateien auf einen Remote-Speicherserver
- Bereitstellung einer von Connectors erfassten Failover-Sammlung von Ereignissen für den (agentenlosen) Quellserver

Die Daten werden über ein automatisiertes Sicherungsskript vom Berichtsserver auf einen Remote-Server (komprimierte Offline-Speicherung) verschoben. Falls Sie Daten aus dem Offline-Speicher wiederherstellen, geschieht dies in der Regel auf dem Berichtsserver. Falls der Speicherplatz auf dem Berichtsserver begrenzt ist, können die Daten auch auf dem (agentenlosen) Quellserver für Protokolldateien wiederhergestellt werden. Da auf dem Quellserver keine großen Datenmengen gespeichert werden und dieser sich in einem Verbund befindet, erhalten Sie dieselben Berichtsergebnisse.

Ferner kann der Berichtsserver als Failover-Empfänger für Ereignisse fungieren, die von einem Connector auf einem Remote-Agent erfasst wurden, falls der Quellserver aus irgendeinem Grund keine Ereignisse mehr empfängt. Sie können den Failover auf Agentenebene konfigurieren. Bei der Failover-Verarbeitung werden Ereignisse an einen oder mehrere alternative CA Enterprise Log Manager-Server gesendet. Die Failover-Ereigniserfassung ist nicht verfügbar für Ereignisse, die über SAPI- und iTech-Listener aus alten Ereignisquellen erfasst wurden.

Weitere Informationen

CA Enterprise Log Manager und Virtualisierung (siehe Seite 291)

Planen des Speicherplatzes

Vergewissern Sie sich bei der Planung Ihrer Umgebung, dass ausreichend Speicherplatz für große Ereignismengen verfügbar ist. Bei (agentenlosen) Quellservern für Protokolldateien bedeutet dies, dass auf jedem Quellserver ausreichend Speicherplatz zur Aufnahme von Spitzenlasten und von normalen Ereignisvolumen bereitsteht. Beim Berichtsserver wird der Speicherplatzbedarf anhand der Ereignismenge und der erforderlichen Online-Verweildauer berechnet.

Online-Datenbanken werden nicht komprimiert. Standby-Datenbanken werden komprimiert. Neben den nicht komprimierten Online-Datenbanken sind auch die komprimierten Standby-Datenbanken online geschaltet. Sie können die Daten in diesen Datenbanken durchsuchen und entsprechende Berichte erstellen. In der Regel stehen zu einem bestimmten Zeitpunkt immer die Daten der letzten 30 bis 90 Tage für die unmittelbare Suche und Berichterstellung bereit. Ältere Datensätze werden auf einem Remote-Server gespeichert. Sie können diese Daten ggf. für die Suche und Berichterstellung wiederherstellen.

(Agentenlose) Quellserver für Protokolldateien unterstützen sowohl Online- als auch Standby-Datenbanken. Da die Verweildauer bei (agentenlosen) Quellservern mit 1 bis 23 Stunden sehr kurz ist, spielt die langfristige Datenspeicherung hier keine Rolle.

Auf dem Verwaltungsserver ist eine Online-Datenbank zum Einfügen selbstüberwachender Ereignismeldungen vorhanden.

Berichtsserver unterstützen kleinere Online-Datenbanken und eine große Anzahl von Standby-Datenbanken. Ferner müssen Berichtsserver genügend zusätzlichen Speicherplatz aufweisen, um ggf. wiederhergestellte Dateien eine Zeit lang aufnehmen zu können. Falls Sie mit DAS (Direct Attached Storage) arbeiten, werden die Partitionen automatisch so erweitert, dass mehr Speicherplatz zur Verfügung steht.

Wissenswertes über den CA EEM-Server

CA Enterprise Log Manager verwendet intern den CA Embedded Entitlements Manager-Server (CA EEM-Server) zum Verwalten von Konfigurationen, zum Autorisieren und Authentifizieren von Benutzern, zum Koordinieren von automatischen Updates für Inhalte und Binärdateien und für weitere Verwaltungsfunktionen. In einer einfachen CA Enterprise Log Manager-Umgebung wird CA EEM mit dem CA Enterprise Log Manager-Verwaltungsserver installiert. Ab diesem Zeitpunkt verwaltet CA EEM die Konfigurationen aller CA Enterprise Log Manager-Quellserver für Protokolldateien sowie deren Agenten und Connectors.

Sie können den CA EEM-Server auch mit den auf der Anwendungsinstallations-CD bereitgestellten Installationspaketen auf einem Remote-Server installieren, oder Sie können einen bereits vorhandenen, mit anderen CA-Produkten verwendeten CA EEM-Server nutzen.

Der CA EEM-Server verfügt über eine eigene Webschnittstelle. Die meisten Konfigurations- und Wartungsaufgaben werden allerdings über die CA Enterprise Log Manager-Benutzeroberfläche durchgeführt. Normalerweise müssen Sie nicht direkt mit den eingebetteten Funktionen des CA EEM-Servers interagieren, außer bei der Failover-Konfiguration und den Sicherungs- und Wiederherstellungsfunktionen, die Teil der Disaster Recovery sind.

Hinweis: Sie müssen bei der CA Enterprise Log Manager-Serverinstallation das Kennwort für das standardmäßige CA EEM-Verwaltungskonto (EiamAdmin) verwenden, damit der CA Enterprise Log Manager-Server ordnungsgemäß registriert wird. Wenn Sie den ersten CA Enterprise Log Manager-Verwaltungsserver installieren, erstellen Sie dieses Kennwort als Teil der Installation. Wenn Sie weitere CA Enterprise Log Manager-Server mit demselben Anwendungsinstanznamen installieren, erstellen Sie automatisch eine Netzwerkumgebung, in der Sie später Föderationsbeziehungen zwischen den CA Enterprise Log Manager-Servern einrichten können.

Richtlinien für die Protokollerfassung

Bedenken Sie während der Planungsphase folgende Richtlinien für die Protokollerfassung:

- Daten werden immer verschlüsselt vom Agenten an den CA Enterprise Log Manager-Server gesendet, unabhängig davon, ob Sie die agentenlose oder agentenbasierte Protokollerfassung verwenden.
- Ziehen Sie einen Mechanismus für die lokale Syslog-Erfassung in Betracht, um potenzielle Probleme bei der garantierten Auslieferung zu umgehen.

Ziehen Sie folgende Faktoren in Betracht, wenn Sie überlegen, ob Sie die direkte Erfassung durch den Standardagenten, die agentenbasierte Erfassung durch einen auf dem Host mit der Ereignisquelle installierten Agenten oder die agentenlose Erfassung, bei der sich der Agent auf einem von den Ereignisquellen unabhängigen Quellserver für Protokolldateien befindet, verwenden möchten:

- Unterstützte Plattformen

  WMI funktioniert beispielsweise für den Protokollsensor nur unter Windows.

- Unterstützte Treiber für bestimmte Protokollsensoren

  Damit ODBC funktioniert, benötigen Sie beispielsweise einen ODBC-Treiber.

- Remote-Zugriff auf die Protokollquelle

  Bei dateibasierten Protokollen benötigen Sie beispielsweise ein freigegebenes Laufwerk, damit diese standortfern (remote) verwendet werden können.

Planen von Föderationen

In CA Enterprise Log Manager ist eine *Föderation* (auch Verbund genannt) ein Netzwerk aus Servern, auf denen Ereignisdaten gespeichert und archiviert und Berichte über diese Daten erstellt werden. Mit einer Föderation können Sie steuern, wie Daten in einem Netzwerk gruppiert und überprüft werden. Sie können die Beziehungen der Server untereinander und somit die Abfrageroute zwischen den Servern festlegen. Ferner haben Sie die Möglichkeit, föderierte Abfragen bei spezifischen Abfragen ggf. zu aktivieren bzw. zu deaktivieren.

Die Entscheidung für oder gegen eine Föderation basiert auf der Kombination aus dem erforderlichen Ereignisvolumen und der geschäftlichen Notwendigkeit, Protokolldaten zu unterteilen und gesonderte Berichte zu erstellen. CA Enterprise Log Manager unterstützt hierarchische Verbunde und Netzverbunde sowie Konfigurationen, bei denen beide Verbundarten ineinander übergehen. Alle CA Enterprise Log Manager-Server, die in einen Verbund (Föderation) aufgenommen werden sollen, müssen denselben Anwendungsinstanznamen in CA EEM verwenden. Jede CA Enterprise Log Manager-Serverinstallation wird automatisch unter Verwendung eines Anwendungsinstanznamens beim CA EEM-Server registriert.

Sie können jederzeit eine Föderation anlegen, nachdem Sie den ersten CA Enterprise Log Manager-Server und mindestens einen weiteren Server installiert haben. Die besten Ergebnisse erzielen Sie jedoch, wenn Sie Ihre Föderation *vor* der Installation planen. Mit Hilfe einer detaillierten Föderationsübersicht können Sie die Konfigurationsschritte schnell und präzise durchführen.

Auf *Netzwerk*-Ebene bedeuten mehrere CA Enterprise Log Manager-Server, dass größere Ereignismengen verarbeitet werden können. Aus Sicht der *Berichterstellung* können Sie mit einer Föderation steuern, wer auf Ereignisdaten zugreifen darf und wie viele Daten diese Personen einsehen können.

In einer einfachen Umgebung mit zwei Servern übernimmt der Verwaltungsserver die Funktion eines Berichtsservers. Der interne CA EEM-Server auf dem CA Enterprise Log Manager-Verwaltungsserver verwaltet die Konfigurationen für die Föderation zentral und global. (Sie können die Konfigurationsoptionen von jedem CA Enterprise Log Manager-Server im Netzwerk aus ändern.) Die (agentenlosen) CA Enterprise Log Manager-Quellserver für Protokolldateien werden als untergeordnete Server des Berichtsservers konfiguriert, so dass Abfragen und Berichte die neuesten Daten enthalten.

Hinweis: Falls Sie bereits über einen CA EEM-Server verfügen, der mit CA Enterprise Log Manager verwendet werden soll, konfigurieren Sie die CA Enterprise Log Manager-Server auf dieselbe Weise. Die Konfigurationen werden auf dem dafür vorgesehenen CA EEM-Remote-Server gespeichert.

Ferner haben Sie die Möglichkeit, lokale Konfigurationsoptionen festzulegen, die die globalen Konfigurationen außer Kraft setzen. So können bestimmte CA Enterprise Log Manager-Server anders arbeiten als die übrigen Server. Beispiele hierfür wären das Senden von E-Mail-Berichten und Alarmen über einen eigenen Mailserver oder die Planung von Berichten für einen spezifischen Zweig des Netzwerks zu individuellen Zeiten.

Weitere Informationen

Hierarchischer Verbund (siehe Seite 212)
Netzverbund (siehe Seite 214)
Abfragen und Berichte in einer föderierten Umgebung (siehe Seite 211)
Konfigurieren einer CA Enterprise Log Manager-Föderation (siehe Seite 215)

Erstellen einer Föderationsübersicht

Das Erstellen einer Föderationsübersicht ist ein nützlicher Schritt bei der Planung und Implementierung Ihrer Föderationskonfiguration. Je größer das Netzwerk, desto hilfreicher ist diese Übersicht beim Durchführen der eigentlichen Konfigurationsaufgaben. Sie können die Übersicht in einem kommerziellen Grafik- oder Zeichenprogramm erstellen oder per Hand skizzieren. Je mehr Details Sie in der Übersicht bereitstellen, desto schneller geht die Konfiguration vonstatten.

So erstellen Sie eine Föderationsübersicht:

1. Beginnen Sie die Übersicht mit den beiden grundlegenden CA Enterprise Log Manager-Servern, dem Verwaltungs- und dem (agentenlosen) Quellserver, und stellen Sie Detailinformationen zu beiden Servern zur Verfügung.
2. Überlegen Sie, ob Sie weitere (agentenlose) Quellserver für Protokolldateien benötigen und ob diese in einer Hierarchie ganz oben stehen oder eine Einheit in einem Netzverbund bilden sollen.
3. Überlegen Sie, ob für Ihre Anforderungen ein hierarchischer Verbund oder ein Netzverbund (Verbund steht synonym für Föderation) geeignet ist.
4. Identifizieren Sie Möglichkeiten für Hierarchien, Zweige oder gegenseitige Verbindungen anhand Ihrer Anforderungen an Geschäftsberichte, Compliance und Ereignismengen.

   Falls Ihr Unternehmen beispielsweise über Niederlassungen auf drei Kontinenten verfügt, sind unter Umständen drei hierarchische Verbunde am besten geeignet. Ferner können Sie die Hierarchien auf einer der oberen Ebenen miteinander vernetzen, so dass die Geschäftsleitung und die Sicherheitsverantwortlichen Berichte für das gesamte Netzwerk erstellen können. Zumindest sollten die grundlegenden CA Enterprise Log Manager-Einfüge- und -Abfrageserver der Umgebung miteinander föderiert werden.
5. Überlegen Sie, wie viele CA Enterprise Log Manager-Server Sie insgesamt bereitstellen müssen.

   Die Anzahl ist abhängig von der Anzahl der Geräte in Ihrem Netzwerk und der von diesen Geräten erzeugten Menge an Ereignissen.

6. Überlegen Sie, wie viele Ebenen an föderierten Servern Sie benötigen.

   Diese Anzahl ist teilweise abhängig von den in Schritt 2 und 3 gefällten Entscheidungen.

7. Identifizieren Sie die Ereignistypen, die auf den jeweiligen CA Enterprise Log Manager-Servern im Verbund eintreffen.

   Falls Ihr Netzwerk über eine große Anzahl Syslog-basierter Geräte und nur wenige Windows-Server verfügt, können Sie ggf. CA Enterprise Log Manager-Server nur für die Windows-Ereigniserfassung einrichten. Für die Verarbeitung der Syslog-Daten dagegen sind eventuell mehrere Server erforderlich. Wenn Sie im Voraus planen, auf welchen CA Enterprise Log Manager-Servern welche Arten von Ereignissen eingehen, lassen sich die lokalen Listener und Services einfacher konfigurieren.

8. Skizzieren Sie eine Übersicht dieses Netzwerks, die Sie bei der Konfiguration der föderierten (untergeordneten) CA Enterprise Log Manager-Server heranziehen können.

   Die Übersicht sollte auch die DNS-Namen und IP-Adressen enthalten, sofern bekannt. Die DNS-Namen der CA Enterprise Log Manager-Server werden bei der Konfiguration der Beziehungen zwischen den Servern verwendet.

Beispiel: Föderationsübersicht für ein großes Unternehmen

Wenn Sie eine Föderationsübersicht erstellen, müssen Sie überlegen, welche Arten von Berichten mit welchen Gruppen von konsolidierten Daten erstellt werden sollen. Nehmen Sie beispielsweise ein Szenario, in dem konsolidierte Daten mit drei Arten von Servergruppierungen erstellt werden sollen:

- Alle Server

  Wenn Sie in Systemberichte über selbstüberwachende Ereignisse alle Server einbeziehen, können Sie den Zustand Ihres gesamten CA Enterprise Log Manager-Servernetzwerks auf einmal analysieren.

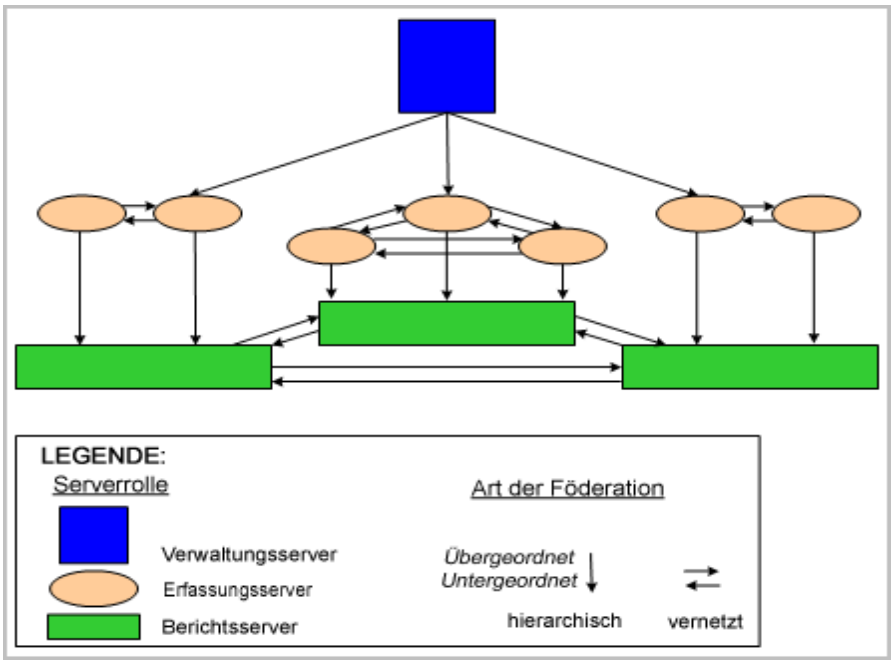
- Alle Berichtsserver

  Falls Sie zusammenfassende Berichte oder Trendberichte wünschen, mit denen Sie die Daten untersuchen können, die von allen Agenten an alle Quellserver gesendet wurden, ohne dass die Quellserver dabei Abfragen zu neuen, aktuellen Ereignissen verarbeiten müssen, müssen Sie föderierte Berichte erstellen, in die nur Berichtsserver einbezogen werden.

- Eine Gruppe von Quellservern mit zugehörigem Berichtsserver

  Falls Sie Berichte wünschen, deren Daten sich auf einen Standort mit einem Berichtsserver beschränken, die allerdings auch Ereignisse beinhalten, die noch nicht von den Quellservern an diesen Server gesendet wurden, müssen Sie föderierte Berichte für diese Untergruppe von Servern ausführen.

Im Folgenden finden Sie ein Beispiel für eine Föderationsübersicht, mit der Sie diese Berichtsziele erreichen können:



Zum Implementieren dieser Föderationsübersicht sind folgende Schritte erforderlich:

- Erstellen eines hierarchischen Verbunds (Föderation) vom Verwaltungsserver zu einem (agentenlosen) Quellserver für Protokolldateien mit einer Beziehung zu jedem Berichtsserver, wobei der Verwaltungsserver der übergeordnete Server ist und alle Quellserver untergeordnete Server sind
- Erstellen eines vollständigen Netzverbunds zwischen den Quellservern für jeden Berichtsserver
- Erstellen eines hierarchischen Verbunds von den einzelnen Quellservern zum jeweiligen Berichtsserver, wobei der Quellserver der übergeordnete und der Berichtsserver der untergeordnete Server ist
- Erstellen eines vollständigen Netzverbunds zwischen den Berichtsservern

Damit ein bestimmtes Berichtsziel erreicht werden kann, muss der Bericht unbedingt auf einem Server ausgeführt werden, der in der Föderationsübersicht eine bestimmte Position einnimmt. Beispiele:

- Um einen Systembericht über selbstüberwachende Ereignisse auf jedem CA Enterprise Log Manager-Server im Netzwerk zu erstellen, führen Sie den Bericht auf dem Verwaltungsserver aus.
- Um zusammenfassende Berichte oder Trendberichte für alle Berichtsserver im Netzwerk zu erstellen, führen Sie den Bericht auf einem der Berichtsserver aus.
- Um einen Bericht zu Daten auf einem Berichtsserver und den zugehörigen Quellservern zu erstellen, führen Sie den Bericht auf einem der Quellserver aus.

Beispiel: Föderationsübersicht für ein mittelgroßes Unternehmen

Legen Sie vor dem Erstellen der Föderationsübersicht die Anzahl der Server fest, die Sie den einzelnen Serverrollen zuweisen möchten. Im folgenden Beispiel dient ein Server für Verwaltungs- und Berichtszwecke, und die verbleibenden Server dienen der Erfassung. Wir empfehlen diese Konfiguration für Umgebungen mittlerer Größe. Sie können die Architektur des Verwaltungs-/Berichtsservers und des Quellservers als Hub-and-Spoke betrachten, wobei der Verwaltungs-/Berichtsserver der Hub ist. Die Föderationsübersicht spiegelt diese Konfiguration nicht. Sie zeigt stattdessen die Ebenen an, so dass Sie hierarchisch föderierte Paare leicht von den vernetzten unterscheiden können.

Wenn Sie eine Föderationsübersicht erstellen, müssen Sie überlegen, welche Berichte und Warnungen mit welchen Gruppen von konsolidierten Daten erstellt werden sollen. Nehmen Sie beispielsweise ein Szenario, in dem konsolidierte Daten mit zwei Arten von Servergruppierungen erstellt werden sollen:

- Nur der Verwaltungs-/Berichtsserver

  Für die meisten Berichte, in denen Sie kürzlich archivierte (warme) Ereignisse untersuchen möchten, ohne dass die Quellserver dabei Abfragen zu neuen, aktuellen Ereignissen verarbeiten müssen.

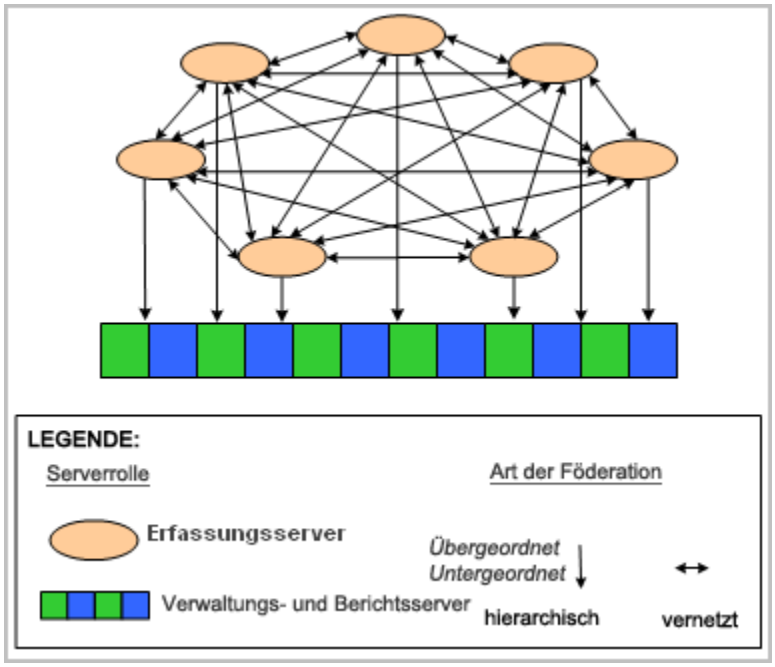
  Hinweis: Ereignisse werden in der Regel stündlich von Quellservern (Spokes) zum Berichtsserver (Hub) archiviert.

- Alle Server

  Für Systemberichte über selbstüberwachende Ereignisse, in denen Sie den Zustand Ihrer gesamten CA Enterprise Log Manager-Server auf einmal analysieren

  Für Warnungen, bei denen es wichtig ist, neue Ereignisse bei allen Quellservern abzufragen

Im Folgenden finden Sie ein Beispiel für eine Föderationsübersicht, mit der Sie diese Berichtsziele erreichen können:



Zum Implementieren dieser Föderationsübersicht sind folgende Schritte erforderlich:

- Erstellen eines vollständigen Netzverbunds zwischen den Quellservern. (Jeder Quellserver ist jedem anderen Quellserver sowohl über- als auch untergeordnet.)
- Erstellen eines hierarchischen Verbunds von den einzelnen Quellservern zum Verwaltungs-/Berichtsserver, wobei der Quellserver der übergeordnete und der Verwaltungs-/Berichtsserver der untergeordnete Server ist.

Damit ein bestimmtes Ziel erreicht werden kann, muss der Bericht oder die Warnung unbedingt auf einem Server ausgeführt werden, der in der Föderationsübersicht eine bestimmte Position einnimmt, und der Grund für die Föderation muss richtig angegeben sein. Beispiele:

- Um einen Systembericht über selbstüberwachende Ereignisse auf jedem CA Enterprise Log Manager-Server in Ihrem Netzwerk zu planen, führen Sie den Bericht auf dem Verwaltungs-/Berichtsserver aus, und geben Sie föderiert an.
- Um einen Bericht zu kürzlichen (warmen) Ereignissen zu planen, führen Sie den Bericht auf dem Verwaltungs-/Berichtsserver aus, und löschen Sie die Föderationsanforderung. Ein solcher Bericht enthält kürzlich archivierte Daten, die von allen Quellservern erfasst wurden. Es wird keine Föderation benötigt.

- Für die Planung von Warnungen, die neue, aktuelle Ereignisse der einzelnen Quellserver sowie archivierte (warme) Ereignisse des Verwaltungs-/Berichtsservers enthalten, führen Sie die Warnung von einem beliebigen Quellserver aus, und geben Sie föderiert an. Sie können einschränken, was an die Quellserver zurückgegeben wird, indem Sie den innerhalb der letzten Stunde vordefinierten Bereich als Ergebnisbedingung angeben.

Weitere Informationen

Konfigurieren eines CA Enterprise Log Manager-Servers als untergeordneter Server (siehe Seite 216)
Serverrollen (siehe Seite 20)
Beispiel: Automatische Archivierung über drei Server hinweg (siehe Seite 164)

Benutzer- und Zugriffsplanung

Nachdem Sie den ersten CA Enterprise Log Manager-Server installiert und sich bei diesem Server als "EiamAdmin"-Benutzer angemeldet haben, können Sie den Benutzerspeicher einrichten, einen Benutzer als Administrator konfigurieren und Kennwortrichtlinien festlegen.

Die Benutzer- und Zugriffsplanung beschränkt sich auf folgende Punkte:

- Überlegen Sie, ob Sie den standardmäßigen Benutzerspeicher auf diesem CA Enterprise Log Manager-Server übernehmen oder einen externen Benutzerspeicher konfigurieren möchten. Falls eine Konfiguration erforderlich ist, notieren Sie sich die entsprechenden Werte in den bereitstehenden Arbeitsblättern.
- Bestimmen Sie den Benutzer, der als erster Administrator fungieren soll. Die CA Enterprise Log Manager-Einstellungen können nur von einem Administrator konfiguriert werden.
- Definieren Sie Kennwortrichtlinien mit dem Ziel, dass starke Kennwörter für CA Enterprise Log Manager-Benutzer verwendet werden.

  Hinweis: Sie können Kennwortrichtlinien nur dann konfigurieren, wenn Sie den Benutzerspeicher als Benutzerspeicher auf diesem CA Enterprise Log Manager-Server einrichten.

Weitere Informationen

Arbeitsblatt für ein externes LDAP-Verzeichnis (siehe Seite 41)
Arbeitsblatt für CA SiteMinder (siehe Seite 43)

Planen des Benutzerspeichers

Melden Sie sich nach der Installation des ersten CA Enterprise Log Manager-Servers bei CA Enterprise Log Manager an, und konfigurieren Sie den Benutzerspeicher. Im konfigurierten Benutzerspeicher werden Benutzernamen und Kennwörter für die Authentifizierung sowie weitere globale Informationen gespeichert.

Bei allen Optionen des Benutzerspeichers werden die Anwendungsbenutzerdaten im CA Enterprise Log Manager-Benutzerspeicher gespeichert. Hierzu gehören Informationen wie Rollen, Benutzerfavoriten und Zeitpunkt der letzten Anmeldung.

Bedenken Sie bei der Planung des zu konfigurierenden Benutzerspeichers folgende Punkte:

- Verwendung des CA Enterprise Log Manager-Benutzerspeichers (Standard)

  Benutzer werden über die in CA Enterprise Log Manager erstellten Benutzernamen und Kennwörter authentifiziert. Sie legen Kennwortrichtlinien fest. Benutzer können ihre eigenen Kennwörter ändern und andere Benutzerkonten freigeben.

- Verweis aus CA SiteMinder

  Benutzernamen, Kennwörter und globale Gruppen werden aus CA SiteMinder in den CA Enterprise Log Manager-Benutzerspeicher geladen. Benutzer werden über die referenzierten Benutzernamen und Kennwörter authentifiziert. Sie können die globale Gruppe einer neuen oder bestehenden Richtlinie zuweisen. Sie können keine neuen Benutzer erstellen, keine Kennwörter ändern und keine Kennwortrichtlinien konfigurieren.

- Verweis aus dem LDAP-Verzeichnis (LDAP = Lightweight Directory Access Protocol)

  Benutzernamen und Kennwörter werden aus dem LDAP-Verzeichnis in den CA Enterprise Log Manager-Benutzerspeicher geladen. Benutzer werden über die referenzierten Benutzernamen und Kennwörter authentifiziert. Die geladenen Benutzerkontodaten werden zu globalen Benutzerkonten. Sie können den globalen Benutzern eine Benutzerrolle zuweisen, die den gewünschten Zugriffsrechten in CA Enterprise Log Manager entspricht. Sie können keine neuen Benutzer erstellen und keine Kennwortrichtlinien konfigurieren.

Wichtig! Sichern Sie möglichst die mit CA Enterprise Log Manager bereitgestellten vordefinierten Zugriffsrichtlinien, bevor Sie oder ein Administrator damit arbeiten. Weitere Informationen finden Sie im *CA Enterprise Log Manager-Administrationshandbuch*.

Weitere Informationen

Übernehmen des Standardbenutzerspeichers (siehe Seite 132)
Verweisen auf ein LDAP-Verzeichnis (siehe Seite 133)
Verweisen auf CA SiteMinder als Benutzerspeicher (siehe Seite 135)

Arbeitsblatt für ein externes LDAP-Verzeichnis

Notieren Sie sich die folgenden Konfigurationsinformationen, bevor Sie auf ein externes LDAP-Verzeichnis verweisen:

Erforderliche Informationen	Wert	Anmerkungen
Type (Typ)		Notieren Sie sich die Art des verwendeten Verzeichnisses. CA Enterprise Log Manager unterstützt verschiedene Verzeichnisse wie Microsoft Active Directory und Sun ONE Directory. Eine vollständige Liste der unterstützten Verzeichnisse finden Sie auf der Benutzeroberfläche.
Host		Notieren Sie sich den Hostnamen des Servers für den externen Benutzerspeicher bzw. das externe Verzeichnis.
Port		Notieren Sie sich die Nummer des Ports, der vom Server des externen Benutzerspeichers bzw. Verzeichnisses überwacht wird. Port 389 ist der Standardport für LDAP (Lightweight Directory Access Protocol). Falls Ihr Registrierungsserver nicht Port 389 verwendet, notieren Sie sich die richtige Portnummer.
Base DN (Basis-DN)		Notieren Sie sich den definierten LDAP-Namen (DN, auch als Distinguished Name bezeichnet), der als Basis verwendet wird. Der DN ist eine eindeutige Kennung für einen Eintrag in einer LDAP-Verzeichnisstruktur. Im Basis-DN dürfen keine Leerzeichen enthalten sein. Nur die unter diesem DN erkannten globalen Benutzer und Gruppen werden zugeordnet und können einer CA Enterprise Log Manager-Anwendungsgruppe oder -Rolle zugewiesen werden.
Password (Kennwort)		Geben Sie das Kennwort für den in der Zeile "User DN" (Benutzer-DN) aufgeführten Benutzer ein, und bestätigen Sie das Kennwort.

Erforderliche Informationen	Wert	Anmerkungen
User DN (Benutzer-DN)		Geben Sie die gültigen Benutzeranmeldeinformationen für alle gültigen Benutzer in der Benutzerregistrierung an, deren Datensatz durchsucht werden kann. Geben Sie den vollständigen definierten Namen (DN) des Benutzers ein. Sie können sich unter jeder Benutzer-ID anmelden, die eine Verwaltungsrolle aufweist. Der "User DN" und das zugehörige Kennwort werden für die Verknüpfung mit dem externen Verzeichnishost verwendet.
Use Transport Layer Security (TLS) (TLS verwenden)		Legt fest, ob der Benutzerspeicher das TLS-Framework als Schutz gegen Klartextübertragungen (d. h. unverschlüsselte Übertragungen) verwendet. Wenn diese Einstellung aktiviert ist, wird beim Herstellen der LDAP-Verbindung zum externen Verzeichnis TLS verwendet.
Include Unmapped Attributes (Nicht zugeordnete Attribute einbeziehen)		Legt fest, ob Felder einbezogen werden sollen, die nicht über das LDAP-Verzeichnis synchronisiert werden. Externe, nicht zugeordnete Attribute können für Suchanfragen und als Filter verwendet werden.
Cache Global Users (Globale Benutzer im Cache speichern)		Legt fest, ob globale Benutzer für einen schnellen Zugriff im Cache gespeichert werden. Die Verwendung dieser Option beschleunigt die Suche auf Kosten der Skalierbarkeit. In einer kleinen Testumgebung wird die Auswahl dieser Einstellung empfohlen.
Cache Update Time (Aktualisierungszeit für Cache)		Falls Sie die Cache-Speicherung globaler Benutzer verwenden, legen Sie (in Minuten) fest, wie oft die globalen Gruppen und Benutzer im Cache aktualisiert werden sollen, damit neue und geänderte Datensätze aufgenommen werden können.
Retrieve Exchange Groups as Global User Groups (Exchange-Gruppen als globale Benutzergruppen abrufen)		Falls es sich bei dem externen Verzeichnis um Microsoft Active Directory handelt, wird mit dieser Option festgelegt, dass globale Gruppen anhand der Microsoft Exchange-Gruppeninformationen erstellt werden. Wenn Sie diese Option aktivieren, können Sie Richtlinien gegen Mitglieder von Verteilerlisten erstellen.

Arbeitsblatt für CA SiteMinder

Notieren Sie sich die folgenden Konfigurationsinformationen, bevor Sie auf CA SiteMinder als Benutzerspeicher verweisen:

Erforderliche Informationen	Wert	Anmerkungen
Host		Gibt den Hostnamen oder die IP-Adresse des referenzierten CA SiteMinder-Systems an. Sie können IPv4- oder IPv6-IP-Adressen verwenden.
Admin Name (Administratorname)		Der Benutzername des CA SiteMinder-Superusers, der System- und Domänenobjekte verwaltet.
Admin Password (Administratorkennwort)		Das Kennwort für den zugehörigen Benutzernamen.
Agent Name (Agentenname)		Der Name des dem Richtlinienserver bereitgestellten Agenten. Bei diesem Namen wird nicht zwischen Groß- und Kleinschreibung unterschieden.
Agent Secret (Agentengeheimnis)		Das für CA SiteMinder definierte "shared secret". Beim Agent Secret wird zwischen Groß- und Kleinschreibung unterschieden.
Cache Global Users (Globale Benutzer im Cache speichern)		Legt fest, ob globale Benutzer für einen schnellen Zugriff im Cache gespeichert werden. Die Verwendung dieser Option beschleunigt die Suche auf Kosten der Skalierbarkeit. **Hinweis:** Globale Benutzer*gruppen* werden immer im Cache gespeichert.
Cache Update Time (Aktualisierungszeit des Cache)		Das Intervall in Minuten, nach dem der Benutzercache automatisch aktualisiert wird.
Include Unmapped Attributes (Nicht zugeordnete Attribute einbeziehen)		Legt fest, ob externe, nicht zugeordnete Attribute für die Verwendung als Filter oder in Suchabfragen einbezogen werden sollen.
Retrieve Exchange Groups as Global User Groups (Exchange-Gruppen als globale Benutzergruppen abrufen)		Falls es sich bei dem externen Verzeichnis um Microsoft Active Directory handelt, wird mit dieser Option festgelegt, dass globale Gruppen anhand der Microsoft Exchange-Gruppeninformationen erstellt werden. Wenn Sie diese Option aktivieren, können Sie Richtlinien gegen Mitglieder von Verteilerlisten erstellen.

Erforderliche Informationen	Wert	Anmerkungen
Authorization Store Type (Art des Autorisierungsspeichers)		Legt die Art des verwendeten Benutzerspeichers fest.
Authorization Store Name (Name des Autorisierungsspeichers)		Gibt den zugewiesenen Namen des Benutzerspeichers an, auf den im Feld "Authorization Store Type" verwiesen wird.

Benutzer mit Administratorrolle

Nur Benutzer, denen die Administratorrolle zugewiesen wurde, können CA Enterprise Log Manager-Komponenten konfigurieren.

Nach der Installation des ersten CA Enterprise Log Manager-Server greifen Sie über einen Browser auf CA Enterprise Log Manager zu, melden sich mit Ihren "EiamAdmin"-Anmeldedaten an und konfigurieren den Benutzerspeicher.

Als Nächstes weisen Sie dem Konto des Benutzers, der die Konfiguration vornehmen soll, die Administrator-Anwendungsgruppe zu. Falls Sie den Benutzerspeicher als standardmäßigen CA Enterprise Log Manager-Benutzerspeicher konfiguriert haben, erstellen Sie ein neues Benutzerkonto und weisen diesem die Administratorrolle zu. Falls Sie auf einen externen Benutzerspeicher verwiesen haben, können Sie keine neuen Benutzer erstellen. In diesem Fall suchen Sie nach dem Benutzerdatensatz der Person, die als Administrator fungieren soll, und weisen diesem Benutzerkonto die Administrator-Anwendungsgruppe zu.

Planen der Kennwortrichtlinien

Falls Sie den Standardbenutzerspeicher übernehmen, definieren Sie neue Benutzer und Kennwortrichtlinien für diese Benutzerkonten in CA Enterprise Log Manager. Starke Kennwörter helfen beim Schutz Ihrer Computerressourcen. Durch Kennwortrichtlinien können Sie starke Kennwörter erzwingen und so die Verwendung schwacher Kennwörter verhindern.

Die mit CA Enterprise Log Manager bereitgestellten standardmäßigen Kennwortrichtlinien sind nur eine *einfache* Form des Kennwortschutzes. So können Benutzer bei der Standardrichtlinie beispielsweise ihren Benutzernamen als Kennwort verwenden und Kennwörter freigeben. Kennwörter können zudem eine unbegrenzte Zeit lang verwendet werden und werden bei Anmeldefehlversuchen nicht gesperrt. Die Standardoptionen weisen absichtlich einen sehr niedrigen Grad des Kennwortschutzes auf, damit Sie Ihre eigenen Kennwortrichtlinien festlegen können.

Wichtig! Sie sollten die Standardkennwortrichtlinien an die in Ihrem Unternehmen üblichen Kennwortrestriktionen anpassen. Es wird dringend davon abgeraten, CA Enterprise Log Manager mit den Standardkennwortrichtlinien in einer Produktionsumgebung auszuführen.

Sie können im Rahmen Ihrer individuellen Kennwortrichtlinie diese Aktivitäten unterbinden, die Verwendung von Kennwortmerkmalen wie Länge, Art der verwendeten Zeichen, zeitliche Begrenzung und Wiederverwendung erzwingen und eine Sperrrichtlinie festlegen, die auf einer definierten Anzahl von Anmeldefehlversuchen basiert.

Weitere Informationen

Konfigurieren von Kennwortrichtlinien (siehe Seite 136)

Benutzername als Kennwort

Damit Kennwörter als "stark" (d. h. sicher) gelten, sollten sie im Rahmen der bewährten Vorgehensweisen für die Sicherheit den Benutzernamen weder enthalten noch ihm ähneln. Die Verwendung des Benutzernamens ist jedoch in der Standardkennwortrichtlinie erlaubt. Dies ist zwar beim Festlegen temporärer Kennwörter für neue Benutzer hilfreich, die Einstellung sollte jedoch in Ihrer Kennwortrichtlinie deaktiviert werden. Wenn Sie diese Option deaktivieren, können Benutzer diese Art von schwachen Kennwörtern nicht verwenden.

Kennwortalter und Wiederverwendung von Kennwörtern

Beachten Sie die folgenden Punkte, wenn Sie Richtlinien für das Alter und die Wiederverwendung von Kennwörtern festlegen:

- Mit der Richtlinie für die Wiederverwendung von Kennwörtern können Sie sicherstellen, dass Kennwörter nicht zu oft wiederholt werden. Durch diese Richtlinie wird eine Kennwortübersicht angelegt. Die Einstellung "0" bedeutet, dass keine Kennwortübersicht verwendet wird. Eine Einstellung über "0" legt fest, wie viele Kennwörter gespeichert und zum Vergleich bei einer Kennwortänderung herangezogen werden. Eine Richtlinie für starke Kennwörter sollte dafür sorgen, dass Benutzer ein Kennwort mindestens ein Jahr lang nicht erneut verwenden können.
- Das empfohlene *Höchstalter* für ein Kennwort ist abhängig von seiner Länge und Komplexität. Eine allgemeine Regel ist, dass ein akzeptables Kennwort nicht mittels "roher Gewalt" innerhalb seines zulässigen Höchstalters entschlüsselt werden kann. Eine gute Faustregel für das Höchstalter sind 30 bis 60 Tage.
- Indem Sie ein *Mindestalter* festlegen, können Sie verhindern, dass Benutzer ihr Kennwort innerhalb einer Sitzung viele Male ändern, um Einschränkungen bei der Wiederverwendung von Kennwörtern zu umgehen. Empfohlen werden hier im Allgemeinen drei Tage.

- Falls Sie ein Kennwortalter festlegen, sollten Benutzer darauf aufmerksam gemacht werden, wenn das Kennwort neu festgelegt werden muss. So kann etwa nach Ablauf der halben Zeit oder auch kurz vor Ablauf der Zeit eine Warnmeldung angezeigt werden.
- Benutzerkonten sollten nach einer bestimmten Anzahl von fehlgeschlagenen Anmeldeversuchen gesperrt werden. Hierdurch lässt sich verhindern, dass Hacker ein Kennwort durch Ausprobieren entschlüsseln. Standardmäßig werden Konten nach drei bis fünf Fehlversuchen gesperrt.

Länge und Format von Kennwörtern

Beachten Sie die folgenden Punkte, wenn Sie überlegen, ob Längenbeschränkungen erzwungen werden sollen:

- Aufgrund der Art und Weise, wie Kennwörter verschlüsselt werden, sind die sichersten Kennwörter zwischen sieben und vierzehn Zeichen lang.
- Achten Sie darauf, dass Kennwortbeschränkungen, die durch ein altes Betriebssystem im Netzwerk vorgegeben werden, nicht überschritten werden.

Beachten Sie die folgenden Punkte, wenn Sie überlegen, ob Richtlinien erzwungen werden sollen, gemäß denen eine maximale Anzahl gleicher Zeichen enthalten sein darf oder eine Mindestanzahl von Zahlen bzw. Ziffern enthalten sein muss.

- Starke Kennwörter sind niemals Wörter aus einem Wörterbuch.
- Starke Kennwörter enthalten ein oder mehrere Zeichen aus mindestens drei der folgenden vier Gruppen: Kleinbuchstaben, Großbuchstaben, Ziffern und Sonderzeichen

Planen von automatischen Software-Updates

Die über den CA-Software-Update-Server bereitgestellten Software-Updates sorgen dafür, dass sich Ihre Ausgabe von CA Enterprise Log Manager immer auf dem neuesten Stand befindet. Automatische Software-Updates können eine oder alle der folgenden Komponenten beinhalten:

- Produkt- und Betriebssystemaktualisierungen, die von den CA Enterprise Log Manager-Servern selbst installiert werden

  Hinweis: Sie können bei jeder Update-Runde wählen, welche Produkt- und Betriebssystemaktualisierungen installiert werden.

- Inhalts- und Konfigurationsaktualisierungen wie die folgenden, die auf den Verwaltungsserver übertragen werden:
  - Berichtsabfragen
  - Berichte

  - Datenzuordnungs- und Nachrichtenanalysedateien
  - Listener, Connectors und andere Services
  - Integrationen
  - Konfigurationsaktualisierungen für CA Enterprise Log Manager-Module
  - Updates für öffentliche Schlüssel
- Für die Agenten bestimmte Updates

  Hinweis: Aktualisieren Sie Ihre CA Enterprise Log Manager-Server, bevor Sie die Agenten aktualisieren. CA Enterprise Log Manager-Server unterstützen Agenten für die aktuelle oder unterhalb ihrer aktuellen Versionsnummer. Um die ordnungsgemäße Speicherung der erfassten Ereignisse sicherzustellen, wenn Sie Agenten konfigurieren oder aktualisieren, sollten Sie sich vergewissern, dass der Agent Ereignisse nur an CA Enterprise Log Manager-Server sendet, deren Ebene der des Agenten entspricht oder höher liegt.

Der erste installierte CA Enterprise Log Manager-Server ist der standardmäßige Online-Proxy-Server für automatische Software-Updates (Online-Update-Proxy). Alle nachfolgenden CA Enterprise Log Manager-Server werden als Clients für automatische Software-Updates (Software-Update-Clients) installiert. Gegebenenfalls können Sie jeden beliebigen CA Enterprise Log Manager-Server als *Offline*-Update-Proxy einrichten. Ferner besteht die Möglichkeit, weitere Online-Update-Proxies zu konfigurieren.

Die Planung automatischer Software-Updates beinhaltet Folgendes:

- Prüfen der Notwendigkeit eines HTTP-Proxys
- Prüfen der Notwendigkeit eines Offline-Proxys für automatische Software-Updates (Offline-Update-Proxys)
- Prüfen der Notwendigkeit einer Proxy-Liste

Komponenten und Ports für automatische Software-Updates

Automatische Software-Updates beinhalten folgende Komponenten:

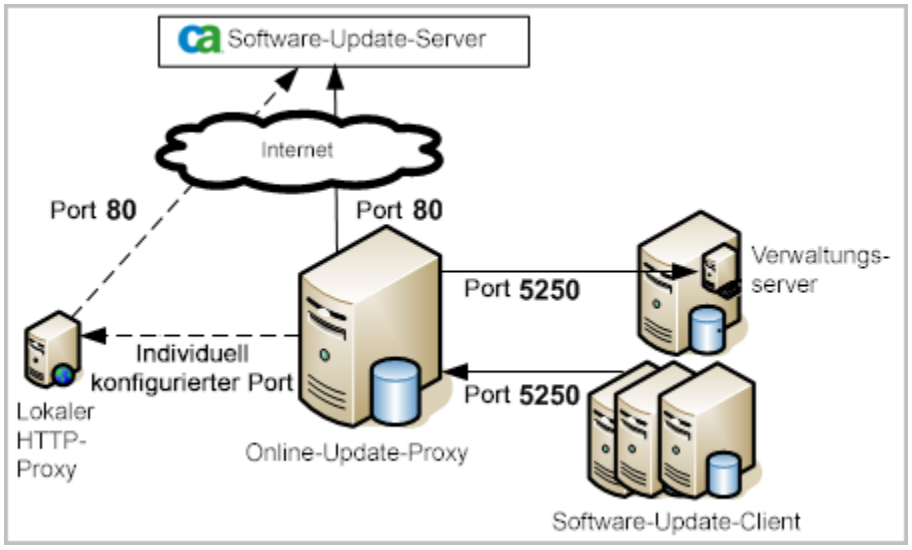
- CA-Software-Update-Server
- (optional) HTTP-Proxy-Server
- Alle CA Enterprise Log Manager-Server, die konfiguriert werden können als:
  - Software-Update-Proxy (online)
  - Software-Update-Client
  - (optional) Offline-Update-Proxy
- Den CA Enterprise Log Manager-Verwaltungsserver, bei dem es sich in der Regel um den CA-Software-Update-Proxy handelt

  Der erste installierte CA Enterprise Log Manager-Server wird normalerweise mit einem lokalen CA EEM installiert und fungiert standardmäßig als CA-Software-Update-Proxy.

CA Enterprise Log Manager verwendet ein Proxysystem, d. h. ein Client- und Serversystem, zur Auslieferung von Inhalts- und Binärdateiaktualisierungen. Der erste installierte CA Enterprise Log Manager-Server wird automatisch als CA-Software-Update-Proxy eingerichtet. Dieser Online-Update-Proxy kontaktiert in regelmäßigen Abständen den CA-Software-Update-Server, um nach Updates zu suchen. Der Kontakt kann direkt oder über einen HTTP-Proxy erfolgen. Standardmäßig sind alle anderen CA Enterprise Log Manager-Server Software-Update-Clients des CA-Software-Update-Proxys. Die Software-Update-Clients kontaktieren den CA-Software-Update-Proxy, um nach Updates zu suchen. Sowohl Clients als auch Proxies installieren die angeforderten Module selbständig.

Der CA Enterprise Log Manager-Benutzerspeicher empfängt Inhalts- und Konfigurationsaktualisierungen und speichert alle Konfigurationen für den Software-Update-Service.

Der für das HTTP-Protokoll bekannte Port 80 wird für Anforderungen verwendet, die über das Internet an den CA-Software-Update-Server gesendet werden. Port 5250 wird für den internen Datenstrom zwischen den CA Enterprise Log Manager-Servern benutzt. Der Port vom Online-Update-Proxy zum HTTP-Proxy wird zusammen mit den anderen HTTP-Proxy-Daten konfiguriert.



Weitere Informationen

Konfigurieren eines Online-Proxy-Servers für automatische Software-Updates (Online-Update-Proxys) (siehe Seite 187)
Standardportzuweisungen (siehe Seite 105)

Zeitpunkt für die Konfiguration automatischer Software-Updates

Konfigurieren Sie die automatischen Software-Updates vorzugsweise erst, nachdem Sie alle gewünschten CA Enterprise Log Manager-Server installiert haben. Falls Sie sofort Software-Updates beziehen möchten, sollten Sie als Aufbewahrungszeit der heruntergeladenen Updates nicht die standardmäßigen 30 Tage verwenden, sondern ein Intervall, das ausreichend Zeit lässt für die Installation und Aktualisierung aller CA Enterprise Log Manager-Server, bevor die erste Bereinigung durchgeführt wird. Alle neuen Server, die als Software-Update-Clients hinzugefügt werden, nachdem eine oder mehrere Bereinigungen durchgeführt wurden, erhalten nicht die vor der Bereinigung verfügbar gemachten Updates. Falls Sie nach einer Bereinigung neue Server installieren, sollten Sie diese als ihre eigenen Software-Update-Proxies einrichten, so dass alle auf dem CA-Software-Update-Server verfügbaren Updates angewendet werden können. Anschließend können Sie die neuen Server als Software-Update-Clients konfigurieren.

Planen des Speicherplatzes

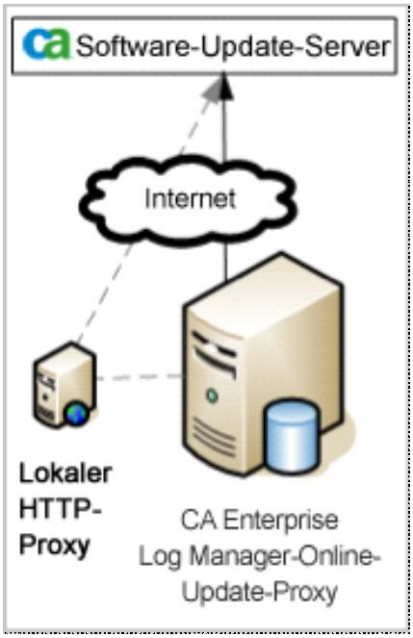
Es ist empfehlenswert, den Speicherplatz regelmäßig zu überprüfen, so dass immer ausreichend freier Platz zum Herunterladen von Software-Updates verfügbar ist. Falls auf einem als Software-Update-Client konfigurierten CA Enterprise Log Manager-Rechner mehr als 90 Prozent des Speicherplatzes belegt sind, wenn das Modul für automatische Software-Updates eine Aktualisierung unternimmt, gibt der Software-Update-Service ein selbstüberwachendes Ereignis aus und unterbricht den Download-Vorgang.

Sie können basierend auf der Abfrage "Wenig Speicherplatz verfügbar" einen Aktionsalarm einplanen.

Hinweis: Ein Beispiel hierfür finden Sie im Abschnitt zu Aktionsalarmen im *CA Enterprise Log Manager-Administrationshandbuch*.

Prüfen der Notwendigkeit eines HTTP-Proxys

Bevor Sie globale Einstellungen für automatische Software-Updates konfigurieren, müssen Sie entscheiden, ob Software-Updates über einen HTTP-Proxy-Server auf das interne Netzwerk heruntergeladen werden. In vielen Unternehmen müssen ausgehende Internetverbindungen über einen HTTP-Proxy-Server stattfinden. Sie legen Anmeldeinformationen für den HTTP-Proxy-Server im Rahmen der Software-Update-Konfiguration fest. Hierdurch kann der Proxy für automatische Software-Updates den HTTP-Proxy umgehen, wenn er nach Updates auf dem CA-Software-Update-Server sucht. Dank der automatischen Umgehung kann die Softwareaktualisierung ohne Anwesenheit eines Benutzers durchgeführt werden.



Falls Sie einen HTTP-Proxy verwenden, sollten Sie sich vor Beginn dieser Konfiguration die IP-Adresse, Portnummer und Anmeldeinformationen notieren.

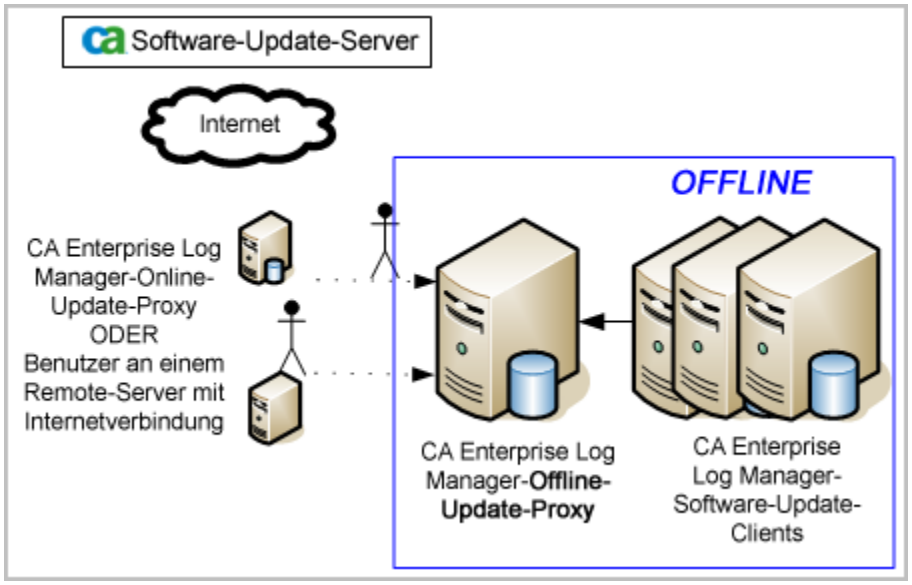
Überprüfen des Zugriffs auf den RSS-Feed für automatische Software-Updates

Überprüfen Sie zu Beginn der Konfiguration der globalen Einstellungen für automatische Software-Updates, ob der CA-Software-Update-Proxy auf die vordefinierte RSS-Feed-URL zugreifen kann. Falls die Liste der verfügbaren herunterzuladenden Module gefüllt ist, war der Zugriff erfolgreich.

Falls der Abschnitt mit den verfügbaren herunterzuladenden Modulen leer ist und sich Ihr Server hinter einer Firewall befindet, müssen Sie die HTTP-Proxy-Einstellungen konfigurieren, so dass Online-Update-Proxies den RSS-Feed kontaktieren können.

Prüfen der Notwendigkeit eines Offline-Proxys für automatische Software-Updates (Offline-Update-Proxys)

Entscheiden Sie vor der Konfiguration der automatischen Software-Updates, ob Sie Offline-Update-Proxies einrichten müssen. Sie benötigen Offline-Update-Proxies, wenn die als Software-Update-Clients konfigurierten CA Enterprise Log Manager-Server aufgrund von Richtlinien, die diesen Servern den Zugriff auf Server mit Internetzugang verwehren, keinen Online-Update-Proxy kontaktieren können. Eventuell wird durch Ihre Richtlinien sogar festgelegt, dass kein CA Enterprise Log Manager-Server als Online-Update-Proxy fungieren darf. In beiden Fällen benötigen Sie einen Offline-Update-Proxy. Der Unterschied zwischen beiden Szenarien liegt darin, wie Software-Updates vom CA-Software-Update-Server abgerufen werden. In einem Fall werden Updates anhand eines Zeitplans von einem Online-Proxy abgerufen. Im anderen Fall werden Updates manuell durch einen Benutzer über einen Remote-Server heruntergeladen.



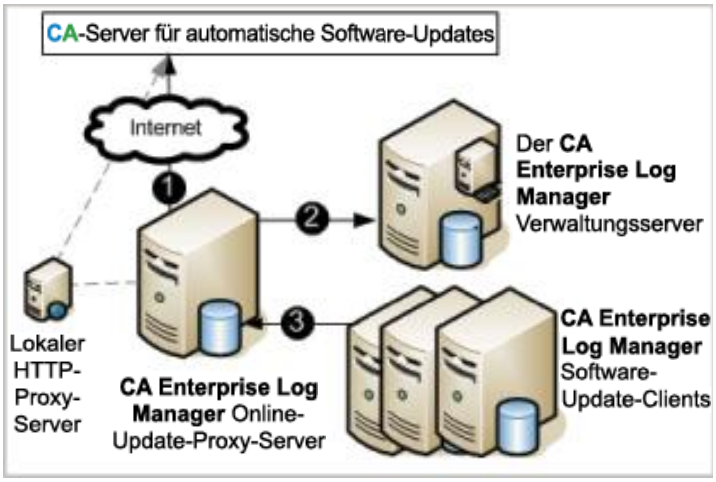
Weitere Informationen

Konfigurieren eines Offline-Proxy-Servers für automatische Software-Updates (Offline-Update-Proxys) (siehe Seite 189)

Automatische Software-Updates mit Online-Clients

Der standardmäßige Online-Update-Proxy und alle weiteren von Ihnen eingerichteten Proxy-Server für automatische Software-Updates empfangen Software-Updates vom CA-Software-Update-Server. Dabei wird der ggf. eingerichtete HTTP-Proxy-Server umgangen.

Die folgende Abbildung zeigt ein einfaches Online-Szenario mit dem CA-Software-Update-Server, dem standardmäßigen Online-Update-Proxy, dem CA Enterprise Log Manager-Verwaltungsserver und einigen Clients für automatische Software-Updates (Software-Update-Clients):



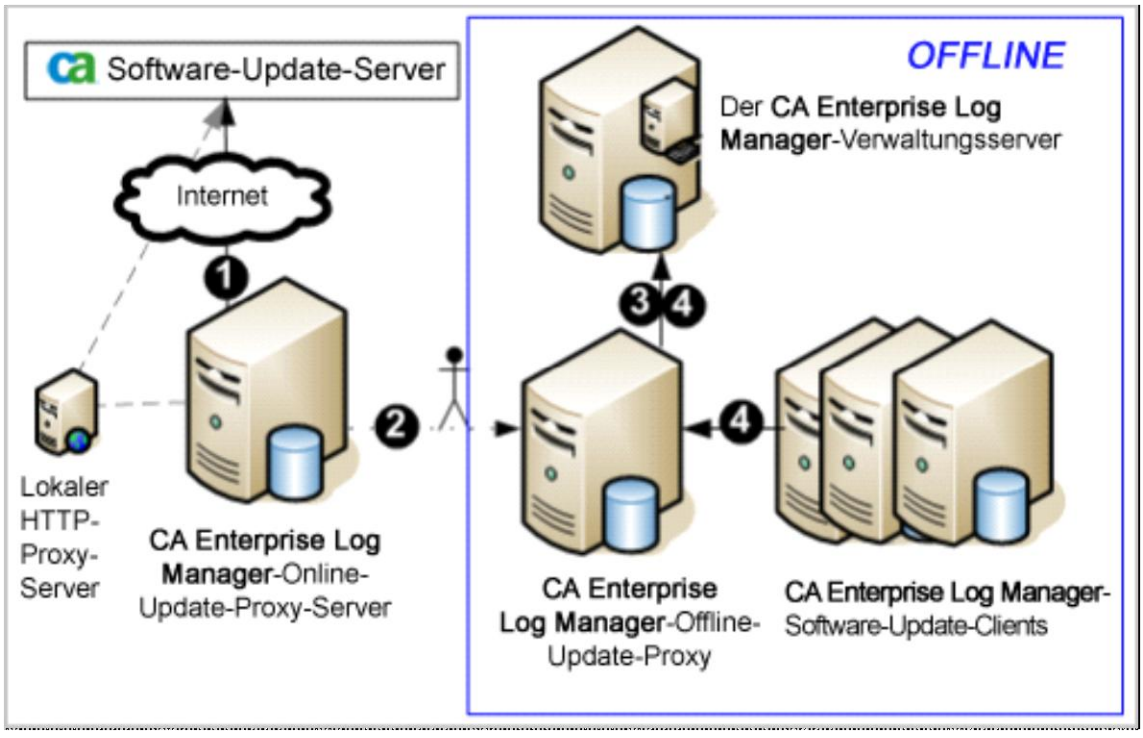
Der Ablauf ist wie folgt (siehe nummerierte Pfeile):

1. Wenn der Administrator am Anfang im Rahmen der globalen Service-Konfiguration das Modul für automatische Software-Updates konfiguriert und die RSS-Feed-URL festlegt, greift der Proxy-Server für automatische Software-Updates über die RSS-Feed-URL auf den CA-Software-Update-Server zu und ruft die Liste der für den Download verfügbaren Module ab. Wenn der Administrator die herunterzuladenden Module auswählt, ermittelt das System, welche Updates noch nicht auf den Online-Proxy heruntergeladen wurden. Der Online-Update-Proxy lädt die neuen Software-Updates (ggf. über einen lokalen HTTP-Proxy-Server) herunter. Zu den Software-Updates gehören Inhaltsaktualisierungen sowie Produkt- und Betriebssystem-Updates.

2. Der Online-Update-Proxy überträgt Inhalts- und Konfigurationsaktualisierungen auf den CA Enterprise Log Manager-Verwaltungsserver, auf dem diese Art von Daten für alle CA Enterprise Log Manager-Server in der Umgebung gespeichert wird.
3. Die Clients für automatische Software-Updates senden Abfragen an den Proxy-Server für automatische Software-Updates. Falls neue Software-Updates verfügbar sind, werden sie von den Software-Update-Clients heruntergeladen. Beim Download-Paket handelt es sich um eine ZIP-Datei mit den Produkt- und Betriebssystem-Updates, einem Installationsskript und der Komponenteninformationsdatei "componentinfo.xml". Falls eine Sicherung erforderlich ist, wird von den Software-Update-Clients eine Sicherung der letzten Installation der Produkt-Updates sowie ein Skript erstellt, mit dem Sie den alten Update-Status wiederherstellen können, falls ein Rollback der Änderungen notwendig wird. (Die Sicherung umfasst keine Betriebssystem-Updates.) Anschließend führen die Software-Update-Clients das Installationsskript aus, mit dem die Produkt-Updates installiert werden.

Automatische Software-Updates mit Offline-Clients

Die folgende Abbildung zeigt ein einfaches Offline-Szenario mit dem CA-Software-Update-Server, dem standardmäßigen Online-Update-Proxy, einem Offline-Update-Proxy, einem Verwaltungsserver mit dem CA Enterprise Log Manager-Benutzerspeicher und einigen Clients für automatische Software-Updates (Software-Update-Clients).

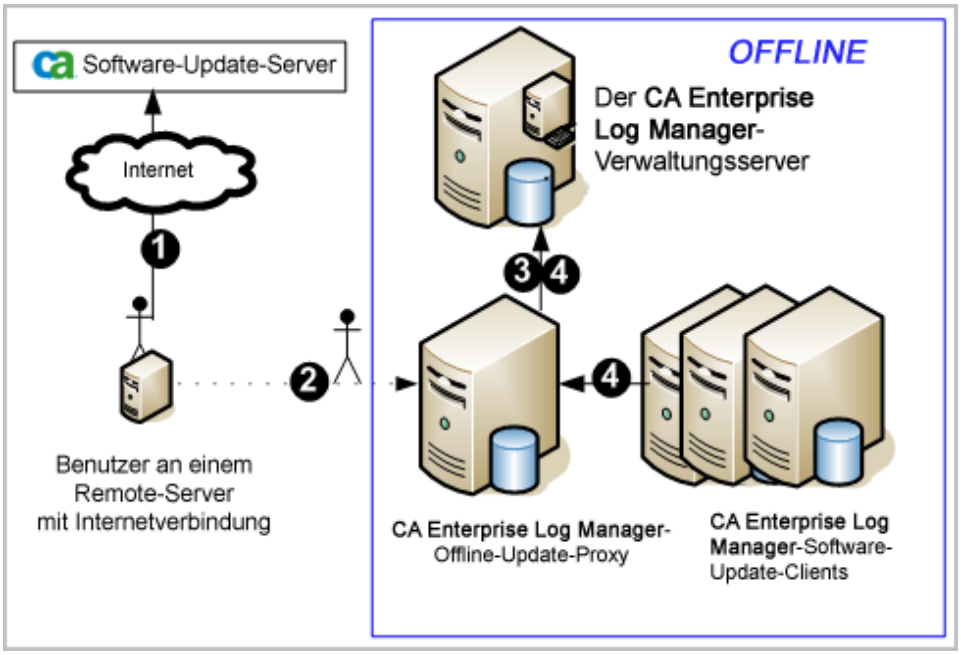


Der Ablauf ist wie folgt (siehe nummerierte Pfeile):

1. Der Online-Update-Proxy greift auf den CA-Software-Update-Server zu und lädt Inhaltsaktualisierungen sowie Produkt- und Betriebssystem-Updates (ggf. über einen lokalen HTTP-Server) herunter. Welche Produkt-Updates heruntergeladen werden, ist abhängig von den ausgewählten herunterzuladenden Modulen. Diese wurden bei der Einrichtung des Moduls für automatische Software-Updates im Rahmen der globalen Service-Konfiguration festgelegt.
2. Sie kopieren alle Elemente im Download-Pfad des Online-Proxys in den Download-Pfad des Offline-Proxys. Für diesen Zweck steht das Hilfsprogramm *scp* (Secure Copy) zur Verfügung. Sie können auch "sftp" verwenden. Zu den kopierten Inhalten gehören Inhaltsaktualisierungen sowie die Binärdateien für Produkt- und Betriebssystem-Updates. Nach dem Kopiervorgang weisen Sie dem "caelmservice"-Benutzer die Eigentümerschaft für die Dateien zu.
3. Der Offline-Update-Proxy überträgt die Inhaltsaktualisierungen auf den CA Enterprise Log Manager-Verwaltungsserver.
4. Die Clients für automatische Software-Updates senden Abfragen an den *Offline*-Proxy-Server für automatische Software-Updates. Falls neue Software-Updates verfügbar sind, werden sie von den Software-Update-Clients heruntergeladen. Beim Download-Paket handelt es sich um eine ZIP-Datei mit den Produkt- und Betriebssystem-Updates, einem Installationsskript und der Komponenteninformationsdatei "componentinfo.xml". Falls eine Sicherung erforderlich ist, wird von den Software-Update-Clients eine Sicherung der letzten Installation der Produkt-Updates sowie ein Skript erstellt, mit dem Sie den alten Update-Status wiederherstellen können, falls ein Rollback der Änderungen notwendig wird. (Die Sicherung umfasst keine Betriebssystem-Updates.) Anschließend führen die Software-Update-Clients das Installationsskript aus, mit dem die Produkt-Updates installiert werden.

Automatische Software-Updates ohne Online-Proxy

Sie können auch ein CA Enterprise Log Manager-System verwenden, in dem kein Server Zugang zum Internet hat. In dieser Ausnahmesituation hat auch der zuerst installierte Server, der automatisch als CA-Software-Update-Proxy (Standard-Proxy für automatische Software-Updates) eingerichtet wird, keinen Online-Zugang. Sie konfigurieren den CA-Software-Update-Proxy als Offline-Proxy. Um Aktualisierungen zu erhalten, müssen Sie manuell auf die angegebene FTP-Seite von CA zugreifen. Diese FTP-Seite enthält einen Ordner für jede größere Version. Ordner für frühere Versionen, wie r12.0, enthalten eine Core-Datei "tar", die die entsprechende Version enthält, Service Packs und alle Aktualisierungen, die im Laufe des Versionszyklus hinzugefügt wurden. Der Ordner für die aktuelle Version enthält eine Core-Datei mit allen Service Packs und zusätzlich eine Datei, die kumulative Inhaltsaktualisierungen und Hotfixes enthält. Sie können die gewünschte Datei mit der Erweiterung "tar" von jedem Server Ihres Netzwerks über FTP herunterladen. Extrahieren Sie die Datei dann im Pfad des Offline-Proxy-Servers. Das Inhalts-Repository und Clients werden wie konfiguriert aktualisiert.



Der Ablauf ist wie folgt (siehe nummerierte Pfeile):

1. Greifen Sie von einem Remote-Server mit einer Internet-Verbindung oder einem FTP-Service auf die FTP-Seite zu, die eine Datei mit der Erweiterung "tar" für jede CA Enterprise Log Manager-Version und alle Service Pack enthält. Öffnen Sie den Ordner für die aktuelle oder gewünschte Version. Laden Sie die Core-Datei "subscription_12.x.x.x.tar" herunter, wenn Sie sie nicht bereits heruntergeladen haben. Wenn Sie diese Datei heruntergeladen haben, laden Sie die zusätzliche Datei herunter.
2. Geben Sie die Aktualisierungen für den Download-Pfad des Offline-Proxys an:
   a. Wenn Sie die Core-Datei mit der Erweiterung "tar" heruntergeladen haben, kopieren Sie diese Datei in das Verzeichnis "/opt/CA/LogManager/data" des Offline-Proxy. Für diesen Zweck steht das Hilfsprogramm scp (Secure Copy) zur Verfügung. Sie können auch "sftp" verwenden.
   b. Benennen Sie das vorhandene Verzeichnis für automatische Software-Updates "subscription.bak"
   c. Entpacken Sie die tar-Datei.

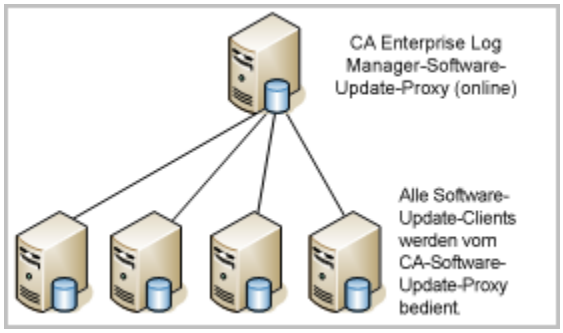
      ```
      tar -xvf subscription_x_x_x_x.tar
      ```

      Die Verzeichnisstruktur von "/opt/CA/LogManager/data/subscription" wird mit den aktuellsten Inhalts- und Binärdateien erstellt. Berechtigungen und Eigentumsrechte werden festgelegt.
   d. Wenn Sie die zusätzliche tar-Datei heruntergeladen haben, kopieren Sie diese Datei in das Verzeichnis "/opt/CA/LogManager/data/subscription" des Offline-Proxy und entpacken Sie die Datei. Damit werden Module und Dateien mit den derzeitigen Versionen aktualisiert.
   e. Starten Sie den iGateway-Service neu.
3. Der Offline-Update-Proxy überträgt die Inhaltsaktualisierungen in das Repository auf dem CA Enterprise Log Manager-Verwaltungsserver.
4. Software-Update-Clients, einschließlich Clients auf Verwaltungsserver und Offline-Proxy, fragen den *Offline*-Proxy-Server für automatische Software-Updates auf Aktualisierungen ab. Falls neue Software-Updates verfügbar sind, werden sie von den Software-Update-Clients heruntergeladen. Beim Download-Paket handelt es sich um eine ZIP-Datei mit den Produkt- und Betriebssystem-Updates, einem Installationsskript und der Komponenteninformationsdatei "componentinfo.xml". Wenn eine Sicherung benötigt wird, erstellen die Software-Update-Clients eine Sicherung der letzten Produktaktualisierungen und erstellen auch ein Skript, das Änderungen zurücksetzen kann. (Die Sicherung umfasst keine Betriebssystem-Updates.) Anschließend führen die Software-Update-Clients das Installationsskript aus, mit dem die Produkt-Updates installiert werden.

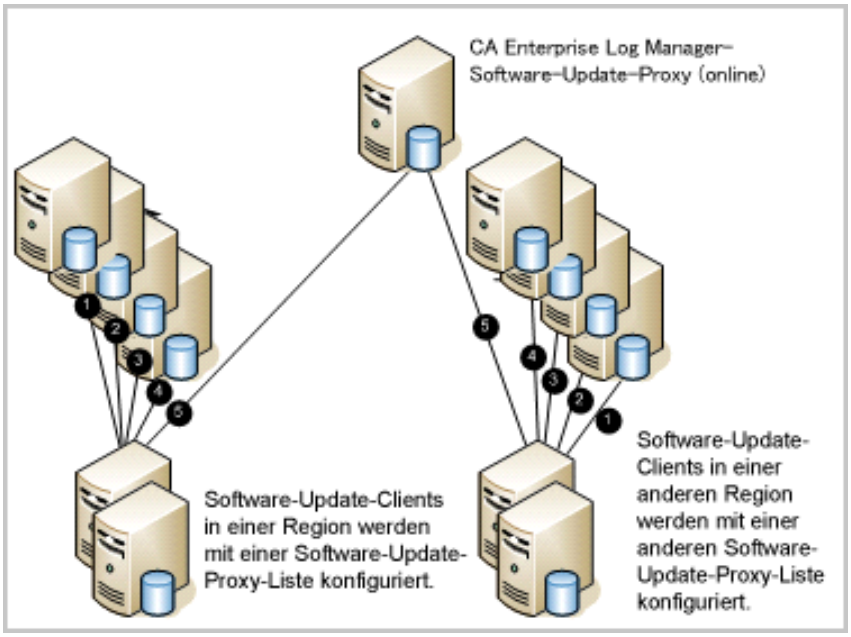
Prüfen der Notwendigkeit einer Proxy-Liste

Legen Sie vor der Konfiguration von Software-Update-Clients die Quelle fest, von der die Software-Update-Clients Inhaltsaktualisierungen abrufen. Software-Update-Clients können Updates direkt vom CA-Software-Update-Proxy abrufen, oder Sie können eine zwischengeschaltete Proxy-Liste für Update-Anforderungen einrichten.

- Für Unternehmen mit wenigen CA Enterprise Log Manager-Servern, die sich in der Nähe des Netzwerks befinden, wird empfohlen, dass alle Software-Update-Clients den CA-Software-Update-Proxy verwenden.



- Für Unternehmen mit einer großen Anzahl von CA Enterprise Log Manager-Servern bzw. weit verteilten CA Enterprise Log Manager-Servern wird die Konfiguration einer Liste mit Software-Update-Proxies für jeden Software-Update-Client empfohlen. Wenn eine Proxy-Liste eingerichtet wurde, kontaktiert jeder Client nacheinander die einzelnen Mitgliedsserver auf der Proxy-Liste. Nur wenn keiner dieser Server erreichbar ist, wird der CA-Software-Update-Proxy kontaktiert.



Beispiel: Konfiguration für automatische Software-Updates mit sechs Servern

Wenn Sie die Konfiguration der automatischen Software-Updates in Angriff nehmen, überlegen Sie, welche anderen Rollen die Server erfüllen, bevor sie deren Rolle im Rahmen der Software-Updates festlegen. Standardmäßig fungiert der Verwaltungsserver, d. h. der erste installierte Server, als Standard-Proxy für automatische Software-Updates (CA-Software-Update-Proxy). Alle anderen Server sind Software-Update-Clients des CA-Software-Update-Proxys. Diese Konfiguration ist zwar akzeptabel, empfehlenswerter ist allerdings die Konfiguration eines Online-Update-Proxys. In diesem Fall fungiert der Standard-Proxy-Server als Failover-Proxy bzw. redundanter Proxy. Weisen Sie die Rolle des Online-Proxys vorzugsweise dem Server mit der geringsten Auslastung zu.

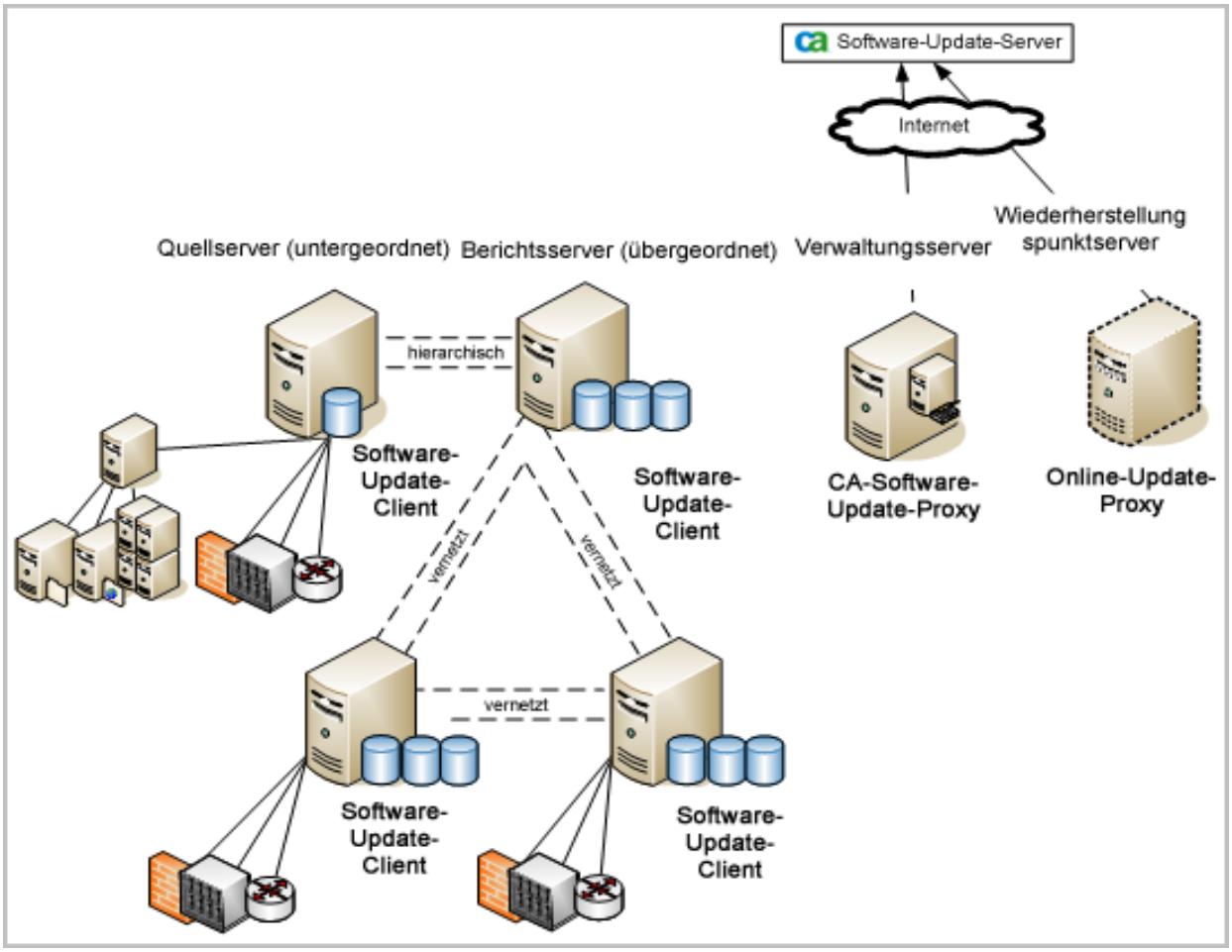
Beispiel: Sechs Server, bei denen der Online-Update-Proxy der am wenigsten ausgelastete Server ist

Das folgende Szenario besteht aus sechs CA Enterprise Log Manager-Servern. Der Verwaltungsserver dient der Authentifizierung und Autorisierung von Benutzern bei der Anmeldung und der Speicherung von Anwendungsinhalten. Vier föderierte Server übernehmen die Ereignisverarbeitung und Berichterstellung. Der sechste Server ist ein eigens dafür eingerichteter Wiederherstellungspunkt für die Überprüfung von Ereignissen aus wiederhergestellten Datenbanken. Der Vorteil eines eigenen Wiederherstellungspunkts ist, dass Sie alte Daten von aktuellen Berichten ausschließen können, indem Sie diesen Server nicht in die Föderation (den Verbund) aufnehmen.

In diesem Beispiel stellen die beiden als Quellserver für Protokolldateien und Berichtsserver ausgewiesenen Server eine Konfiguration mit extrem hohen Verarbeitungsanforderungen dar. Diese Server befinden sich in einem hierarchischen Verbund, in dem der Quellserver dem Berichtsserver untergeordnet ist. Die beiden Server, die sowohl als Quellserver als auch als Berichtsserver fungieren, stellen eine Konfiguration mit normalen Ereignisvolumen und geplanten Berichten dar. Diese Server befinden sich untereinander und mit dem ausgewiesenen Berichtsserver in einem Netzverbund, das heißt, dass diese drei Server gleichrangig sind. Das Ziel eines Serververbunds (Föderation) ist, dass Sie umfassendere Abfrageergebnisse von den föderierten Servern erhalten können. Eine föderierte Abfrage auf einem der Server im Netzverbund erbringt Ereignisse von diesem Server und den übrigen Servern im Verbund.

Hinweis: Falls Sie konsolidierte Berichte über selbstüberwachende Ereignisse erstellen möchten, nehmen Sie den Verwaltungsserver in die Föderation auf.

In diesem Szenario ist es empfehlenswert, den Wiederherstellungspunkt als Online-Update-Proxy einzurichten, da es sich hierbei um den Server mit der geringsten Auslastung handelt. Konfigurieren Sie dann alle Clients so, dass sie auf diesen Online-Proxy zeigen, damit der Standard-Proxy-Server (CA-Software-Update-Proxy) als Backup-Server fungieren kann, sollte der Online-Proxy belegt oder nicht verfügbar sein.



Weitere Informationen

Konfigurieren einer CA Enterprise Log Manager-Föderation (siehe Seite 215)
Konfigurieren von CA Enterprise Log Manager-Servern für automatische Software-Updates (siehe Seite 187)
Serverrollen (siehe Seite 20)

Agentenplanung

Agenten verwenden Connectors, um Ereignisse zu erfassen und auf den CA Enterprise Log Manager-Server zu übertragen. Sie können einen Connector auf dem mit dem CA Enterprise Log Manager-Server installierten Standardagenten konfigurieren, oder Sie können einen Agenten auf einem Server bzw. einer Ereignisquelle im Netzwerk installieren. Die Entscheidung, ob externe Agenten verwendet werden, basiert auf dem Ereignisvolumen, dem Agentenstandort, der Notwendigkeit zum Filtern von Daten und anderen Aspekten. Die Planung der Agenteninstallation beinhaltet Folgendes:

- Kenntnisse der Beziehungen zwischen folgenden Komponenten:
  - Integrationen und Listener
  - Agenten
  - Connectors
- Bestimmen der Netzwerkgröße als Entscheidungspunkt für die Anzahl der zu installierenden Agenten

Installieren Sie die Agenten relativ nahe bei den Ereignisquellen, deren Ereignisprotokolle erfasst werden sollen. Die meisten Connectors erfassen nur die Ereignisse einer einzigen Ereignisquelle. Bei Syslog-Ereignissen kann ein einzelner Syslog-Listener Ereignisse aus mehreren Arten von Ereignisquellen empfangen. Ein Agent kann den Ereignisstrom von mehreren Connectors steuern und verarbeiten.

Wissenswertes über die Syslog-Ereigniserfassung

CA Enterprise Log Manager kann Ereignisse direkt von Syslog-Quellen empfangen. Die Syslog-Erfassung unterscheidet sich von anderen Erfassungsmethoden, da mehrere unterschiedliche Ereignisquellen gleichzeitig Ereignisse an CA Enterprise Log Manager senden können. Netzwerk-Router und VPN-Concentrators sind zwei mögliche Ereignisquellen. Beide können über Syslog Ereignisse direkt an CA Enterprise Log Manager senden, das Protokollformat und die Protokollstruktur sind allerdings unterschiedlich. Ein Syslog-Agent kann beide Arten von Ereignissen gleichzeitig über den bereitgestellten Syslog-Listener empfangen.

Allgemein kann die Ereigniserfassung in zwei Kategorien unterteilt werden:

- CA Enterprise Log Manager *sucht* auf konfigurierbaren Ports nach Syslog-Ereignissen.
- CA Enterprise Log Manager *überwacht* andere Ereignisquellen auf Ereignisse, beispielsweise mittels WMI zum Erfassen von Windows-Ereignissen.

Mehrere Syslog-Ereignisquellen können Ereignisse über einen einzelnen Connector senden, da der Listener den gesamten Datenverkehr auf dem angegebenen Port empfängt. CA Enterprise Log Manager kann auf jedem Port nach Syslog-Ereignissen suchen. (Falls Sie einen Agenten unter einem Nicht-Root-Benutzer ausführen, dürfen eventuell keine Ports unterhalb von Port 1024 verwendet werden.) Die Standardports empfangen möglicherweise einen Ereignisstrom, der viele unterschiedliche Arten von Syslog-Ereignissen enthält. Hierzu können UNIX, Linux, Snort, Solaris, CiscoPIX, Check Point Firewall 1 und andere gehören. CA Enterprise Log Manager verarbeitet Syslog-Ereignisse mit Hilfe von Listenern, bei denen es sich um eine besondere Art von Integrationskomponente handelt. Sie erstellen Syslog-Connectors anhand von Listenern und Integrationen:

- Der Listener stellt die Verbindungsinformationen wie etwa Ports oder vertrauenswürdige Hosts bereit.
- Die Integration definiert die Nachrichtenanalysedateien (XMP) und die Datenzuordnungsdateien (DM).

Da ein einzelner Syslog-Connector Ereignisse von vielen Ereignisquellen empfangen kann, sollten Sie überlegen, ob Syslog-Ereignisse basierend auf dem Typ oder der Quelle weitergeleitet werden sollen. Wie Sie den Empfang von Syslog-Ereignissen gestalten, ist abhängig von der Größe und Komplexität Ihrer Umgebung:

Viele Syslog-Arten: 1 Connector

Falls ein einzelner Connector Ereignisse von verschiedenen Syslog-Quellen verarbeiten muss und das Ereignisvolumen sehr groß ist, muss der Connector alle zutreffenden Integrationen (XMP-Dateien) durchsuchen, bis eine Übereinstimmung für ein Ereignis gefunden wird. Dies kann aufgrund des größeren Verarbeitungsaufwands zu einer langsameren Leistung führen. Falls das Ereignisvolumen allerdings nicht allzu groß ist, ist ein einzelner Connector auf dem Standardagenten möglicherweise ausreichend, um alle erforderlichen Ereignisse zur Speicherung zu erfassen.

1 Syslog-Art: 1 Connector

Falls Sie eine Reihe einzelner Connectors konfigurieren, die Ereignisse eines einzelnen Syslog-Typs verarbeiten, können Sie die Verarbeitungslast auf mehrere Connectors verteilen. Zu viele Connectors auf einem einzelnen Agenten können allerdings auch die Leistung verschlechtern, da jeder Connector eine separate Instanz ist, die einzeln verarbeitet werden muss.

Einige Syslog-Arten: 1 Connector

Falls in Ihrer Umgebung bestimmte Arten von Syslog-Ereignissen gehäuft auftreten, können Sie für diese Syslog-Typen jeweils einen eigenen Connector einrichten. Anschließend können Sie einen oder mehrere weitere Connectors konfigurieren, die mehrere Syslog-Ereignistypen mit einem geringeren Ereignisvolumen erfassen. Auf diese Weise können Sie

die Last der Syslog-Ereigniserfassung auf eine kleinere Anzahl von Connectors verteilen und so die Leistung verbessern.

Sie sollten nicht unbedingt eigene Syslog-Listener erstellen müssen, dies ist jedoch ggf. möglich. Sie können verschiedene Syslog-Listener mit unterschiedlichen Standardwerten für Ports, vertrauenswürdige Hosts usw. erstellen. Hierdurch lässt sich eventuell die Erstellung von Connectors vereinfachen, falls Sie beispielsweise viele Connectors für jede Art von Syslog-Ereignis erstellen müssen.

Weitere Informationen

Standardbenutzerkonten (siehe Seite 103)
Standardportzuweisungen (siehe Seite 105)
Umleiten von Firewall-Ports für Syslog-Ereignisse (siehe Seite 110)

Agenten und das Agentenzertifikat

Das vordefinierte Zertifikat "CAELM_AgentCert.cer" wird von allen Agenten verwendet, um mit ihrem CA Enterprise Log Manager-Server zu kommunizieren.

Wenn Sie dieses Zertifikat durch ein benutzerdefiniertes Zertifikat ersetzen, empfehlen wir, dies vor der Installation von Agenten durchzuführen. Wenn Sie ein benutzerdefiniertes Zertifikat implementieren, nachdem Agenten installiert und am CA Enterprise Log Manager-Server registriert worden sind, müssen Sie jeden Agenten deinstallieren, die Agenteneingabe aus dem Agenten-Explorer löschen, den Agenten neu installieren und die Connectors neu konfigurieren.

Wissenswertes über Agenten

Agenten werden nach der Installation als Service oder Daemon ausgeführt. Sie sind optionale Produktkomponenten, die in den folgenden Situationen verwendet werden können:

- Ein kleiner, entfernter Standort muss Ereignisdaten erfassen, benötigt jedoch keine vollständige CA Enterprise Log Manager-Software-Appliance.
- Sie möchten Daten auf der Ereignisquelle filtern, um den Datenverkehr im Netzwerk bzw. die Menge der gespeicherten Daten zu reduzieren.

- Sie müssen aus rechtlichen Gründen die Auslieferung der Daten an den Ereignisprotokollspeicher gewährleisten.
- Sie müssen die Protokollübertragung im Netzwerk mit Datenverschlüsselung sicherstellen.

Agenten fungieren als Prozessmanager für Connectors, die Daten von spezifischen Anwendungen, Betriebssystemen oder Datenbanken erfassen. Agenten leiten Befehle für die Connector-Verwaltung wie "Start", "Beenden" und "Neu starten" von der Agenten-Explorer-Schnittstelle in CA Enterprise Log Manager weiter. Über die Agenten werden zudem Konfigurationsänderungen und Aktualisierungen der Binärdateien an die Connectors weitergegeben.

Sie können Agenten auf einzelnen Ereignisquellen installieren oder auf Remote-Hostservern, wenn Ereignisse von mehreren Ereignisquellen erfasst werden sollen. Die CA Enterprise Log Manager-Serverinstallation installiert automatisch Ihren eigenen Agenten. Sie können diesen Standardagenten für die direkte Syslog-Ereigniserfassung verwenden.

Ferner haben Sie die Möglichkeit, über jeden CA Enterprise Log Manager-Server im Netzwerk den Status der einzelnen Agenten im Agenten-Explorer anzuzeigen. Agenten verfügen über einen Watchdog-Überwachungsservice, der Agenten neu startet, falls diese unerwartet angehalten wurden, und der nach Aktualisierungen für die Agenten- und Connector-Binärdateien sucht. Agenten senden zudem selbstüberwachende Ereignisse an den Ereignisprotokollspeicher, mit denen Änderungen und Status nachverfolgt werden.

Wissenswertes über Agentengruppen

Sie können Agentengruppen erstellen. Hierbei handelt es sich um logische Gruppierungen von Agenten, die die Agentenverwaltung erleichtern. Nachdem Sie einen Agenten zu einer Agentengruppe hinzugefügt haben, können Sie Konfigurationen ändern und die Connectors in einer Gruppe gleichzeitig starten und stoppen. So können Sie beispielsweise Agenten anhand ihres physischen (d. h. geografischen) Standorts gruppieren.

Im Agenten-Explorer können Sie Gruppen erstellen und Agenten zwischen Gruppen verschieben. Falls Sie keine Agentengruppe definieren, befinden sich alle Agenten in einer Standardgruppe, die während der Installation von CA Enterprise Log Manager angelegt wird.

Die Datensätze für die Agentenkonfigurationen und Agentengruppen werden auf dem Verwaltungsserver gespeichert. Jedes Mal, wenn Sie einen Agenten installieren, wird der neue Agent für jeden CA Enterprise Log Manager-Server, der beim Verwaltungsserver unter demselben Anwendungsinstanznamen registriert ist, im Agenten-Explorer verfügbar gemacht. So haben Sie die Möglichkeit, jeden Agenten von jedem CA Enterprise Log Manager-Server im Netzwerk aus zu steuern und zu konfigurieren.

Benutzerkontoberechtigungen für Agenten

Agenten können unter Benutzerkonten mit wenigen Berechtigungen ausgeführt werden. Erstellen Sie vor der Installation des Agenten ein Gruppen- und ein Servicebenutzerkonto auf dem Zielhost. Sie legen den Benutzernamen während der Agenteninstallation fest, und das Installationsprogramm weist die entsprechenden Berechtigungen zu. Auf Linux-Systemen ist der Agentenbenutzer Eigentümer aller Agentenbinärdateien, mit Ausnahme der Binärdateien für den Überwachungsdienst (Watchdog-Service), dessen Eigentümer der "root"-Benutzer ist.

Wissenswertes über Integrationen

Bei den mitgelieferten vorgefertigten Integrationen handelt es sich im Wesentlichen um eine Vorlagenbibliothek. Diese Vorlagen enthalten den spezifischen, für die Erfassung von Ereignissen einer bestimmten Protokollquelle erforderlichen Code. Eine Integration wird zu einem Connector, wenn sie aus der Bibliothek entnommen, konfiguriert und auf eine Ereignisquelle angewendet wird. Integrationen enthalten folgende Arten von Informationen:

- Datenzugriffsdatei mit Informationen für eine bestimmte Ereignisquelle
- Nachrichtenanalysedatei zum Erstellen von Namen-Wert-Paaren anhand der erfassten Ereignisprotokolle
- Datenzuordnungsdatei zum Zuordnen der Namen-Wert-Paare zur ELM-Schemadefinition, die das Datenbankschema für den Ereignisprotokollspeicher des CA Enterprise Log Manager-Servers bildet

CA Enterprise Log Manager stellt eine Reihe von Integrationen für beliebte und gängige Ereignisquellen wie etwa CA-Produkte, gängige Firewalls, Datenbanken, Betriebssysteme und Anwendungen bereit. Sie können weitere Integrationen auf folgende Weise beziehen:

- Automatische Software-Updates mit neuen Integrationen bzw. neuen Versionen bestehender Integrationen
- Erstellen von benutzerdefinierten Integrationen mit Hilfe der verfügbaren Assistenten

Mit den Integrationen legen Sie bei der Konfiguration Ihrer Connectors fest, welche Art von Ereigniserfassung durchgeführt werden soll.

Wissenswertes über Connectors

Connectors suchen nach Ereignissen und senden in regelmäßigen Abständen Statusereignisse zur Übergabe an den CA Enterprise Log Manager-Server an den Agenten. Bei einem *Connector* handelt es sich um einen Prozess, der mit einem Protokollsensor und einer Integration eine Konfiguration für erfasste Ereignisse einer bestimmten Ereignisquelle erstellt. Anders als bei Syslog verwenden Connectors Integrationen als Konfigurationsvorlage. Syslog-Connectors basieren auf Listenern.

Agenten erfassen Ereignisse mit Hilfe von Connectors. Nachdem Sie einen Agenten installiert haben, können Sie mit dem Agenten-Explorer auf jedem CA Enterprise Log Manager-Server einen oder mehrere Connectors für diesen Agenten konfigurieren. (Die CA Enterprise Log Manager-Server müssen unter demselben Verwaltungsserver (bzw. demselben externen CA EEM-Server) und mit demselben Anwendungsinstanznamen registriert sein, damit Agenten auf diese Weise konfiguriert werden können.)

Im Allgemeinen gibt es einen Connector für jede Ereignisquelle im Netzwerk. Bei Syslog-Ereignissen kann je nach Konfiguration auch ein Connector für mehrere Ereignisquellen vorhanden sein. Sie können mehrere Connectors erstellen, die dieselbe Integration verwenden, allerdings mit leicht unterschiedlichen Konfigurationsdetails für den Zugriff auf verschiedene Ereignisquellen. Einige Connectors bieten eine Konfigurationshilfe, mit der die für den Zugriff auf die Ereignisquelle notwendigen Informationen gesammelt werden. Falls Sie einen Connector benötigen, für den es derzeit noch keine Integration gibt, können Sie die Integration mit dem Integrationsassistenten erstellen.

Wissenswertes über Protokollsensoren

Bei einem *Protokollsensor* handelt es sich um eine Komponente in einem Connector, die weiß, wie auf Ereignisquellen zugegriffen wird. CA Enterprise Log Manager stellt Protokollsensoren für folgende Arten von Ereignisquellen und Protokollformate bereit:

ACLogsensor

Dieser Protokollsensor liest CA Access Control-Ereignisse, wenn CA Access Control Ereignisse mithilfe von selogrd weiterleitet.

FileLogSensor

Dieser Protokollsensor liest Ereignisse aus einer Datei.

LocalSyslog

Dieser Protokollsensor sammelt Ereignisse aus den lokalen Syslog-Dateien aller UNIX-Server.

ODBCLogSensor

Dieser Protokollsensor verwendet ODBC, um eine Verbindung mit einer Datenbankereignisquelle herzustellen und Ereignisse daraus abzurufen.

OPSECLogSensor

Dieser Protokollsensor liest Ereignisse aus einer Check Point-OPSEC-Ereignisquelle.

SDEELogSensor

Dieser Protokollsensor liest Ereignisse aus Cisco-Geräten.

Syslog

Dieser Protokollsensor sucht nach Syslog-Ereignissen.

TIBCOLogSensor

Dieser Protokollsensor liest Ereignisse aus einer TIBCO-EMS-Warteschlange (EMS = Event Message Service) in CA Access Control-Implementierungen.

W3CLogSensor

Dieser Protokollsensor liest Ereignisse aus einer W3C-Protokolldatei.

WinRMLinuxLogSensor

Dieser Protokollsensor aktiviert den Standardagenten (Linux) auf dem CA Enterprise Log Manager-Server zum Erfassen von Windows-Ereignissen.

WMILogSensor

Dieser Protokollsensor erfasst mittels Windows Management Instrumentation (WMI) Ereignisse aus Windows-Ereignisquellen.

Weitere Protokollsensoren werden unter Umständen über Software-Updates bereitgestellt. Weitere Informationen zum Konfigurieren von Protokollsensoren finden Sie in der Online-Hilfe und im *Administrationshandbuch*.

Bestimmen der Größe Ihres CA Enterprise Log Manager-Netzwerks

Wenn Sie die Anzahl der benötigten Agenten planen, können Sie ein einfaches Schema zur Größenberechnung heranziehen, wie das folgende. Ermitteln Sie zunächst die Anzahl der benötigten Connectors. Es muss nicht auf jeder Ereignisquelle ein Agent installiert werden. Sie müssen allerdings für jede Nicht-Syslog-Ereignisquelle, auf der Ereignisse erfasst werden sollen, einen Connector einrichten. (Sie können WMI-Ereignisse aus mehreren Ereignisquellen auf einem einzelnen Connector sammeln, indem Sie für jede Ereignisquelle einen Protokollsensor hinzufügen. Vergewissern Sie sich, dass Sie aggregierte Ereignismengen berücksichtigen, wenn Sie einen Connector auf diese Art und Weise konfigurieren.)

Syslog-Connectors können auf verschiedene Art und Weise konfiguriert werden. So besteht zum Beispiel die Möglichkeit, einen einzelnen Syslog-Connector einzurichten, der alle Syslog-Ereignisse unabhängig vom Typ empfängt. Es hat sich bewährt, als Grundlage für Ihre Syslog-Connectors Ereignismengen der einzelnen Syslog-Ereignisquellen heranzuziehen.

Sie können Agenten auf einer einzelnen Ereignisquelle installieren. Wir empfehlen diese Vorgehensweise, wenn die Anzahl der Ereignisse dieser Quelle hoch ist. Unterscheiden Sie bei der Planung zwischen Agenten auf einer Ereignisquelle und Agenten auf einem Host, die als Collectors für verschiedene Arten von Ereignissen fungieren.

Auswirkungen von Unterdrückungsregeln

Bei der Planung sollten Sie die Auswirkung von *Unterdrückungsregeln* berücksichtigen, die verhindert, dass Ereignisse entweder in den Ereignisprotokollspeicher eingefügt oder von einem Connector erfasst werden. Unterdrückungsregeln werden immer an einen Connector angehängt. Sie können Unterdrückungsregeln entweder auf Agenten- oder Gruppenebene oder auf dem CA Enterprise Log Manager-Server selbst anwenden. Die Platzierungsorte haben verschiedene Auswirkungen:

- Unterdrückungsregeln, die auf Agenten- oder Gruppenebene angewendet werden, verhindern die Erfassung von Ereignissen und reduzieren so den zum CA Enterprise Log Manager-Server *gesendeten* Netzwerkverkehr.
- Unterdrückungsregeln, die auf dem CA Enterprise Log Manager-Server angewendet werden, verhindern, dass Ereignisse in die Datenbank *eingefügt* werden, und reduzieren so die Menge an Informationen, die gespeichert wird.

Wenn Sie Unterdrückungsregeln auf Ereignisse anwenden, nachdem diese auf dem CA Enterprise Log Manager-Server eingegangen sind, müssen Sie unter Umständen Leistungsbeeinträchtigungen berücksichtigen. Dies gilt insbesondere, wenn Sie mehrere Unterdrückungsregeln erstellen oder die Ereignisflussrate hoch ist.

Es empfiehlt sich beispielsweise, *einige* der Ereignisse von einer Firewall oder von manchen Windows-Servern zu unterdrücken, durch die doppelte Ereignisse für dieselbe Aktion erstellt werden. Wenn Sie auf die Erfassung dieser Ereignisse verzichten, kann dies die Übertragung der Ereignisprotokolle beschleunigen, die Sie speichern möchten. Zudem wird weniger Verarbeitungszeit auf dem CA Enterprise Log Manager-Server benötigt. In solchen Fällen wenden Sie eine oder mehrere geeignete Unterdrückungsregeln auf Agentenkomponenten an.

Falls Sie alle Ereignisse eines bestimmten Typs von mehreren Plattformen oder aus Ihrer gesamten Umgebung unterdrücken möchten, wenden Sie eine oder mehrere geeignete Unterdrückungsregeln auf dem CA Enterprise Log Manager-Server an. Die Auswertung von Ereignissen im Hinblick auf die Unterdrückung findet statt, wenn die Ereignisse auf dem CA Enterprise Log Manager-Server eintreffen. Bei der Anwendung einer großen Anzahl von Unterdrückungsregeln auf dem Server sinkt möglicherweise die Leistung, da der Server nicht nur die Ereignisse in den Ereignisprotokollspeicher einfügen, sondern zusätzlich die Unterdrückungsregeln anwenden muss.

Bei kleineren Implementierungen können Sie die Unterdrückung auf dem CA Enterprise Log Manager-Server ausführen. Für Bereitstellungen mit Zusammenfassung (Aggregation) können Sie die Unterdrückung ebenfalls auf dem Server anwenden. Wenn Sie nur wenige Ereignisse von einer Ereignisquelle einfügen, die in großem Umfang Ereignisinformationen generiert, können Sie trotzdem unerwünschte Ereignisse auf der Agenten- oder Agentengruppenebene unterdrücken, um Verarbeitungszeit auf dem CA Enterprise Log Manager-Server einzusparen.

Kapitel 3: Installieren von CA Enterprise Log Manager

Dieses Kapitel enthält folgende Themen:

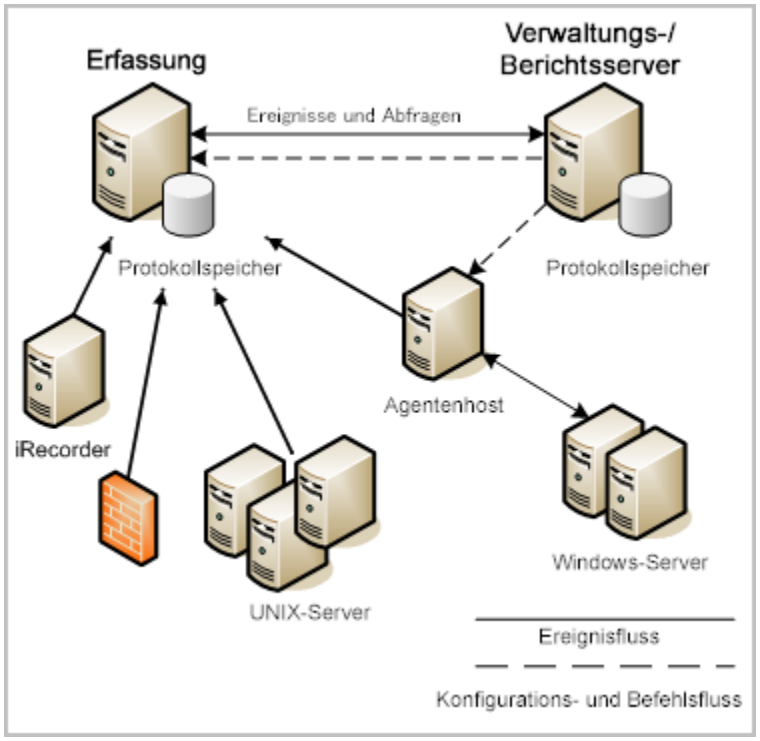
Wissenswertes über die CA Enterprise Log Manager-Umgebung

CA Enterprise Log Manager ist darauf ausgelegt, dass Sie das Produkt innerhalb kürzester Zeit nach Beginn der Installation verwenden, Protokollinformationen erfassen und Berichte erstellen können. Sie müssen die CA Enterprise Log Manager-Software-Appliance auf einem eigens dafür vorgesehenen System installieren.

Wichtig! Damit der CA Enterprise Log Manager-Server eine leistungsstarke Ereignisprotokollerfassung durchführen kann, sollten Sie keine anderen Anwendungen auf dem Hostserver installieren. Weitere Anwendungen können sich negativ auf die Leistung des CA Enterprise Log Manager-Servers auswirken.

Es gibt verschiedene Möglichkeiten, die Umgebung zu konfigurieren. Empfohlen wird die folgende, spezifische Konfiguration, mit der große Ereignismengen in Unternehmensumgebungen verarbeitet werden können.

Installieren Sie für eine einfache Produktionsumgebung auf Unternehmensniveau mindestens zwei CA Enterprise Log Manager-Server in Ihrem bestehenden Netzwerk. Die CA Enterprise Log Manager-Server verwenden die vorhandenen DNS-Server im Netzwerk für die Arbeit mit benannten Ereignisquellen und Agentenhosts. Der eine Server dient vornehmlich der Erfassung von Ereignisprotokollen, der andere der Berichterstellung über die erfassten Ereignisprotokolle. In einer Umgebung mit zwei Servern übernimmt der zuerst installierte Verwaltungsserver die Funktion eines Berichtsservers. Als Verwaltungsserver führt dieser Server die Benutzerauthentifizierung und -autorisierung sowie weitere Verwaltungsfunktionen durch. In der folgenden Abbildung ist eine solche einfache Umgebung mit einigen Ereignisquellen dargestellt:



Die durchgezogenen Linien zeigen den Ereignisfluss von den Ereignisquellen zum (agentenlosen) Quellserver bzw. zu einem Agentenhost und dann zum (agentenlosen) Quellserver für Protokolldateien. Syslog-Ereignisse können direkt mit dem Standardagenten auf dem (agentenlosen) CA Enterprise Log Manager-Quellserver für Protokolldateien erfasst werden. Ferner können Sie einen oder mehrere Connectors auf einem separaten Agentenhost konfigurieren, die Daten von mehreren Syslog-Quellen erfassen (nicht abgebildet).

Bei der Windows-Ereigniserfassung wird Windows Management Instrumentation (WMI) zur Überwachung der Windows-Server auf Ereignisse eingesetzt. Hierfür müssen Sie einen WMI-Connector auf einem Agenten, der auf einem Windows-Host installiert ist, als (agentenbasierten) Quellserver für Protokolldateien konfigurieren. Bei einigen anderen Ereignisarten bietet sich eventuell die Verwendung eines eigenständigen CA-iRecorders auf einem Hostserver an.

Sie können die Agenten und Connectors für diese Ereignisquellen über jeden CA Enterprise Log Manager-Server im Netzwerk konfigurieren und verwalten. Die gestrichelten Linien in der Abbildung stehen für den Konfigurations- und Steuerungsaustausch zwischen dem Verwaltungsserver und den Agenten sowie zwischen den einzelnen anderen CA Enterprise Log Manager-Servern. In einer Umgebung, wie sie in der Abbildung dargestellt ist, werden die Konfigurationen vom Verwaltungsserver aus vorgenommen. Hierdurch können sich die (agentenlosen) Quellserver für Protokolldateien auf die Ereignisverarbeitung konzentrieren.

Die Protokollerfassungsumgebung, in der Sie CA Enterprise Log Manager-Server installieren, weist folgende Merkmale auf:

- Der CA Enterprise Log Manager-Verwaltungsserver handhabt die Benutzerauthentifizierung und -autorisierung und verwaltet die Konfigurationen für alle CA Enterprise Log Manager-Server, -Agenten und -Connectors im Netzwerk mit Hilfe des lokalen CA EEM-Servers.

  Je nach Größe Ihres Netzwerks und des Ereignisvolumens können Sie auch mehrere Verwaltungsserver installieren und unter jedem Verwaltungsserver einen Verbund (Föderation) aus (agentenlosen) Quellservern für Protokolldateien anlegen. Ferner können Sie mehrere Server für die Berichterstellung bestimmen, wobei alle Berichtsserver bei dem einen Verwaltungsserver registriert werden. In diesem Szenario findet der Ereignisfluss von den Ereignisquellen über den konfigurierten (agentenlosen) Quellserver für Protokolldateien hin zum konfigurierten Berichtsserver statt.

- Die eingehenden Ereignisse werden auf einem oder mehreren (agentenlosen) CA Enterprise Log Manager-Quellservern für Protokolldateien verarbeitet und gespeichert.

- Die Ereignisse werden von verschiedenen Ereignisquellen durch das Protokollerfassungsnetzwerk geleitet, *nachdem* Sie die entsprechenden Connectors bzw. Adapter konfiguriert haben.

Weitere Informationen

Serverplanung (siehe Seite 19)

Erstellen der Installations-DVDs

Die CA Enterprise Log Manager-Software steht in Form herunterladbarer, verpackter ISO-Images zur Verfügung. Nachdem Sie die Software heruntergeladen haben, müssen Sie DVD-Datenträger erstellen, bevor Sie die Installation durchführen können. Gehen Sie wie unten beschrieben vor, um die ISO-Images herunterzuladen und die Installationsmedien zu erstellen.

So erstellen Sie die Installations-DVDs:

1. Greifen Sie auf einem mit dem Internet verbundenen Computer über http://ca.com/support auf den Download-Server zu.
2. Klicken Sie auf den Link für den technischen Support und dann auf den Link für das Download-Center.
3. Wählen Sie im Feld für die Produktauswahl ("Select a Product") den Eintrag "CA Enterprise Log Manager" aus, und wählen Sie dann im Feld für die Releaseauswahl ("Select a Release") die gewünschte Version aus.
4. Aktivieren Sie das Kontrollkästchen zur Auswahl aller Komponenten ("Select all components"), und klicken Sie auf "Go".

   Die Download-Seite für veröffentlichte Lösungen ("Published Solutions Downloads") wird angezeigt.
5. Wählen Sie das Download-Paket aus.

   Die Seite für das Lösungsdokument ("Solution Document") wird angezeigt.
6. Blättern Sie zum Ende der Seite, und wählen Sie den Link "Download" neben dem Paketnamen aus.

   Das Paket wird heruntergeladen.

   Hinweis: Je nach Verbindungsgeschwindigkeit kann der Download-Vorgang eine Weile dauern.
7. Entpacken Sie die beiden Installations-Images.
8. Erstellen Sie zwei getrennte Installationsmedien, indem Sie das Image für das Betriebssystem und das CA Enterprise Log Manager-ISO-Image auf zwei verschiedene DVD-RW-Datenträger brennen.

   Die beiden Installationsmedien enthalten alle Betriebssystem- und Produktkomponenten für Ihre CA Enterprise Log Manager-Umgebung. Sie können allerdings auch weitere Komponenten wie SAPI-Recorder oder iRecorder in Ihrer Umgebung verwenden. Diese können gesondert von der Website für den CA-Support heruntergeladen werden.
9. Führen Sie die Installation mit den neu erstellten Installations-DVDs durch.

Installieren eines CA Enterprise Log Manager-Servers

Der Installationsvorgang umfasst die folgenden Schritte:

- Ausfüllen des Arbeitsblatts für den CA Enterprise Log Manager-Server
- Installieren des CA Enterprise Log Manager-Verwaltungsservers

  Hinweis: Wenn Sie SAN-Speicher verwenden, treffen Sie Vorsichtsmaßnahmen, um zu vermeiden, auf einem SAN-Laufwerk zu installieren.
- Installieren von mindestens einem CA Enterprise Log Manager-Sammelserver
- (Optional) Installieren eines oder mehrerer Berichtsserver

  Hinweis: Falls Sie keinen gesonderten Server für die Berichterstellung installieren, kann auch der Verwaltungsserver die Rolle des Berichtsservers übernehmen.
- (Optional) Installieren eines Wiederherstellungspunktservers
- Überprüfen der Installation
- Anzeigen selbstüberwachender Ereignisse

Wichtig! Konfigurieren Sie Ihre Speichermedien in einem RAID-Array, *bevor* Sie die CA Enterprise Log Manager-Installation starten. Konfigurieren Sie die ersten beiden Datenträger als RAID 1, und machen Sie dieses Array zu einem bootbaren Array. Konfigurieren Sie die übrigen Datenträger als einzelnes RAID 5-Array. Falls Sie kein RAID-Array einrichten, können Daten verloren gehen.

Im Rahmen der Gesamtsicherheit für den CA Enterprise Log Manager-Server selbst ist das GRUB-Hilfsprogramm (Grand Unified Bootloader) kennwortgeschützt.

Arbeitsblatt für den CA Enterprise Log Manager-Server

Notieren Sie sich die Informationen in der folgenden Tabelle, bevor Sie einen CA Enterprise Log Manager-Server installieren. Wenn Sie sich die Daten im Arbeitsblatt notieren, können Sie sie während der Installation zu Rate ziehen. Sie können für jeden zu installierenden CA Enterprise Log Manager-Server ein eigenes Arbeitsblatt ausdrucken und ausfüllen.

CA Enterprise Log Manager-Daten	Wert	Kommentare
OS Disk (BS-Datenträger)		

CA Enterprise Log Manager-Daten	Wert	Kommentare
Keyboard Type (Tastatur)	*entsprechender Wert*	Geben Sie mit Hilfe der nationalen Spracheinstellung an, welche Art von Tastatur verwendet werden soll. Als Standardwert werden die Hardwareeinstellungen für die Tastatur verwendet, die beim Start des Servers an den Server angeschlossen war.
Time Zone Selection (Zeitzonenauswahl)	*Ihre gewünschte Zeitzone*	Wählen Sie die Zeitzone aus, in der sich der Server befindet.
Root Password ("root"-Kennwort)	*neues "root"-Kennwort*	Erstellen und bestätigen Sie ein neues "root"-Kennwort für diesen Server.
Application Disk (Anwendungsdatenträger)		
New Hostname (neuer Hostname)	*Hostname für diesen CA Enterprise Log Manager-Server* Beispiel: CA-ELM1	Geben Sie den Hostnamen für diesen Server an. Verwenden Sie dabei nur für Hostnamen zulässige Zeichen. Empfohlen werden die Buchstaben A-Z (unabhängig von Groß- oder Kleinschreibung), die Zahlen 0-9 und der Bindestrich, wobei das erste Zeichen ein Buchstabe und das letzte Zeichen ein alphanumerisches Zeichen ist. Verwenden Sie keine Unterstriche in Hostnamen. **Hinweis:** Hängen Sie an diesen Hostnamenwert keinen Domänennamen an.
Select a device (Gerät auswählen)	*Gerätename*	Wählen Sie den Namen des Netzwerkadapters aus, der für die Ereignisprotokollerfassung und Kommunikation verwendet wird. Drücken Sie die LEERTASTE, um die Konfiguration für das Gerät einzugeben.
IP Address, Subnet Mask, and Default Gateway (IP-Adresse, Teilnetzmaske und Standard-	*relevante IP-Werte*	Geben Sie eine gültige IP-Adresse für diesen Server ein. Geben Sie eine gültige

CA Enterprise Log Manager-Daten	Wert	Kommentare
Gateway)		Teilnetzmaske und ein Standard-Gateway für die Verwendung mit diesem Server ein.
Domain name (Domänenname)	*der Name Ihrer Domäne*	Geben Sie den voll qualifizierten Namen der Domäne ein, in der dieser Server fungiert, z. b. meineFirma.com. **Hinweis:** Der Domänenname muss beim DNS-Server (DNS = Domain Name Server) in Ihrem Netzwerk registriert sein, damit der Hostname in eine IP-Adresse aufgelöst werden kann.
List of DNS servers (Liste der DNS-Server)	*relevante IPv4- bzw. IPv6-Adressen*	Geben Sie eine oder mehrere DNS-Server-IP-Adressen für die Verwendung in Ihrem Netzwerk ein. In der Liste sind die Einträge durch Komma *ohne* Leerzeichen zwischen den Einträgen getrennt. Falls Ihre DNS-Server IPv6-Adressen verwenden, geben Sie diese Adressen im entsprechenden Format ein.
System Date and Time (Systemdatum und -uhrzeit)	*lokales Datum und lokale Uhrzeit*	Geben Sie ggf. ein neues Systemdatum und eine neue Uhrzeit ein.
Update Time through NTP? (Zeit über NTP aktualisieren?)	Yes (empfohlen) oder No	Geben Sie an, ob der CA Enterprise Log Manager-Server so konfiguriert werden soll, dass Datum und Uhrzeit anhand eines bestimmten NTP-Servers (NTP = Network Time Protocol) aktualisiert werden. **Hinweis:** Die Synchronisierung der Uhrzeit hilft sicherzustellen, dass Alarme vollständige Daten enthalten.
NTP Server Name or Address (Name oder Adresse des NTP-Servers)	*relevanter Hostname bzw. IP-Adresse*	Geben Sie den Hostnamen bzw. die gültige IP-Adresse des NTP-Servers ein, von dem dieser CA Enterprise Log Manager-Server die Informationen zu Datum und

CA Enterprise Log Manager-Daten	Wert	Kommentare
		Uhrzeit beziehen soll.
Sun Java JDK EULA (Sun Java JDK-Lizenzvereinbarung)	Ja	Lesen Sie die Lizenzvereinbarung, und blättern Sie bis zu der Frage, ob Sie die Bedingungen der Lizenzvereinbarung akzeptieren [ja oder nein].
CA EULA (CA-Lizenzvereinbarung)	Ja	Lesen Sie die CA-Lizenzvereinbarung, und blättern Sie bis zu der Frage, ob Sie die Bedingungen der Lizenzvereinbarung akzeptieren [ja oder nein].
Local or Remote CA Embedded Entitlements Manager server? (Lokaler CA Embedded Entitlements Manager-Server oder CA Embedded Entitlements Manager-Remote-Server?)	Local: beim ersten installierten Server (Verwaltungsserver) Remote: bei jedem weiteren Server	Geben Sie an, ob Sie einen lokalen oder einen standortfernen CA EEM-Server verwenden möchten. Wählen Sie bei einem CA Enterprise Log Manager-Verwaltungsserver die Option "Local". Sie werden im Zuge der Installation aufgefordert, ein Kennwort für das "EiamAdmin"-Standardbenutzerkonto anzulegen. Wählen Sie bei jedem weiteren Server die Option "Remote". Sie werden im Zuge der Installation nach dem Namen des Verwaltungsservers gefragt. Unabhängig davon, ob Sie die Option "local" oder "remote" gewählt haben, müssen Sie bei der ersten Anmeldung bei *jedem* CA Enterprise Log Manager-Server die "EiamAdmin"-Konto-ID und das "EiamAdmin"-Kennwort verwenden.
Enter name of the CA EEM server (Name des CA EEM-Servers eingeben)	*IP-Adresse oder Hostname*	Diese Eingabeaufforderung wird nur angezeigt, wenn Sie bei der Eingabeaufforderung für den lokalen oder standortfernen Server die Option "Remote" gewählt haben. Geben Sie die IP-Adresse bzw. den

CA Enterprise Log Manager-Daten	Wert	Kommentare
		Hostnamen des CA Enterprise Log Manager-Verwaltungsservers ein, den Sie zuerst installiert haben. Der Hostname muss auf dem DNS-Server registriert sein.
CA EEM Server Admin password (Kennwort des CA EEM-Serveradministrators)	*Kennwort des "EiamAdmin"-Kontos*	Notieren Sie sich das Kennwort für das Standardadministratorkonto "EiamAdmin". Der CA Enterprise Log Manager-Server *benötigt* diese Kontoanmeldeinformationen für die erste Anmeldung. Falls Sie den Verwaltungsserver installieren, erstellen und bestätigen Sie hier ein neues "EiamAdmin"-Kennwort. Notieren Sie sich dieses Kennwort, da Sie es für die Installation der übrigen CA Enterprise Log Manager-Server und Agenten benötigen. **Hinweis:** Das hier eingegebene Kennwort dient auch als anfängliches Kennwort für das "caelmadmin"-Standardkonto, mit dem Sie direkt über SSH auf den CA Enterprise Log Manager-Server zugreifen. Sie können nach der Installation ggf. weitere Administratorkonten erstellen, um auf die CA EEM-Funktionen zuzugreifen.
Application Instance Name (Anwendungsinstanzname)	CAELM	Wenn Sie den ersten CA Enterprise Log Manager-Server im Netzwerk installieren, erstellen Sie bei dieser Eingabeaufforderung einen Anwendungsinstanzwert. Nachfolgende CA Enterprise Log Manager-Server verwenden diesen Wert für die Registrierung beim Verwaltungsserver. Der standardmäßige

CA Enterprise Log Manager-Daten	Wert	Kommentare
		Anwendungsinstanzname lautet CAELM. Sie können allerdings jeden beliebigen Namen für diesen Wert verwenden. Notieren Sie sich den Anwendungsinstanznamen zur Verwendung bei weiteren CA Enterprise Log Manager-Installationen.
Möchten Sie den CAELM-Server im FIPS-Modus ausführen?	"Yes" oder "No"	Ihre Antwort auf diese Frage entscheidet darüber, ob der CA Enterprise Log Manager-Server im FIPS-Modus gestartet wird. **inweis:** Wenn Sie einen Server zu einer vorhandenen CA Enterprise Log Manager-Bereitstellung hinzufügen möchten, muss der CA Enterprise Log Manager-Verwaltungsserver bzw. der CA EEM-Remote-Server ebenfalls im FIPS-Modus ausgesführt werden. Anderenfalls wird der neue Server nicht registriert, und Sie müssen ihn von Neuem installieren.

Hinweis: Sie erhalten im Zuge der Installation Gelegenheit, die CA EEM-Serverdaten zu überprüfen und zu ändern, bevor ein Verbindungsversuch unternommen wird.

Falls das Installationsprogramm keine Verbindung mit dem angegebenen Verwaltungsserver herstellen kann und Sie die Installation fortsetzen, können Sie den CA Enterprise Log Manager-Server manuell über die eingebetteten CA EEM-Funktionen registrieren. In diesem Fall müssen Sie auch die Inhalts-, ELM-Schemadefinitions- und Agentenverwaltungsdateien manuell importieren. Weitere Informationen und Anleitungen finden Sie im Abschnitt zur Fehlerbehebung während der Installation.

Weitere Informationen:

Registrieren des CA Enterprise Log Manager-Servers beim CA EEM-Server (siehe Seite 123)
Beziehen von Zertifikaten vom CA EEM-Server (siehe Seite 124)
Importieren von CA Enterprise Log Manager-Berichten (siehe Seite 124)
Importieren von CA Enterprise Log Manager-Datenzuordnungsdateien (siehe Seite 125)
Importieren von CA Enterprise Log Manager-Nachrichtenanalysedateien (siehe Seite 126)

Importieren der Dateien für die ELM-Schemadefinition (siehe Seite 126)
Importieren von Dateien für die allgemeine Agentenverwaltung (siehe Seite 127)

Installation von CA Enterprise Log Manager

Gehen Sie wie unten beschrieben vor, um einen CA Enterprise Log Manager-Server zu installieren.

So installieren Sie die CA Enterprise Log Manager-Software:

1. Booten Sie den Server mit der Installations-DVD für das Betriebssystem.

   Die Installation des Betriebssystems wird automatisch gestartet.

2. Verwenden Sie bei den Eingabeaufforderungen die Informationen aus dem Arbeitsblatt für den CA Enterprise Log Manager-Server.

   Falls Sie der Lizenzvereinbarung nicht zustimmen, wird die Installation beendet und der Server heruntergefahren.

3. Wenn Sie zum Neustart des Computers aufgefordert werden, entfernen Sie zunächst den Datenträger und klicken dann auf die Option zum Neustarten.

4. Legen Sie den CA Enterprise Log Manager-Anwendungsdatenträger ein, wenn Sie dazu aufgefordert werden, und drücken Sie die EINGABETASTE.

5. Verwenden Sie bei den Eingabeaufforderungen die Informationen aus dem Arbeitsblatt.

   Die Installation wird fortgesetzt. Am Ende der Installation wird eine Meldung angezeigt, dass CA Enterprise Log Manager erfolgreich installiert wurde.

   Hinweis: Falls Sie weitere CA Enterprise Log Manager-Server installieren, wird möglicherweise im Installationsprotokoll eine Meldung angezeigt, die besagt, dass der Anwendungsname, der während der Installation beim CA EEM-Server registriert werden sollte, bereits vorhanden ist. Sie können diese Meldung ignorieren, da bei jeder CA Enterprise Log Manager-Installation versucht wird, den Anwendungsnamen als neuen Namen zu erstellen.

Nach Abschluss der Installation müssen Sie den CA Enterprise Log Manager-Server konfigurieren, damit Ereignisse empfangen werden können. Hierzu gehört eventuell auch die Konfiguration eines Connectors auf dem Standardagenten, damit Syslog-Ereignisse empfangen werden können.

Weitere Informationen

Fehlerbehebung bei der Installation (siehe Seite 121)
Konfigurieren des Standardagenten (siehe Seite 195)

Überprüfen der Ausführung des iGateway-Prozesses

Falls Sie nach der Installation nicht auf die Webschnittstelle des CA Enterprise Log Manager-Servers zugreifen können und sich sicher sind, dass die Netzwerkschnittstellenports richtig konfiguriert wurden, kann es sein, dass der iGateway-Prozess nicht ausgeführt wird.

Gehen Sie wie unten beschrieben vor, um eine schnelle Überprüfung des iGateway-Prozessstatus vorzunehmen. Der iGateway-Prozess muss ausgeführt werden, damit der CA Enterprise Log Manager-Server Ereignisse erfassen kann und die Benutzeroberfläche verfügbar ist.

So überprüfen Sie den iGateway-Daemon:

1. Rufen Sie auf dem CA Enterprise Log Manager-Server eine Befehlszeile auf.
2. Melden Sie sich mit den Anmeldedaten des "caelmadmin"-Kontos an.
3. Schalten Sie Benutzer mit folgendem Befehl auf das "root"-Konto um:

   ```
   su - root
   ```

4. Überprüfen Sie mit dem folgenden Befehl, ob der iGateway-Prozess ausgeführt wird:

   ```
   ps -ef | grep igateway
   ```

   Das Betriebssystem gibt die Daten für den iGateway-Prozess und eine Liste der unter iGateway ausgeführten Prozesse zurück.

Weitere Informationen

Beheben von Fehlern bei der Netzwerkschnittstellenkonfiguration (siehe Seite 122)

Starten des iGateway-Daemon oder -Service

Beim iGateway-Daemon bzw. -Service handelt es sich um den Prozess, der alle Aufrufe an die Benutzerschnittstelle von CA EEM und CA Enterprise Log Manager verarbeitet. Der Prozess muss ausgeführt werden, damit Sie auf diese beiden Anwendungen zugreifen können. Gehen Sie wie unten beschrieben vor, um den iGateway-Prozess zu starten, falls er nicht ausgeführt wird.

Hinweis: Falls Sie iGateway nicht starten können, vergewissern Sie sich, dass für den Ordner "/" ausreichend Speicherplatz verfügbar ist. Falls zu wenig Speicherplatz verfügbar ist, kann iGateway nicht gestartet werden.

So starten Sie den iGateway-Daemon oder -Service:

1. Melden Sie sich als "caelmadmin"-Benutzer beim CA Enterprise Log Manager-Server an.
2. Schalten Sie Benutzer mit folgendem Befehl auf das "root"-Konto um:

   ```
   su -
   ```

3. Starten Sie den iGateway-Prozess mit dem folgenden Befehl:

   ```
   $IGW_LOC/S99igateway start
   ```

   "S99igateway" ist das Startskript für den iGateway-Prozess. Eigentümer des Skripts ist das "root"-Konto. Der gestartete iGateway-Prozess wird unter dem "caelmservice"-Benutzerkonto ausgeführt.

Beenden des iGateway-Daemon oder -Service

Beim iGateway-Daemon bzw. -Service handelt es sich um den Prozess, der alle Aufrufe an die Benutzerschnittstelle von CA EEM und CA Enterprise Log Manager verarbeitet. Der Prozess muss ausgeführt werden, damit Sie auf diese beiden Anwendungen zugreifen können. Gehen Sie wie unten beschrieben vor, um den iGateway-Prozess zu beenden. Sie müssen den Prozess beispielsweise stoppen, wenn Sie ihn neu starten möchten oder einen CA Enterprise Log Manager-Server aus dem Netzwerk entfernen.

So beenden Sie den iGateway-Daemon oder -Service:

1. Melden Sie sich als "caelmadmin"-Benutzer beim CA Enterprise Log Manager-Server an.
2. Schalten Sie Benutzer mit folgendem Befehl auf das "root"-Konto um:

   ```
   su -
   ```

3. Beenden Sie den iGateway-Prozess mit dem folgenden Befehl:

   ```
   $IGW_LOC/S99igateway stop
   ```

   "S99igateway" ist das Skript zum Stoppen des iGateway-Prozesses. Eigentümer des Skripts ist das "root"-Konto. Der gestartete iGateway-Prozess wird unter dem "caelmservice"-Benutzerkonto ausgeführt.

Starten des CA Enterprise Log Manager-Agent-Daemon bzw. des CA Enterprise Log Manager-Agent-Service

Mit dem CA Enterprise Log Manager-Agent-Daemon bzw. -Service werden Connectors verwaltet, die erfasste Ereignisse an einen CA Enterprise Log Manager-Server senden. Der Prozess muss ausgeführt werden, damit Connectors Ereignisse erfassen können. Gehen Sie wie unten beschrieben vor, um den CA Enterprise Log Manager-Agentenprozess zu starten, falls er noch nicht ausgeführt wird.

So starten Sie den CA ELM-Agent-Daemon bzw. -Service:

1. Melden Sie sich als "root"-Benutzer oder Windows-Administrator an.
2. Öffnen Sie eine Eingabeaufforderung, und geben Sie den folgenden Befehl ein:

   ```
   Linux, UNIX, Solaris: /opt/CA/ELMAgent/bin/S99elmagent start

   Windows: net start ca-elmagent
   ```

Stoppen des CA Enterprise Log Manager-Agent-Daemon oder des CA Enterprise Log Manager-Agent-Service

Mit dem CA Enterprise Log Manager-Agent-Daemon bzw. -Service werden Connectors verwaltet, die erfasste Ereignisse an einen CA Enterprise Log Manager-Server senden. Der Prozess muss ausgeführt werden, damit Connectors Ereignisse erfassen können. Gehen Sie wie unten beschrieben vor, um den CA Enterprise Log Manager-Agentenprozess zu stoppen. Normalerweise werden Start- und Stopp-Befehle im Agenten-Explorer auf einem CA Enterprise Log Manager-Server ausgegeben. Sie können diesen Befehl beispielsweise verwenden, um den Neustart eines Agentenprozesses und seiner Connectors vorzubereiten.

So stoppen Sie den CA ELM-Agent-Daemon bzw. -Service:

1. Melden Sie sich als "root"-Benutzer oder Windows-Administrator an.
2. Öffnen Sie eine Eingabeaufforderung, und geben Sie den folgenden Befehl ein:

   ```
   Linux, UNIX, Solaris: /opt/CA/ELMAgent/bin/S99elmagent stop

   Windows: net stop ca-elmagent
   ```

Überprüfen der CA Enterprise Log Manager-Serverinstallation

Sie haben die Möglichkeit, die CA Enterprise Log Manager-Serverinstallation mit einem Webbrowser zu überprüfen. Eine erste Überprüfung der Installation können Sie vornehmen, indem Sie sich beim CA Enterprise Log Manager-Server anmelden.

Hinweis: Wenn Sie sich zum ersten Mal bei der CA Enterprise Log Manager-Anwendung anmelden, müssen Sie die Anmeldeinformationen für den "EiamAdmin"-Benutzer verwenden, unter dem Sie den CA Enterprise Log Manager-Server installiert haben. Nachdem Sie sich mit diesem Benutzerkonto angemeldet haben, haben Sie nur Zugang zu bestimmten Funktionen für die Benutzer- und Zugriffsverwaltung. Sie müssen dann den Benutzerspeicher konfigurieren und ein neues CA Enterprise Log Manager-Benutzerkonto erstellen, damit Sie Zugang zu den übrigen CA Enterprise Log Manager-Funktionen erhalten.

So überprüfen Sie die CA Enterprise Log Manager-Serverinstallation:

1. Öffnen Sie einen Webbrowser, und geben Sie die folgende URL ein:

   `https://<Server-IP-Adresse>:5250/spin/calm`

   Der CA Enterprise Log Manager-Anmeldebildschirm wird angezeigt.

2. Melden Sie sich als "EiamAdmin"-Verwaltungsbenutzer an.

   Auf der Registerkarte "Verwaltung" wird die untergeordnete Registerkarte "Benutzer- und Zugriffsverwaltung" angezeigt. Wenn Sie sich beim CA Enterprise Log Manager-Server anmelden können, war die Installation erfolgreich.

   Hinweis: Sie müssen mindestens einen Ereignisquellenservice konfigurieren, bevor Sie Ereignisdaten empfangen und Berichte anzeigen können.

Anzeigen von selbstüberwachenden Ereignissen

Sie können mit Hilfe von selbstüberwachenden Ereignissen überprüfen, ob der CA Enterprise Log Manager-Server ordnungsgemäß installiert wurde. Bevor Sie mit CA Enterprise Log Manager Ereignisprotokolldaten im Netzwerk erfassen und entsprechende Berichte erstellen können, müssen Sie zwar zunächst noch einige Konfigurationsaufgaben durchführen. Die vom CA Enterprise Log Manager-Server erzeugten selbstüberwachenden Ereignisse können allerdings sofort angezeigt werden.

Die Anmeldung beim CA Enterprise Log Manager-Server ist der erste und beste Test der Installation. Selbstüberwachende Ereignisse sind eine weitere Möglichkeit, den Status des CA Enterprise Log Manager-Servers zu überprüfen. Es gibt verschiedene Arten von selbstüberwachenden Ereignissen. Gehen Sie wie unten beschrieben vor, um zusätzliche Ereignisdaten für Ereignisse anzuzeigen, die vom CA Enterprise Log Manager-Server selbst erzeugt wurden.

So zeigen Sie selbstüberwachende Ereignisse an:

1. Melden Sie sich beim CA Enterprise Log Manager-Server an.
2. Klicken Sie auf die Registerkarte "Berichte".
3. Klicken Sie auf die System-Kennung, und wählen Sie den Bericht "Selbstüberwachende Ereignisse des Systems - Details" aus.

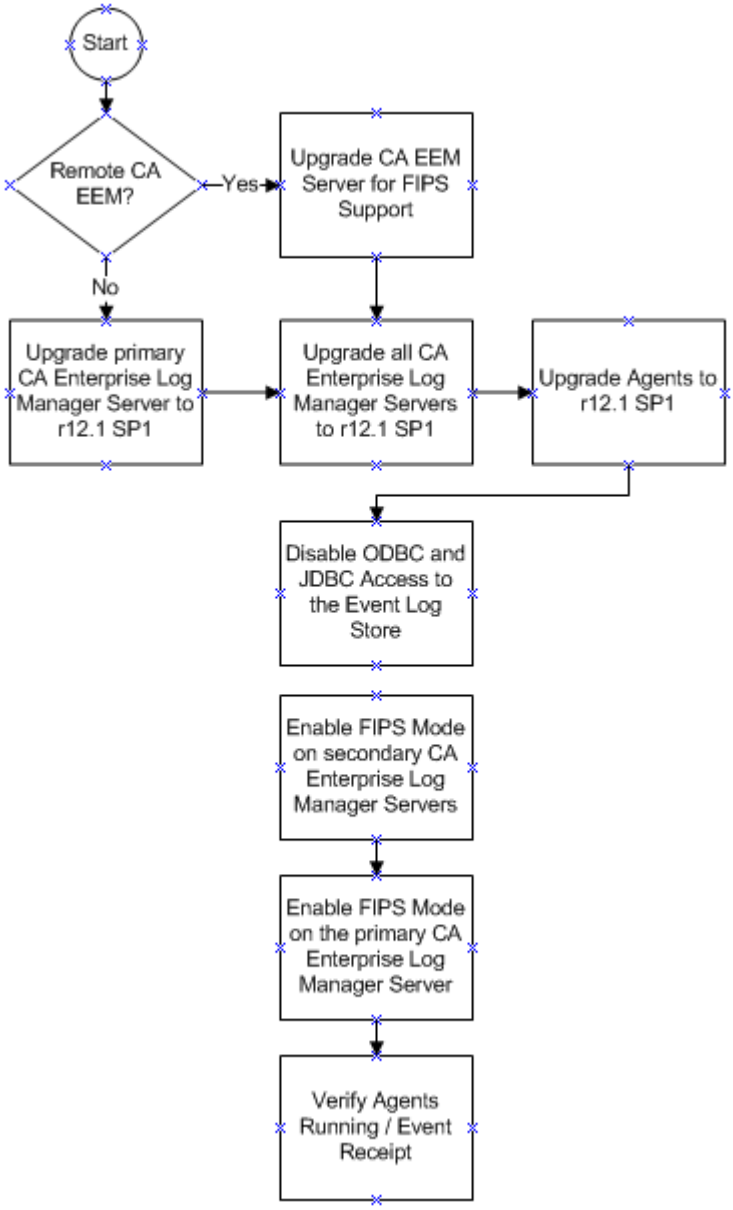
   Der Bericht über die selbstüberwachenden Ereignisse wird geladen.
4. Überprüfen Sie, ob der Bericht die selbstüberwachenden Ereignisse für Ihre Anmeldung und andere vorläufige Konfigurationsaktivitäten enthält.

Durchführen eines Upgrades vorhandener CA Enterprise Log Manager-Server und Agenten für FIPS-Unterstützung

Sie können FIPS-Unterstützung für vorhandene CA Enterprise Log Manager-Server und -Agenten über das Modul für automatische Software-Updates erreichen. Für diesen Upgrade-Vorgang wird Folgendes angenommen:

- CA Enterprise Log Manager r12.1 wurde installiert, oder ein Upgrade von r12.0 SP3 durchgeführt.
- Sie möchten den FIPS-Modus für Ihre CA Enterprise Log Manager-Föderation aktivieren.

Gehen Sie wie folgt vor, um ein Upgrade für Ihre Server durchzuführen:



Das Upgrade und der FIPS-Aktivierungsprozess umfassen die folgenden Schritte:

1. Führen Sie ein Upgrade für den Primär- oder Verwaltungsserver auf r12.1 SP1 durch.

   Wenn Sie einen CA EEM-Remote-Server verwenden, stellen Sie sicher, dass dieser über eine Version verfügt, die den FIPS-Betrieb unterstützt. Weitere Informationen zum Upgrade der FIPS-Unterstützung finden Sie in *CA EEM-Versionshinweise*.

   Detaillierte Anweisungen zur Verwendung des Moduls für automatische Software-Updates, um sowohl für CA Enterprise Log Manager-Server als auch -Agenten ein Upgrade durchzuführen, sind im *Administrationshandbuch* verfügbar.

2. Führen Sie für alle anderen CA Enterprise Log Manager-Server in der Föderation ein Upgrade auf r12.1 SP1 durch.

3. Führen Sie für alle Agenten ein Upgrade auf r12.1 SP1 durch und aktualisieren Sie nach Bedarf die Connector-Protokollsensoren.

   Wichtig! Wenn Sie einen Connector bereitstellen, der den Syslog-Protokollsensor auf einem Windows-Host verwendet, aktualisieren Sie alle Connector-Konfigurationen, um den aktuellsten Syslog-Sensor für diese Version zu verwenden, wenn der FIPS-Modus aktiviert wurde. Weitere Informationen zur aktuellsten Liste der Integrationen, die den Syslog-Protokollsensor verwenden, finden Sie in der CA Enterprise Log Manager-Produktintegrationsmatrix https://support.ca.com/irj/portal/anonymous/phpdocs?filePath=0/8238/8238_integration_certmatrix.html.

4. Deaktivieren Sie den ODBC- und JDBC-Zugriff zum Ereignisprotokollspeicher.

5. Aktivieren Sie den FIPS-Modus auf allen sekundären CA Enterprise Log Manager-Servern in der Föderation.

   Agenten erkennen automatisch die Betriebsart des CA Enterprise Log Manager-Servers, der sie verwaltet.

6. Aktivieren Sie den FIPS-Modus auf dem Primär- oder Verwaltungsserver.

7. Überprüfen Sie über das Dashboard des Agenten-Explorers, dass die Agenten im FIPS-Modus ausgeführt werden.

   Sie können auch über Abfragen oder Berichte feststellen, ob die Agenten Ereignisse senden. Alternativ dazu können Sie die Registerkarte "Selbstüberwachende Ereignisse" im Bereich "Systemstatus-Service" überprüfen.

Wenn Sie für einen vorhandenen Agenten ein Upgrade auf r12.1 SP1 durchführen, aktualisiert die Verarbeitung von automatischen Software-Updates den Agenten standardmäßig im Nicht-FIPS-Modus. Sie legen den FIPS-Modus für den CA Enterprise Log Manager-Server fest, der einen Agenten verwaltet. Ein Agent erkennt den FIPS-Modus des Servers, der ihn verwaltet, und startet sich bei Bedarf im entsprechenden Modus neu. Verwenden Sie das Dashboard des Agenten-Explorers in der CA Enterprise Log Manager-Benutzeroberfläche, um den FIPS-Modus eines Agenten anzuzeigen. Dazu benötigen Sie Administratorrechte. Weitere Informationen zu Upgrades finden Sie im Abschnitt zur Installation von CA Enterprise Log Manager des *Implementierungshandbuchs*, oder in der Online-Hilfe für Agentenverwaltungsaufgaben.

Weitere Informationen:

Aktivieren des Betriebs im FIPS-Modus (siehe Seite 91)
Anzeigen des Agenten-Dashboards (siehe Seite 93)

Voraussetzungen für ein Upgrade der FIPS-Unterstützung

Die folgenden Punkte sind Voraussetzungen für ein Upgrade von CA Enterprise Log Manager, um FIPS 140-2 zu unterstützen:

- Installation von CA Enterprise Log Manager r12.0 SP3 oder von r12.1
- Upgrade auf CA Enterprise Log Manager r12.1 SP1 über automatisches Software-Update

Weitere Informationen:

Hinzufügen eines neuen CA Enterprise Log Manager-Servers zu einer bereits vorhandenen Föderation, in der FIPS-Modus aktiviert ist (siehe Seite 94)

Upgrade-Richtlinien

Die folgenden Richtlinien gelten für Upgrades auf CA Enterprise Log Manager mit FIPS-Unterstützung:

- Wenn die Föderation mehr als einen CA Enterprise Log Manager-Server enthält, führen Sie das Upgrade auf r12.1 SP1 zuerst für den Primärserver oder Verwaltungsserver von CA Enterprise Log Manager durch. Danach können Sie das Upgrade für alle anderen Server in gewünschter Reihenfolge durchführen. Wenn das Upgrade durchgeführt wurde, starten die Server nur im Nicht-FIPS-Modus. Nur ein Benutzer mit Administratorrechten kann den Betriebsmodus manuell abändern und somit den FIPS-Modus aktivieren.

  Wichtig! Wechseln Sie während der Verarbeitung von automatischen Software-Updates nicht den FIPS-Modus auf einem sekundären CA Enterprise Log Manager-Server. Dadurch kann die Verarbeitung von automatischen Software-Updates fehlschlagen.

- CA Enterprise Log Manager-Server der Version r12.1 SP1 können mit r12.1-Agenten kommunizieren, aber FIPS-Unterstützung auf Agentenebene ist erst verfügbar, wenn Sie ein Upgrade auf r12.1 SP1 durchführen.

- Wenn Sie den FIPS-Modus aktivieren, können nur FIPS-aktivierte Agenten der Version r12.1 SP1 und höher mit dem CA Enterprise Log Manager-Server kommunizieren. Wenn Sie den *Nicht*-FIPS-Modus aktivieren, ist der CA Enterprise Log Manager-Server komplett abwärtskompatibel mit älteren Agenten, aber der Betrieb im FIPS-Modus ist nicht verfügbar. Wir empfehlen, dass Sie *nur* Agenten mit der Version r12.1 SP1 installieren, nachdem Sie für Ihre CA Enterprise Log Manager-Server ein Upgrade auf r12.1 SP1 durchgeführt haben.

- Mit einem CA Enterprise Log Manager-Server verknüpfte Agenten erkennen Änderungen des Servermodus automatisch und starten sich im entsprechenden Modus neu.

- Das Hinzufügen eines neuen CA Enterprise Log Manager-Servers zu einer vorhandenen Föderation, in der FIPS-Modus aktiviert ist, benötigt eine spezielle Handhabung. Weitere Informationen zum Hinzufügen eines neuen CA Enterprise Log Manager-Servers zu einer bereits vorhanden Föderation finden Sie im *Implementierungshandbuch*.

Durchführen von Upgrades für CA EEM-Remote-Server

Wenn Sie einen eigenständigen CA EEM-Server bei Ihrer CA Enterprise Log Manager-Installation verwenden, führen Sie zuerst für diesen Server ein Upgrade auf FIPS-Unterstützung durch, bevor Sie andere CA Enterprise Log Manager-Server oder -Agenten aktualisieren. Weitere Informationen und Anweisungen finden Sie in den Anleitungen im *CA EEM-Handbuch – Erste Schritte*.

Deaktivieren des ODBC- und JDBC-Zugriffs auf den Ereignisprotokollspeicher

Sie können den Zugriff von ODBC und JDBC auf Ereignisse im Ereignisprotokollspeicher verhindern, indem Sie die Optionen im Dialogfeld "Konfiguration des ODBC-Dienstes" verwenden. Wenn Sie Ihr föderiertes Netzwerk im FIPS-Modus ausführen möchten, deaktivieren Sie den ODBC- und JDBC-Zugriff, um in Übereinstimmung mit Bundesstandards zu bleiben.

So deaktivieren Sie den ODBC- und JDBC-Zugriff

1. Melden Sie sich beim CA Enterprise Log Manager-Server an, und wählen Sie die Registerkarte "Verwaltung" aus.
2. Klicken Sie auf die Unterregisterkarte "Services" und erweitern Sie dann den Knoten "ODBC-Service".
3. Wählen Sie den gewünschten Server aus.
4. Deaktivieren Sie das Kontrollkästchen "Dienste aktivieren" und klicken Sie anschließend auf "Speichern".

   Hinweis: Deaktivieren Sie die ODBC-Option für *alle* CA Enterprise Log Manager-Server in einer Föderation, um sicherzustellen, dass ODBC und JDBC deaktiviert wurden.

Aktivieren des Betriebs im FIPS-Modus

Sie können die FIPS-Modus-Optionen im Systemstatusdienst verwenden, um den FIPS-Modus ein- und auszuschalten. Der standardmäßige FIPS-Modus ist Nicht-FIPS. Die Administratoren unter den Benutzern müssen den FIPS-Modus für jeden CA Enterprise Log Manager-Server in einem Verbund festlegen.

Wichtig! Sie können innerhalb des gleichen Verbunds nicht mit gemischten Modi arbeiten. Server innerhalb eines Verbunds, die in einem unterschiedlichen Modus ausgeführt werden, können keine Berichts- und Abfragedaten erfassen und nicht auf die Anfragen der anderen Server antworten.

So wechseln Sie zwischen FIPS- und Nicht-FIPS-Modus

1. Melden Sie sich beim CA Enterprise Log Manager-Server an.
2. Klicken Sie auf der Registerkarte "Verwaltung" auf die Unterregisterkarte "Services".
3. Erweitern Sie den Knoten "Systemstatus" und wählen Sie den gewünschten CA Enterprise Log Manager-Server aus.

   Das Dialogfeld zur Konfiguration des Systemstatusdienstes wird angezeigt.
4. Wählen Sie den gewünschten FIPS-Modus - "Ein" oder "Aus" - aus der Dropdown-Liste aus.
5. Klicken Sie auf "Speichern".

   Der CA Enterprise Log Manager-Server startet im ausgewählten Modus neu. Sie können sich erneut anmelden, um vom Agenten-Explorer aus den FIPS-Modus des Agenten anzuzeigen.
6. Überprüfen Sie den Betriebsmodus des CA Enterprise Log Manager-Servers, indem Sie nach dem Neustart des Servers das Dialogfeld des Systemstatusdienstes kontrollieren.

   Sie können auch selbstüberwachende Ereignisse verwenden, um zu überprüfen, ob der CA Enterprise Log Manager-Server im gewünschten Modus gestartet wurde. Suchen Sie auf der Registerkarte "Selbstüberwachende Ereignisse" im Dialogfeld "Systemstatus" nach folgenden Ereignissen:

   ```
   FIPS-Modus des Servers erfolgreich auf EIN geschaltet
   FIPS-Modus des Servers erfolgreich auf AUS geschaltet
   FIPS-Modus des Servers konnte nicht auf EIN geschaltet werden
   FIPS-Modus des Servers konnte nicht auf AUS geschaltet werden
   ```

Wenn der FIPS-Modus für den Primär- oder Management-Server deaktiviert wird, geben die Abfragen und Berichte der Verbünde keine Daten mehr zurück. Außerdem werden keine geplanten Berichte ausgeführt. Diese Bedingung hält an, bis alle Server im Verbund wieder im gleichen Modus laufen.

Hinweis: FIPS auf dem Management- oder Remote-CA EEM-Server zu deaktivieren, stellt eine der Anforderungen dafür dar, zu einem Verbund von im FIPS-Modus ausgeführten Servern einen neuen CA Enterprise Log Manager-Server hinzuzufügen.

Weitere Informationen:

Deaktivieren des ODBC- und JDBC-Zugriffs auf den Ereignisprotokollspeicher (siehe Seite 91)

Anzeigen des Agenten-Dashboards

Sie können das Agenten-Dashboard anzeigen, um den Status von Agenten in Ihrer Umgebung anzuzeigen. Das Dashboard zeigt auch Einzelheiten wie den aktuellen FIPS-Modus (FIPS oder Nicht-FIPS) sowie Nutzungsdetails an. Diese schließen die Zahl der geladenen Ereignisse pro Sekunde, die CPU-Auslastung in Prozent und das Datum und die Uhrzeit der letzten Aktualisierung ein.

So zeigen Sie das Agenten-Dashboard an:

1. Klicken Sie auf die Registerkarte "Verwaltung" und anschließend auf die Unterregisterkarte "Protokollerfassung".

   Die Ordnerliste "Protokollerfassung" wird angezeigt.

2. Wählen Sie den Ordner "Agenten-Explorer" aus.

   Im Detailfenster werden Schaltflächen für die Agentenverwaltung angezeigt.

3. Klicken Sie auf "Agentenstatusüberwachung und -Dashboard": 

   Das Agentensuchfenster wird geöffnet. Hier wird der Status aller verfügbaren Agents in einem Diagramm aufgeführt. Beispiel:

   ```
   Summe: 10 Wird ausgeführt: 8 Ausstehend: 1 Beendet: 1 Antwortet nicht: 0
   ```

4. (Optional) Wählen Sie ein Suchkriterium für Agenten aus, um die Liste der angezeigten Agenten einzugrenzen. Sie können unter den folgenden Kriterien wählen:

   - Agentengruppe: Gibt nur die Agenten zurück, die der ausgewählten Gruppe zugewiesen sind
   - Plattform: Gibt nur die Agenten zurück, die auf der ausgewählten Plattform ausgeführt werden
   - Status: Gibt nur Agenten mit dem ausgewählten Status zurück, z. B. "Wird ausgeführt".
   - Agentennamensmuster: Gibt nur die Agenten zurück, die das angegebene Namensmuster enthalten

5. Klicken Sie auf "Status anzeigen".

   Eine Liste der Agenten, die den Suchkriterien entsprechen, wird eingeblendet. Sie enthält unter anderem folgende Informationen:

   - Name und Version des lokalen Connectors
   - Aktueller CA Enterprise Log Manager-Server
   - FIPS-Modus des Agenten (FIPS oder Nicht-FIPS)
   - Letztes aufgezeichnetes Ereignis pro Sekunde, das vom Agenten verarbeitet wurde

- Letzter aufgezeichneter CPU-Auslastungswert
- Letzter aufgezeichneter Speicherauslastungswert
- Aktuelle Konfigurationsaktualisierung
- Status der Konfigurationsaktualisierung

Hinzufügen eines neuen CA Enterprise Log Manager-Servers zu einer bereits vorhandenen Föderation, in der FIPS-Modus aktiviert ist

Es gelten einige besondere Richtlinien für das Hinzufügen von neuen CA Enterprise Log Manager-Server in eine Server-Föderation, die bereits im FIPS-Modus ausgeführt wird. Neu installierte CA Enterprise Log Manager-Server werden standardmäßig im *Nicht*-FIPS-Modus ausgeführt, es sei denn, Sie geben den FIPS-Modus ausdrücklich während der Installation an. Server im Nicht-FIPS-Modus können nicht mit Server im FIPS-Modus kommunizieren.

Als Teil der Installation muss ein neuer CA Enterprise Log Manager-Server bei dem lokalen, auf dem Verwaltungsserver eingebetteten CA EEM-Server oder bei einem eigenständigen CA EEM-Remote-Server registriert werden. Der Prozess für das Hinzufügen eines Servers zu einem vorhandenen Netzwerk basiert auf dem Standort des CA EEM-Verwaltungsservers.

Nehmen Sie den folgenden Ablauf zur Kenntnis:

Der Prozess für das Hinzufügen eines neuen Servers umfasst die folgenden Schritte:

1. Aktivieren Sie den Nicht-FIPS-Modus auf dem CA Enterprise Log Manager-Verwaltungsserver (Primärserver) oder auf dem CA EEM-Remote-Server.
2. Unter Verwendung des ISO-Images oder der DVDs für CA Enterprise Log Manager 12.1 SP 1 oder höher installieren Sie einen oder mehrere neue CA Enterprise Log Manager-Sekundärserver.

   Wichtig! Vergewissern Sie sich, dass Sie während der Installation den FIPS-Modus angeben. Anderenfalls wird der neu installierte Server nicht in der Lage sein, mit dem Verwaltungsserver oder mit dem CA EEM-Remoteserver zu kommunizieren, und Sie müssen den neuen CA Enterprise Log Manager-Sever erneut installieren.

Da der CA Enterprise Log Manager-Verwaltungsserver bzw. der CA EEM-Remotserver im FIPS-Modus ausgeführt werden, kann der neue CA Enterprise Log Manager-Server registriert und in die Föderation aufgenommen werden.

Weitere Informationen:

Aktivieren des Betriebs im FIPS-Modus (siehe Seite 91)
Anzeigen des Agenten-Dashboards (siehe Seite 93)

Installationshinweise für ein System mit SAN-Laufwerken

Wenn Sie das Betriebssystem für die CA Enterprise Log Manager-Anwendung auf einem System mit SAN-Laufwerken installieren, treffen Sie Vorsichtsmaßnahmen, um zu verhindern, dass CA Enterprise Log Manager auf einem SAN-Laufwerk installiert wird. Diese Installation würden fehl schlagen.

Folgen Sie einem der folgenden Ansätze, um eine erfolgreiche Installation zu garantieren:

- Deaktivieren Sie die SAN-Laufwerke. Installieren Sie das Betriebssystem und die CA Enterprise Log Manager-Anwendung wie gewohnt. Konfigurieren Sie dann die SAN-Laufwerke für CA Enterprise Log Manager und starten Sie CA Enterprise Log Manager erneut, um die SAN-Konfiguration zu aktivieren.
- Lassen Sie die SAN-Laufwerke aktiviert. Beginnen Sie mit der Betriebssysteminstallation. Verlassen Sie diese Prozedur, wie beschrieben, um den in der Kickstart-Datei angegebenen Betriebsablauf zu verändern. Setzen Sie den Installationsprozess fort und schließen Sie ihn wie angegeben ab.

Installieren mit deaktivierten SAN-Laufwerken

CA Enterprise Log Manager unterstützt gegenwärtig die Verwendung von gefixten Hardwarekonfigurationen von Dell, IBM und HP. Im folgenden Beispiel wird angenommen, dass die Hardware aus HP-Blade-Servern besteht, die eine QLogic Fiber Channel-Karte zur Verbindung mit einem Storage Area Network (SAN) für die Datenspeicherung verwenden. Die HP-Blade-Servern verfügen über SATA-Laufwerke und sind als RAID-1 (gespiegelt) konfiguriert.

Wenn Sie die Kickstart-Startdatei im Originalzustand verwenden, stellen Sie sicher, dass die SAN-Laufwerke deaktiviert sind, bevor die Installation beginnt. Starten Sie den Installationsprozess mit der OS5-DVD und schließen Sie die Installation, wie angegeben, ab.

Hinweis: Wenn Sie die Installation mit aktivierten SAN-Laufwerken starten, wird CA Enterprise Log Manager auf dem SAN installiert. In diesem Fall erscheint ein rotes Fenster mit der Meldung "Ungültiger Opcode", nachdem CA Enterprise Log Manager erneut gestartet wurde.

Verwenden Sie den folgenden Ablauf, um eine CA Enterprise Log Manager-Anwendung auf einem System mit SAN-Laufwerken zu installieren, wobei Sie die SAN-Laufwerke deaktivieren, bevor Sie das Betriebssystem installieren.

1. Deaktivieren Sie die SAN-Laufwerke.
2. Installieren Sie das Betriebssystem auf der Anwendung.
3. Installieren Sie den CA Enterprise Log Manager-Server.
4. Richten Sie eine Multipfadkonfiguration für SAN-Speicher ein.
5. Erstellen Sie logisches Volume.
6. Bereiten Sie das logische Volume für CA Enterprise Log Manager vor.
7. Starten Sie die CA Enterprise Log Manager erneut.
8. Überprüfen Sie den Erfolg der Installation.

Wenn Sie das Betriebssystem mit deaktivierten SAN-Laufwerken installieren, arbeiten Sie mit den folgenden Dateien:

lvm.conf

Die Konfigurationsdatei für den Logical Volume Manager von Linux (LVM2).

multipath.conf (/etc/multipath.conf)

Die Konfigurationsdatei für den Linux-Multipfad.

fstab (/etc/fstab)

Die Datei der Dateisystemtabelle, die Geräte zu Verzeichnissen in einem Linux-System zuordnet.

Deaktivieren des SAN-Laufwerks

Verwenden Sie die empfohlenen Prozeduren des Anbieters Ihres SAN-Laufwerks, um die SAN-Laufwerke auf der Hardware, auf der Sie die Soft-Appliance installieren möchten, zu deaktivieren.

Deaktivieren Sie die SAN-Laufwerke, bevor Sie das Soft-Appliance-BS oder die CA Enterprise Log Manager-Anwendung installieren.

Einrichten einer Multipfadkonfiguration für SAN-Speicher

Der Multipfad muss für CA Enterprise Log Manager-Systeme konfiguriert werden, die auf einem RAID-System installiert sind, das SAN-Speicher verwenden soll. Physische Datenträger auf dem SAN werden in Speicherplätze, sogenannte logische Einheitennummern (LUNs), aufgeteilt.

So richten Sie eine Multipfadkonfiguration für SAN-Speicher ein

1. Melden Sie sich bei der CA Enterprise Log Manager-Anwendung an und wechseln Sie den Benutzer auf "root" (su to root).
2. (Optional) Erstellen Sie eine Verzeichnisliste von "/dev/mapper", um den Konfigurationsstatus anzuzeigen, bevor der Multipfad und logische Volumes eingerichtet werden. Die Ergebnisse ähneln den folgenden Angaben:

```
drwxr-xr-x  2 root root     120 Jun 18 12:09 .
drwxr-xr-x 11 root root    3540 Jun 18 16:09 ..
crw-------  1 root root  10, 63 Jun 18 12:09 control
brw-rw----  1 root disk 253,  0 Jun 18 16:09 VolGroup00-LogVol00
brw-rw----  1 root disk 253,  2 Jun 18 12:09 VolGroup00-LogVol01
brw-rw----  1 root disk 253,  1 Jun 18 16:09 VolGroup00-LogVol02
```

3. Öffnen Sie die Datei "... /etc./multipath.conf" zur Bearbeitung und fahren Sie folgendermaßen fort:
   a. Fügen Sie den folgenden Abschnitt unter "device {" für jede vom SAN-Administrator bereitgestellte LUN hinzu:

```
device {
    vendor                "NETAPP"
    product               "LUN"
    path_grouping_policy  multibus
    features              "1 queue_if_no_path"
    path_checker          readsector0
    path_selector         "round-robin 0"
    failback              immediate
    no_path_retry         queue
         }
```

b. Entfernen Sie die Kommentarmarkierung des Abschnitts "blacklist" für alle Geräte. Dieser Abschnitt aktiviert Multipfade auf Standardgeräten.

```
blacklist {
    devnode "^(ram|raw|loop|fd|md|dm-|sr|scd|st)[0-9]*"
    devnode "^hd[a-z]"
    devnode "^cciss!c[0-9]d[0-9]*"
}
```

c. Speichern und schließen Sie die Datei "multipath.conf".

4. Stellen Sie sicher, dass Multipfad aktiviert wurde und dass die LUNs aufgelistet werden, indem Sie Folgendes ausführen:

```
multipath -l
```

Hinweis: Pfade werden als "mpath0" und "mpath1" angezeigt. Wenn die LUNs nicht angezeigt werden, starten Sie neu und führen Sie "multipath" erneut aus.

5. Zeigen Sie die verfügbaren Laufwerke an.

```
fdisk -l
```

6. Erstellen Sie eine Liste der verfügbaren Partitionen und überprüfen Sie, dass "mpath0" und "mpath1" aufgelistet werden.

```
ls -la /dev/mapper
```

7. Ordnen Sie die erste Partition folgendermaßen zu:

```
kpartx -a /dev/mapper/mpath0
```

8. Ordnen Sie die zweite Partition folgendermaßen zu:

```
kpartx -a /dev/mapper/mpath1
```

Erstellen eines logischen Volumes

Sie können Software zur Verwaltung der Volumes verwenden, um mehrere LUNs in ein logisches Volume zu vereinen, auf das CA Enterprise Log Manager zugreifen kann. Logical Volume Manager (LVM) verwaltet Festplattenlaufwerke und ähnliche Massenspeichergeräte auf dem Linux-Betriebssystem. Mit dem LVM erstellte Speicherspalten können angepasst oder auf die Backend-Geräte, wie SAN-Speicher, verschoben werden.

So erstellen Sie logische Volumes

1. Erstellen Sie das erste physische Volume:

```
pvcreate /dev/mapper/mpath0
```

2. Erstellen Sie das zweite physische Volume:

```
pvcreate /dev/mapper/mpath1
```

3. Zeigen Sie alle physischen Volumes auf dem System an:

   ```
   pvdisplay
   ```

4. Erstellen Sie die Volume-Gruppe "VolGroup01". Die Volume-Gruppe "VolGroup00" ist bereits vorhanden).

   ```
   vgcreate VolGroup01 /dev/mapper/mpath0 /dev/mapper/mpath1
   ```

   Hinweis: Dieser Befehl erstellt ein Volume und fügt die zwei physischen Volumes in die Gruppe.

5. Erstellen Sie ein logisches Volume innerhalb der Volume-Gruppe:

   ```
   lvcreate –n LogVol00 –l 384030 VolGroup01
   ```

6. Erstellen Sie ein Dateisystem:

   ```
   mkfs –t ext3 /dev/VolGroup01/LogVol00
   ```

Vorbereiten des logischen Volumes für CA Enterprise Log Manager

Nachdem Sie ein logisches Volume erstellt haben, übernehmen Sie die erwartete Verzeichnisstruktur und weisen Sie die von CA Enterprise Log Manager benötigten Besitzrechte und Gruppenvereinigungen zu. Verwenden Sie den vi-Texteditor, um die Datei "fstab" zu ändern, damit sie auf das von Ihnen erstellte logische Volume gerichtet ist. Anschließend laden Sie das neue Datenverzeichnis.

So bereiten Sie logische Volumes für CA Enterprise Log Manager vor

1. Erstellen Sie ein temporäres Verzeichnis, /data1, ändern Sie die Besitzrechte des Verzeichnisses "/data1" auf "caelmservice", und ändern Sie die mit diesem Verzeichnis verknüpfte Gruppe auf "caelmservice":

   ```
   mkdir /data1
   chown caelmservice /data1
   chgrp caelmservice /data1
   ```

2. Halten Sie die iGateway-Prozesse des CA Enterprise Log Manager-Servers an:

   ```
   /opt/CA/SharedComponents/iTechnology/S99igateway stop
   ```

3. Ändern Sie die Verzeichnisse auf das Verzeichnis, in dem der CA Enterprise Log Manager-Agent ausgeführt wird, halten Sie den Agenten an und stellen Sie sicher, dass der Dienst angehalten wurde:

   ```
   cd /opt/CA/ELMAgent/bin/
   ./caelmagent –s
   ps –ef | grep /opt/CA
   ```

4. Wechseln Sie ins Verzeichnis "/directory".
5. Laden Sie das neue Dateisystem auf "/data1", kopieren Sie den Inhalt des Verzeichnisses "/data" ins Verzeichnis "/data1", und überprüfen Sie, dass die zwei Verzeichnisse übereinstimmen:

   ```
   mount –t ext3 /dev/VolGroup01/LogVol00 /data1
   cp –pR /data/* /data1
   diff –qr /data /data1
   ```

6. Entladen Sie den vorhandenen Datenbereitstellungspunkt und entladen Sie anschließend den Bereitstellungspunkt "data1":

   ```
   umount /data
   umount /data1
   ```

7. Löschen Sie das Verzeichnis "/data" und benennen Sie das Verzeichnis "/data1" um in "/data".

   ```
   rm –rf /data
   mv /data1 data
   ```

8. Ändern Sie in "/etc/fstab" die Zeile, die sich auf das Verzeichnis "/data" bezieht und richten Sie es auf das neue logischen Volume. Das heißt, ändern Sie "/dev/VolGroup00/LogVol02" in "/dev/VolGroup01/LogVol00". Die veränderten Daten werden in Fettdruck in der folgenden Wiedergabe der Beispieldatei "fstab" angezeigt.

Gerätename	**Bereitstellungspunkt**	**Typ des Dateisystems**	**Optionen**	**Speicherfreq. / Durchlaufnr.**
Keine	/dev/VolGroup00/LogVol00/	ext3	Standard	1 1
Keine	**/dev/VolGroup01/LogVol00/data**	ext3	Standard	2 1
LABEL=/boot	/boot	ext3	Standard	2 1
tmpfs	/dev/shm	tmpfs	Standard	0 0
devpts	/dev/pts	devpts	gid=5,mode=620	0 0
sysfs	/sys	sysfs	Standard	0 0
proc	/proc	proc	Standard	0 0
Keine	/dev/VolGroup00/LogVol01	swap	Standard	0 0

9. Laden Sie das neue Datenverzeichnis und stellen Sie sicher, dass alle Partitionen in "/etc/fstab" geladen wurden:

   ```
   mount -a
   ```

   ```
   mount
   ```

Neustarten des CA Enterprise Log Manager-Servers

Nachdem Sie ein logisches Volume erstellt haben, starten Sie CA Enterprise Log Manager neu, damit Sie das logische Volume verwenden können. Um den ordnungsgemäßen Ablauf zu überprüfen, durchsuchen Sie CA Enterprise Log Manager und zeigen Sie Ereignisse an, die von der Abfrage "Alle Ereignisse des Systems - Details" zurückgegeben wurden.

So starten Sie CA Enterprise Log Manager-Server neu:

1. Starten Sie die iGateway-Prozesse des CA Enterprise Log Manager-Servers:

   ```
   /opt/CA/SharedComponents/iTechnology/S99igateway start
   ```

2. Starten Sie den ELMAgent-Dienst
   ```
   /opt/CA/ELMAgent/bin/caelmagent –b
   ```

3. Starten Sie den CA Enterprise Log Manager-Server neu.

Installieren mit aktivierten SAN-Laufwerken

Das Thema "Beispiel: Festlegen des SAN-Speichers für CA Enterprise Log Manager" enthält die Empfehlungen, die SAN-Laufwerke (LUNs) zu deaktivieren, bevor das Betriebssystem auf der CA Enterprise Log Manager-Anwendung installiert wird.

Alternativ dazu können Sie die SAN-Laufwerke auch aktiviert lassen, und die Kickstart-Datei "ca-elm-ks.cfg" mit einem ISO-Editionstool ändern, nachdem Sie die Betriebssysteminstallation gestartet haben. Diese Änderung stellt sicher, dass die Installation und der Start auf der lokalen Festplatte und nicht auf SAN durchgeführt wird.

So starten Sie von der lokalen Festplatte (nicht SAN)

1. Starten Sie den Server mit der Installations-DVD für das Betriebssystem.
2. Machen Sie Angaben in der ersten Eingabeaufforderung nach dem Tastaturtyp.
3. Drücken Sie auf Alt+F2, um die Eingabeaufforderung für Anaconda/Kickstart anzuzeigen.

4. Geben Sie Folgendes ein:

   ```
   list-hardrives
   ```

   Die Liste der verfügbaren Laufwerke wird angezeigt und kann dem hier aufgeführten Beispiel ähnlich sein:

   ```
   cciss/c0d0 – 68GB RAID 1 (cciss is HP Smart Array)
   Sda – 500GB SAN  (sda – h is the SAN Multipathed)
   Sdb – 500GB SAN
   Sdc – 500GB SAN
   Sdd – 500GB SAN
   Sde – 500GB SAN
   Sdf – 500GB SAN
   Sdg – 500GB SAN
   Sdh – 500GB SAN
   ```

5. Identifizieren Sie die lokale Festplatte. In diesem Fall "cciss/c0d0".

6. Führen Sie die folgenden Schritte aus:

   a. Öffnen Sie die Kickstart-Datei "ca-elm-ks.cfg" für das CA Enterprise Log Manager-Betriebssystem zur Bearbeitung. Verwenden Sie einen ISO-Editor.

   b. Suchen Sie die folgende Zeile zur Bearbeitung:

      ```
      bootloader --location=mbr --driveorder=sda,sdb
      ```

      Verändern Sie sie wie folgt:

      ```
      bootloader --location=mbr --driveorder=cciss/c0d0
      ```

      Mit dieser Änderung wird nur von der lokalen Festplatte gestartet.

   c. Suchen Sie die folgenden Zeilen zur Bearbeitung:

      ```
      clearpart --all --initlabel
      part /boot --fstype "ext3" --size=100
      part pv.4 --size=0 –grow
      ```

      Verändern Sie sie wie folgt:

      ```
      part /boot --fstype "ext3" --size=100 --ondisk cciss/c0d0
      part pv.4 --size=0 --grow --ondisk cciss/c0d0
      ```

      Mit diesen Änderungen in den Zeilen der Partitionsdefinition wird sichergestellt, dass die Partitionen auf dem Datenträger "cciss/c0d0" nach Namen erstellt werden. Mit "--ondisk" werden die vorhandenen Variablen für "$disk1" und "$disk2" ersetzt.

   d. Entfernen Sie bei Bedarf die "IF/When"-Klausel für die Anzahl der Laufwerke, und behalten Sie nur den ersten Teil der Festplattenbefehle bei (Zeilen 57 - 65).

   e. Speichern Sie das neue ISO-Image.

7. Verlassen Sie die Eingabeaufforderung "Anaconda" und kehren Sie zu den Eingabeaufforderungen der Betriebssysteminstallation zurück.
8. Fahren Sie unter Verwendung der angegebenen Vorgehensweisen mit der Installation fort.

Erste CA Enterprise Log Manager-Serverkonfigurationen

Bei der Installation des ersten CA Enterprise Log Manager-Servers wird ein Anwendungsname mit dem Standardwert CAELM erstellt. Dieser Name wird während der Installation beim eingebetteten CA EEM-Server registriert. Wenn bei nachfolgenden Installationen derselbe Anwendungsinstanzname verwendet wird, verwaltet der CA Enterprise Log Manager-Verwaltungsserver alle Konfigurationen unter diesem einen Anwendungsinstanznamen.

Nach Abschluss der Installation verfügt der Server über ein Betriebssystem und einen CA Enterprise Log Manager-Server. Das 32-Bit-Betriebssystem unterstützt sowohl 32-Bit- als auch 64-Bit-Hardware. Die anfänglichen Konfigurationen umfassen folgende Bereiche:

- Standardbenutzerkonten
- Standardverzeichnisstruktur
- benutzerspezifisches Betriebssystem-Image
- Standardportzuweisungen

Standardbenutzerkonten

Während der CA Enterprise Log Manager-Installation wird der standardmäßige administrative Benutzer "caelmadmin" mit eigenem Kennwort erstellt. Für den direkten Zugriff auf den Hostserver müssen Sie dieses Konto für die Anmeldung verwenden, da die Anmeldefunktionen des "root"-Kontos nach der Installation eingeschränkt werden. Mit dem "caelmadmin"-Konto ist lediglich die Anmeldung möglich. Für den Zugang zu den Hilfsprogrammen für die Systemverwaltung auf Betriebssystemebene müssen Sie dann Benutzer auf das "root"-Konto mit dem Kennwort dieses Kontos umschalten.

Das Standardkennwort für dieses Konto entspricht dem Kennwort, das Sie für das "EiamAdmin"-Konto angelegt haben. Ändern Sie das Kennwort für das "caelmadmin"-Konto möglichst sofort nach der Installation.

Während der Installation wird ferner das Standardservice-Benutzerkonto "caelmservice" erstellt, mit dem Sie sich *nicht* beim System anmelden können. Sie können ggf. Benutzer auf dieses Konto umschalten, um Prozesse zu starten und zu stoppen. Der iGateway-Prozess und der eingebettete CA EEM-Server (sofern auf dem CA Enterprise Log Manager-Server installiert) werden unter diesem Benutzerkonto ausgeführt, wodurch eine zusätzliche Sicherheitsebene bereitgestellt wird.

Der iGateway-Prozess wird nicht unter einem "root"-Benutzerkonto ausgeführt. Die Portweiterleitung wird automatisch aktiviert, so dass HTTPS-Anforderungen auf Port 80 und Port 443 neben Port 5250 auf die CA Enterprise Log Manager-Benutzeroberfläche zugreifen können.

Standardverzeichnisstruktur

Die Softwarebinärdateien werden bei der CA Enterprise Log Manager-Installation im Verzeichnispfad "/opt/CA" abgelegt. Falls das System über ein zweites Festplattenlaufwerk verfügt, wird dieses als "/data" konfiguriert. Der Installationsvorgang erstellt einen symbolischen Link von dem Verzeichnis "/opt/CA/LogManager/data" zu dem Verzeichnis "/data". Im Folgenden finden Sie eine Übersicht über die standardmäßige Installationsverzeichnisstruktur:

Dateitypen	**Verzeichnis**
iTechnology-bezogene Dateien (iGateway)	/opt/CA/SharedComponents/iTechnology
CA Enterprise Log ManagerEEM-Server-bezogene Dateien	/opt/CA/LogManager/EEM
CA Enterprise Log Manager-Installationsdateien	/opt/CA/LogManager/install
Datendateien (Links zu "/data" im Falle mehrerer Laufwerke)	/opt/CA/LogManager/data
Protokolldateien	/opt/CA/SharedComponents/iTechnology

Unter normalen Umständen müssen Sie nur auf das Hilfsprogramm *ssh* auf dem CA Enterprise Log Manager-Server zugreifen, wenn Sie Archivdateien für die Sicherung oder langfristige Speicherung verschieben oder Festplattenlaufwerke hinzufügen möchten.

Benutzerspezifisches Betriebssystem-Image

Bei der Installation wird das Betriebssystem angepasst, indem ein Minimal-Image erstellt und der Zugriff auf so wenige Kanäle wie möglich eingeschränkt wird. Nicht unbedingt erforderliche Services werden nicht installiert. Der CA Enterprise Log Manager-Server hört eine kleine Anzahl von Ports ab und deaktiviert explizit nicht verwendete Ports.

Während der Installation des Betriebssystems erstellen Sie ein Kennwort für das "root"-Konto. Nach Abschluss der CA Enterprise Log Manager-Installation wird das "root"-Konto gesperrt, so dass keine weitere Anmeldung mit diesem Konto möglich ist. Der CA Enterprise Log Manager-Installationsvorgang erstellt den Standardbenutzer *caelmadmin*, der lediglich das Recht zur Anmeldung besitzt.

Um auf "root"-Ebene auf den CA Enterprise Log Manager-Server zuzugreifen, melden Sie sich mit diesem Konto beim Server an und schalten Benutzer dann auf das "root"-Konto um, damit diese Zugriff auf Verwaltungstools erhalten. Falls Sie sich als "root"-Benutzer anmelden möchten, müssen Sie also das Kennwort für den *caelmadmin*- und den *root*-Benutzer kennen.

Mit CA Enterprise Log Manager wird keine weitere Sicherheitssoftware installiert. Um eine optimale Leistung zu erzielen, sollten auf dem CA Enterprise Log Manager-Server keine weiteren Anwendungen installiert werden.

Standardportzuweisungen

Der CA Enterprise Log Manager-Server ist standardmäßig so konfiguriert, dass er unter Verwendung des HTTPS-Protokolls Port 5250 sowie Port 80 und Port 443 abhört. Da CA Enterprise Log Manager-Prozesse und -Daemons nicht unter dem "root"-Konto ausgeführt werden, können sie keine Ports unterhalb von Port 1024 öffnen. Daher wird bei der Installation automatisch eine Umleitung (über "iptables") erstellt, mit der die an den Ports 80 und 443 eingehenden Benutzerschnittstellenanforderungen an Port 5250 umgeleitet werden.

Der Syslog-Daemon des lokalen Betriebssystems des CA Enterprise Log Manager-Servers wird nicht konfiguriert, da CA Enterprise Log Manager den Systemstatus mit seinen eigenen selbstüberwachenden Ereignissen verfolgt. Sie können mit Hilfe der selbstüberwachenden Ereignisse andere lokale Ereignisse anzeigen und Berichte zu Aktionen auf dem lokalen CA Enterprise Log Manager-Server erstellen.

Im Folgenden finden Sie eine Übersicht über die in der CA Enterprise Log Manager-Umgebung verwendeten Ports:

Port	Komponente	Beschreibung
53	CA Enterprise Log Manager-Server	TCP/UDP-Port, der für die DNS-Kommunikation verfügbar sein muss, um Hostnamen für IP-Adressen von Servern aufzulösen, zum Beispiel dem CA Enterprise Log Manager-Server, dem Remote-CA EEM-Server, wenn konfiguriert, und dem NTP-Server, wenn Sie NTP-Zeitsynchronisation zum Zeitpunkt der Installation ausgewählt haben. DNS-Kommunikation wird nicht benötigt, wenn Sie Hostnamen zu IP-Adressen in der lokalen Datei "/etc/hosts" zuweisen.
80	CA Enterprise Log Manager-Server	TCP-Kommunikation mit der Benutzerschnittstelle des CA Enterprise Log Manager-Servers über HTTPS; automatische Umleitung an Port 5250.
111	Portmapper (SAPI)	Audit-Client-Kommunikation mit dem Portmapper-Prozess zum Empfang dynamischer Portzuweisungen.
443	CA Enterprise Log Manager-Server	TCP-Kommunikation mit der Benutzerschnittstelle des CA Enterprise Log Manager-Servers über HTTPS; automatische Umleitung an Port 5250.
514	Syslog	Standardmäßiger UDP-Syslog-Listening-Port; dieser Portwert kann geändert werden. Um den Standardagenten als Nicht-Root-Benutzer auszuführen, wird der Standardport auf 40514 gesetzt, und die Installation wendet eine Firewall-Regel zum CA Enterprise Log Manager-Server an.
1468	Syslog	Standardmäßiger TCP-Syslog-Listening-Port; dieser Portwert kann geändert werden.

Port	Komponente	Beschreibung
2123	DXadmin	CA-Directory-LDAP-DXadmin-Port, falls Sie einen CA EEM-Server auf dem gleichen physischen Server verwenden, auf dem sich auch der CA Enterprise Log Manager-Server (Verwaltungsserver) befindet.
5250	CA Enterprise Log Manager-Server	TCP-Kommunikation mit der Benutzerschnittstelle des CA Enterprise Log Manager-Servers unter Verwendung von iGateway. TCP-Kommunikation zwischen: ■ CA Enterprise Log Manager-Server und CA EEM-Server ■ Föderierten CA Enterprise Log Manager-Servern ■ Agent und CA Enterprise Log Manager-Server für Statusaktualisierungen
6789	Agent	Agent-Befehls- und Steuerungs-Listening-Port. **Hinweis:** Falls kein ausgehender Datenverkehr zulässig ist, müssen Sie diesen Port öffnen, damit Vorgänge ordnungsgemäß ablaufen können.
17001	Agent	TCP-Port für sichere Kommunikation zwischen Agent und CA Enterprise Log Manager-Server; dieser Portwert kann geändert werden. **Hinweis:** Falls kein ausgehender Datenverkehr zulässig ist, müssen Sie diesen Port öffnen, damit Vorgänge ordnungsgemäß ablaufen können.
17002	ODBC/JDBC	Für die Kommunikation zwischen ODBC- oder JDBC-Treiber und dem CA Enterprise Log Manager-Ereignisprotokollspeicher wird ein Standard-TCP-Port verwendet.
17003	Agent	TCP-Port, den der Qpid-Nachrichtenbus für r12.1-Agenten zur Kommunikation verwendet.
57000	Dispatcher SME-Listener	TCP-Port für den Dispatcher-Dienst auf dem Localhost des Agenten zum Überwachen selbstüberwachender Ereignisse zwischen Agentenprozessen.
57001	Dispatcher Ereignis-Listener	Der TCP-Port für den Dispatcher-Dienst ist SSL-fähig (ETPKI wird verwendet), um Ereignisse von Client-Connectors zu überwachen.
zufällig	SAPI	Für die Ereigniserfassung verwendete, vom Portmapper zugewiesene UDP-Ports; Sie können den SAPI-Router und -Collector auch so konfigurieren, dass ein fester Portwert über 1024 verwendet wird.

Liste der verwandten Prozesse

In der folgenden Tabelle finden Sie eine Übersicht der Prozesse, die als Teil einer CA Enterprise Log Manager-Implementierung ausgeführt werden. In der Liste nicht enthalten sind Systemprozesse, die zum jeweiligen Betriebssystem gehören.

Prozessname	Standardport	Beschreibung
caelmagent	6789, 17001	Dies ist der CA Enterprise Log Manager-Agentenprozess.
caelmconnector	Je nachdem, wonach der Prozess sucht bzw. womit er verbunden wird.	Dies ist der CA Enterprise Log Manager-Connector-Prozess. Für jeden auf einem Agenten konfigurierten Connector wird ein eigener Connector-Prozess ausgeführt.
caelmdispatcher		Dieser CA Enterprise Log Manager-Prozess verarbeitet die Ereignisübergabe und Statusinformationen zwischen Connector und Agent.
caelmwatchdog	Keiner	Der CA Enterprise Log Manager-Überwachungsprozess (Watchdog-Prozess), der andere Prozesse überwacht, um einen kontinuierlichen Betrieb zu gewährleisten.
caelm-eemsessionsponsor		Der Hauptprozess von CA EEM, der die gesamte Kommunikation mit CA EEM für lokale Sponsoren, die unter "safetynet" auf dem CA Enterprise Log Manager-Server ausgeführt werden, verwaltet. Dieser Prozess kann unter "safetynet" ausgeführt werden.
caelm-logdepot	17001	Der CA Enterprise Log Manager-Ereignisprotokollspeicherprozess, der die Ereignisspeicherung, Erstellung von Archivdateien und andere Funktionen übernimmt. Dieser Prozess kann unter "safetynet" ausgeführt werden.
caelm-sapicollector		Dies ist der SAPI-Collector-Serviceprozess. Dieser Prozess kann unter "safetynet" ausgeführt werden.
caelm-sapirouter		Dies ist der SAPI-Router-Serviceprozess. Dieser Prozess kann unter "safetynet" ausgeführt werden.

Prozessname	Standardport	Beschreibung
caelm-systemstatus		Dieser Prozess erfasst den Systemstatus zur Anzeige auf der CA Enterprise Log Manager-Benutzeroberfläche. Dieser Prozess kann unter "safetynet" ausgeführt werden.
dxadmind		CA Directory-Prozess; wird auf dem Server ausgeführt, auf dem CA EEM installiert ist.
dxserver		CA Directory-Prozess; wird auf dem Server ausgeführt, auf dem CA EEM installiert ist.
iGateway	5250	Hauptprozess von CA Enterprise Log Manager; dieser Prozess muss für die Erfassung und Speicherung von Ereignissen ausgeführt werden.
Meldungsbroker		CA Enterprise Log Manager-Prozess für die Kommunikation zwischen Agent und CA Enterprise Log Manager-Server zum Senden von Ereignissen.
oaserver	17002	CA Enterprise Log Manager-Prozess, der für die Verarbeitung von ODBC- und JDBC-Anforderungen für den Zugriff zum Ereignisprotokollspeicher auf der Serverseite ausgeführt wird.
safetynet		Das CA Enterprise Log Manager-Prozess-Framework, das den fortlaufenden Betrieb gewährleistet.
ssld		CA Directory-Prozess; wird auf dem Server ausgeführt, auf dem CA EEM installiert ist.

Betriebssystemhärtung

Die CA Enterprise Log Manager-Soft-Appliance enthält eine vereinfachte und gehärtete Version des Red Hat Linux-Betriebssystems. Die folgenden Härtungsverfahren sind enthalten:

- Der Zugriff auf SSH als Stammbenutzer wird deaktiviert.
- Die Verwendung der Tastenkombination "Strg-Alt-Entf", um den Server von der Konsole neu zu starten, ohne sich anzumelden, wird deaktiviert.
- Umleitungen werden in "iptables" für folgenden Porte angewandt:
  - TCP-Port 80 und 443 werden an 5250 umgeleitet
  - UDP-Port 514 wird an 40514 umgeleitet

- Das GRUB-Paket ist kennwortgeschützt.
- Die Installation fügt die folgenden Benutzer mit eingeschränkten Berechtigungen hinzu:
  - caelmadmin - Betriebssystemkonto mit Anmeldeberechtigung bei der CA Enterprise Log Manager-Serverkonsole
  - caelmservice - Service-Konto, unter dem die iGateway- und Agent-Prozesse laufen. Sie können sich nicht direkt mit diesem Konto anmelden

Umleiten von Firewall-Ports für Syslog-Ereignisse

Sie können den auf Standardports eintreffenden Datenverkehr an einen anderen Port umleiten, falls zwischen einem Agenten und dem CA Enterprise Log Manager-Server eine Firewall geschaltet ist.

Die bewährten Vorgehensweisen für die Sicherheit geben in diesem Fall vor, die minimale, für die Ausführung von Anwendungsprozessen und Daemons erforderliche Benutzerberechtigung zu verwenden. UNIX- und Linux-Daemons, die unter einem Nicht-Root-Konto ausgeführt werden, können keine Ports unterhalb von Port 1024 öffnen. Der standardmäßige UDP-Syslog-Port ist 514. Dies kann Probleme bereiten bei Geräten wie Routern und Switches, die nur Standardports verwenden können.

Als Lösung des Problems können Sie die Firewall so konfigurieren, dass sie Port 514 auf eintreffende Daten abhört und diese dann über einen anderen Port an den CA Enterprise Log Manager-Server sendet. Die Umleitung findet auf dem Host des Syslog-Listeners statt. Falls Sie einen nicht standardmäßigen Port verwenden möchten, müssen Sie alle Ereignisquellen so neu konfigurieren, dass Ereignisse über diesen Port gesendet werden.

So leiten Sie einen durch eine Firewall eintreffenden Ereignisstrom um:

1. Melden Sie sich als "root"-Benutzer an.
2. Öffnen Sie eine Eingabeaufforderung.
3. Geben Sie einen Befehl ein, mit dem die Ports für Ihre spezifische Firewall umgeleitet werden.

   Im Folgenden finden Sie ein Beispiel für eine Befehlszeileneingabe für das netfilter/iptables-Paketfiltertool unter Red Hat Linux:

   ```
   chkconfig --level 345

   iptables on iptables -t nat -A PREROUTING -p udp --dport 514 -j REDIRECT --to <Ihr_neuer_Port>

   service iptables save
   ```

4. Ersetzen Sie die Variable <*Ihr_neuer_Port*> durch eine verfügbare Portnummer über 1024.

   Anleitungen für den Umgang mit Ports bei anderen Implementierungen erhalten Sie vom Hersteller Ihrer Firewall.

Installieren Sie den <ODBC>-Client.

Für die Installation eines ODBC-Clients in Windows-Systemen sind folgende Schritte erforderlich:

1. Überprüfen Sie, ob Sie über die notwendigen Berechtigungen verfügen, und erwerben Sie einen Lizenzschlüssel für den ODBC-Client-Treiber (Voraussetzungen).
2. Installieren Sie den <ODBC>-Client.
3. Erstellen Sie mit dem Hilfsprogramm Windows Data Source (ODBC) eine Datenquelle.
4. Konfigurieren Sie die Verbindungsdetails für den ODBC-Client.
5. Testen Sie die Datenbankverbindung.

Voraussetzungen

Ein ODBC-Zugriff auf den Ereignisprotokollspeicher ist nur ab CA Enterprise Log Manager-Release r12.1 verfügbar. Lesen Sie die Hinweise zur ODBC-Datenquelle, bevor Sie mit der Installation beginnen.

Die Benutzer dieser Funktion müssen einer Benutzergruppe angehören, die in der Standard-Datenzugriffsrichtlinie (in den CALM-Zugriffsrichtlinien) über das *Datenzugriffs*-Privileg verfügt. Weitere Informationen zu Zugriffsrichtlinien finden Sie im *CA Enterprise Log Manager r12.1 Administrationshandbuch*.

Für einen ODBC-Client gelten folgende Voraussetzungen:

- Sie müssen über Administratorrechte verfügen, um den ODBC-Client auf einem Windows-Server zu installieren.
- Für die Installation des ODBC-Clients benötigen Sie den Microsoft Windows Installer-Dienst. Falls dieser nicht gefunden werden kann, wird eine Meldung angezeigt.
- Konfigurieren Sie den ODBC-Server-Service in CA Enterprise Log Manager. Stellen Sie dabei sicher, dass das Kontrollkästchen "Dienste aktivieren" aktiviert ist.

- Konfigurieren Sie mit dem Hilfsprogramm Datenquellen (ODBC) der Systemsteuerung eine ODBC-Datenquelle für Windows-Systeme.
- Sie müssen über die Rechte zum Erstellen von Dateien in dem Verzeichnis verfügen, in dem Sie den Client in UNIX- und Linux-Systemen installieren möchten.

Einzelheiten zu den einzelnen Plattformen, die für die Nutzung mit den ODBC- und JDBC-Funktionen unterstützt werden, finden in der CA Enterprise Log Manager-Support-Zertifizierungsmatrix unter http://www.ca.com/Support.

Konfigurieren des ODBC-Server-Services

Mit diesem Verfahren können Sie den ODBC- und JDBC-Zugriff auf den CA Enterprise Log Manager-Ereignisprotokollspeicher konfigurieren.

So konfigurieren Sie den ODBC- und JDBC-Zugriff:

1. Melden Sie sich als Administrator beim CA Enterprise Log Manager-Server an.
2. Klicken Sie auf der Registerkarte "Verwaltung" auf die Unterregisterkarte "Services".
3. Klicken Sie auf den ODBC-Server-Dienst, um die globalen Einstellungen zu öffnen, oder erweitern Sie den Knoten, und wählen Sie einen bestimmten CA Enterprise Log Manager-Server aus.
4. Stellen Sie einen Portwert für das Feld "Dienstport" ein, falls Sie nicht den Standardwert als Port verwenden möchten.
5. Legen Sie fest, ob SSL aktiviert werden soll, um den Datentransport zwischen ODBC-Client und CA Enterprise Log Manager-Server zu verschlüsseln.

   Hinweis: Die Einstellungen "Dienstport" und "SSL aktiviert" müssen sowohl auf Server- als auch auf ODBC-Clientseite übereinstimmen. Der Standardwert für den Port ist 17002, und die SSL-Verschlüsselung ist aktiviert. Falls diese Einstellungen nicht mit den Einstellungen am ODBC-Client übereinstimmen, kann die Verbindung nicht hergestellt werden.

Installieren des ODBC-Clients in Windows-Systemen

Verwenden Sie diese Vorgehensweise, um den ODBC-Client auf einem Windows-System zu installieren.

Hinweis: Für die Installation des ODBC-Clients benötigen Sie ein Windows-Administratorkonto.

So installieren Sie den ODBC-Client:

1. Suchen Sie das Verzeichnis ODBC-Client auf der Anwendungs-DVD oder im Installations-Image im Verzeichnis \CA\ELM\ODBC.
2. Doppelklicken Sie auf die Anwendung "Setup.exe".
3. Stimmen Sie der Lizenzvereinbarung zu, und klicken Sie auf "Weiter".

   Das Fenster "Zielspeicherort auswählen" wird angezeigt.
4. Geben Sie einen Zielspeicherort ein oder akzeptieren Sie den Standardspeicherort, und klicken Sie auf "Weiter".

   Das Fenster zum Auswählen des Programmordners wird angezeigt.
5. Wählen Sie einen Programmordner aus oder akzeptieren Sie die Standardauswahl, und klicken Sie auf "Weiter".

   Das Fenster "Kopieren der Dateien starten" wird angezeigt.
6. Klicken Sie auf "Weiter", um mit dem Kopieren der Dateien zu beginnen.

   Das Fenster "Installationsstatus" zeigt den Fortschritt der Installation an. Wenn die Installation mit dem Kopieren der Dateien fertig ist, wird ein Fenster angezeigt, dass der InstallShield Wizard abgeschlossen ist.
7. Klicken Sie auf "Fertig stellen", um die Installation abzuschließen.

Erstellen einer ODBC-Datenquelle in Windows-Systemen

Gehen Sie wie unten beschrieben vor, um die benötigte ODBC-Datenquelle in Windows-Systemen zu erstellen. Sie können die Datenquelle entweder als Benutzer-DSN oder als System-DSN erstellen.

So erstellen Sie die Datenquelle:

1. Öffnen Sie die Windows-Systemsteuerung, und wählen Sie "Verwaltung" aus.
2. Doppelklicken Sie auf das Hilfsprogramm "Datenquellen (ODBC)". Das Fenster "ODBC-Datenquellenadministrator" wird angezeigt.

3. Klicken Sie auf "Hinzufügen", um das Fenster "Neue Datenquelle erstellen" anzuzeigen.
4. Wählen Sie den Eintrag "CA Enterprise Log Manager-ODBC-Treiber" aus, und klicken Sie auf "Fertig stellen".

   Das Fenster "CA Enterprise Log Manager-ODBC-Treiber-Setup" wird angezeigt.
5. Geben Sie entsprechend der Beschreibung im Abschnitt mit Hinweisen zur ODBC-Datenquelle Werte in die Felder ein, und klicken Sie auf "OK".

Hinweise zur ODBC-Datenquelle

Der folgende Abschnitt erläutert die ODBC-Datenquellenfelder im Zusammenhang mit CA Enterprise Log Manager:

Datenquellenname

Erstellen Sie einen Namen für diese Datenquelle. Client-Anwendungen, die auf diese Daten zugreifen möchten, verwenden diesen Namen für die Verbindung zur Datenquelle.

Service-Host

Gibt den Namen des CA Enterprise Log Manager-Servers an, zu dem der Client eine Verbindung herstellt. Sie können entweder einen Hostnamen oder eine IPv4-Adresse verwenden.

Dienstport

Gibt den TCP-Dienstport an, der vom CA Enterprise Log Manager-Server hinsichtlich von ODBC-Clientverbindungen abgehört wird. Der Standardwert ist "17002". Der Wert, den Sie hier festlegen, muss mit der Einstellung für den ODBC-Server-Dienst übereinstimmen, oder die Verbindung schlägt fehl.

Service-Datenquelle

Lassen Sie dieses Feld leer, da der Verbindungsversuch andernfalls fehlschlägt.

Verschlüsselt (SSL)

Gibt an, ob die Kommunikation zwischen dem Client und dem CA Enterprise Log Manager-Server verschlüsselt werden soll. Standardmäßig ist die SSL-Verschlüsselung aktiviert. Der Wert, den Sie hier festlegen, muss mit der Einstellung für den ODBC-Server-Dienst übereinstimmen, oder die Verbindung schlägt fehl.

Benutzerdefinierte Eigenschaften

Definiert die Verbindungseigenschaften, die für den Ereignisprotokollspeicher verwendet werden sollen. Die einzelnen Eigenschaften werden durch ein Semikolon ohne Leerzeichen getrennt. Folgende Standardwerte werden empfohlen:

querytimeout

Gibt den Wert für das Zeitlimit in Sekunden an, nach dem die Abfrage geschlossen wird, wenn keine Daten zurückgegeben werden. Für diese Eigenschaft wird folgende Syntax verwendet:

```
querytimeout=300
```

queryfederated

Gibt an, ob eine föderierte Abfrage durchgeführt werden soll. Wenn Sie für diesen Wert "false" festlegen, wird nur für CA Enterprise Log Manager-Server eine Abfrage durchgeführt, zu dem die Datenbankverbindung hergestellt wird. Für diese Eigenschaft wird folgende Syntax verwendet:

```
queryfederated=true
```

queryfetchrows

Gibt an, wie viele Zeilen in einem einzelnen Fetch-Vorgang abgerufen werden sollen, wenn die Abfrage erfolgreich ist. Der minimale Wert beträgt "1" und der maximale Wert "5000". Der Standardwert ist "1000". Für diese Eigenschaft wird folgende Syntax verwendet:

```
queryfetchrows=1000
```

offsetmins

Gibt den Offset für die Zeitzone für diesen ODBC-Client an. Bei einem Wert von 0 wird GMT verwendet. Sie können diese Feld verwenden, um die Abweichung Ihrer Zeitzone von GMT festzulegen. Für diese Eigenschaft wird folgende Syntax verwendet:

```
offsetmins=0
```

suppressNoncriticalErrors

Gibt das Verhalten des Interface Providers bei nicht kritischen Fehlern an, z. B. wenn eine Datenbank nicht reagiert oder ein Host nicht antwortet.

Für diese Eigenschaft wird folgende Syntax verwendet:

```
suppressNoncriticalErrors=false
```

Testen der Verbindung des ODBC-Clients zur Datenbank

Der ODBC-Client ist mit einem Tool zur SQL-Abfrage (ISQL) installiert, das mit der Befehlszeile interaktiv ist. Sie können dieses Tool verwenden, um Ihre Konfigurationseinstellungen und die Konnektivität zwischen ODBC-Client und CA Enterprise Log Manager-Ereignisprotokollspeicher zu testen.

So testen Sie die Client-Verbindung zur Datenbank:

1. Öffnen Sie eine Eingabeaufforderung, und navigieren Sie zu dem Verzeichnis, in dem Sie den ODBC-Client installiert haben.
2. Starten Sie das ISQL-Hilfsprogramm, odbcisql.exe.
3. Geben Sie folgenden Befehl ein, um die Client-Verbindung zur Datenbank zu testen:

   ```
   connect User*Password@DSN_name
   ```

   Verwenden Sie den Namen der Datenquelle, die Sie für diese ODBC-Verbindung zur Datenbank für den Wert DSN_name erstellt haben. Wenn Ihre Verbindungsparameter richtig sind, erhalten Sie eine ähnliche Antwortmeldung wie die folgende:

   ```
   SQL: connecting to database: DSN_name
   Elapsed time 37 ms.
   ```

Serverabruf von der Datenbank testen

Verwenden Sie diese Testabfrage, um festzulegen, ob eine ODBC-Client-Anwendung in der Lage ist, die Daten eines CA Enterprise Log Manager-Ereignisprotokollspeichers über die festgelegte Datenverbindung abzurufen. Dieser Vorgang verwendet das gleiche ISQL-Hilfsprogramm, das Sie zum Testen der ODBC-Verbindung verwendet haben.

Hinweis: Kopieren und verwenden Sie die SQL-Abfragen in den CA Enterprise Log Manager-Abfragen und Berichten nicht, um Ihre ODBC-Verbindung zu testen. Diese SQL-Anweisungen werden nur vom CA Enterprise Log Manager-Server mit dem Ereignisprotokollspeicher verwendet. Erstellen Sie Ihre ODBC SQL-Abfragen anhand von Standardkonstruktionen gemäß den ANSI SQL-Standards.

So testen Sie den Datenabruf der Serverkomponente:

1. Öffnen Sie eine Eingabeaufforderung, und navigieren Sie zu dem Verzeichnis, in dem Sie den ODBC-Client installiert haben.
2. Starten Sie das ISQL-Hilfsprogramm, odbcisql.exe.

3. Geben Sie folgende SELECT-Anweisung ein, um den Abruf aus dem Ereignisprotokollspeicher zu testen:

```
select top 5 event_logname, receiver_hostname, SUM(event_count) as Count from
view_event where event_time_gmt < now() and event_time_gmt >
timestampadd(mi,-15,now()) GROUP BY receiver_hostname, event_logname;
```

Installieren des JDBC-Clients

Mit dem JDBC-Client haben Sie über alle Java-aktivierten Applets, Anwendungen oder den Anwendungsserver Zugriff auf JDBC. Er liefert einen leistungsstarken Point-to-Point- und n-Tier-Zugriff auf Datenquellen. Der Client ist für die Java-Umgebung optimiert, so dass Sie die Java-Technologie einbeziehen und die Funktionalität und Leistung Ihres vorhandenen Systems erweitern können.

Der JDBC-Client wird auf 32-Bit- und 64-Bit-Plattformen ausgeführt. Vorhandene Anwendungen müssen nicht geändert werden, um auf 64-Bit-Plattformen ausgeführt zu werden.

Die Installation des JDBC-Clients besteht aus folgenden Schritten:

1. Vergewissern Sie sich, dass ein Web-Anwendungsserver mit Funktionen für die Verbindungspoolkonfiguration installiert ist und ausgeführt wird.
2. Erwerben Sie den Lizenzschlüssel für den JDBC-Client-Treiber.
3. Installieren Sie den JDBC-Client.
4. Konfigurieren Sie die Verbindung zur Datenbank mit den Verwaltungsfunktionen des Verbindungspools Ihres Web-Anwendungsservers.
5. Testen Sie die Datenbankverbindung.

Voraussetzungen für den JDBC-Client

Ein JDBC-Zugriff auf den Ereignisprotokollspeicher ist nur ab CA Enterprise Log Manager-Release r12.1 verfügbar. Sie können den JDBC-Client auf Windows und UNIX-Systemen installieren.

Die Benutzer dieser Funktion müssen einer CA Enterprise Log Manager-Benutzergruppe angehören, die in der Standard-Datenzugriffsrichtlinie (in den CALM-Zugriffsrichtlinien) über das *Datenzugriffs*-Privileg verfügt. Weitere Informationen zu Zugriffsrichtlinien finden Sie im *CA Enterprise Log Manager r12.1 Administrationshandbuch*.

Für einen JDBC-Client gelten folgende Voraussetzungen:

- Sie müssen über Administratorrechte verfügen, um den JDBC-Client auf einem Windows-Server zu installieren.
- Überprüfen Sie, ob im Fenster der ODBC-Serverkonfiguration das Kontrollkästchen "Dienste aktivieren" ausgewählt (aktiviert) ist.
- Sie müssen über die Rechte zum Erstellen von Dateien in dem Verzeichnis verfügen, in dem Sie den Client in UNIX- und Linux-Systemen installieren möchten.
- Stellen Sie Ihre Datenbankverbindungen für Anwendungen, die unter J2SE v 1.4.2.x laufen, programmatisch ein, wie in einer bestimmen Anwendung definiert.
- Verwenden Sie für Anwendungen, die ab Version J2EE 1.4.2.x laufen, einen Web-Anwendungsserver, wie BEA WebLogic oder Red Hat JBoss, um die Verwaltung Ihres Verbindungspools zu konfigurieren.

Einzelheiten zu den einzelnen Plattformen, die für die Nutzung mit den ODBC- und JDBC-Funktionen unterstützt werden, finden in der CA Enterprise Log Manager-Support-Zertifizierungsmatrix unter http://www.ca.com/Support.

Installieren des JDBC-Clients in Windows-Systemen

Verwenden Sie diese Vorgehensweise, um den JDBC-Client-Treiber auf einem Windows-System zu installieren.

So installieren Sie den JDBC-Treiber:

1. Suchen Sie im Verzeichnis CA/ELM/JDBC der Anwendungs-DVD oder des Installations-Images nach folgenden zwei .jar-Dateien:

   ```
   LMjc.jar
   LMssl14.jar
   ```

2. Kopieren Sie die .jar-Dateien in das gewünschte Verzeichnis des Zielservers, und notieren Sie sich den Pfad.

Installieren des JDBC-Clients in UNIX-Systemen

Verwenden Sie diese Vorgehensweise, um den JDBC-Client-Treiber auf einem UNIX-System zu installieren.

So installieren Sie den JDBC-Treiber:

1. Suchen Sie im Verzeichnis CA/ELM/JDBC der Anwendungs-DVD oder des Installations-Images nach folgenden zwei .jar-Dateien:

   ```
   LMjc.jar
   LMssl14.jar
   ```

2. Kopieren Sie die .jar-Dateien in das gewünschte Verzeichnis des Zielservers, und notieren Sie sich den Pfad.

3. Führen Sie folgenden (oder einen ähnlichen) Befehl manuell im Installationsverzeichnis aus, nachdem Sie den JDBC-Client für JDBC auf UNIX installiert haben:

   ```
   chmod -R ugo+x file_location
   ```

   Der Wert für *file_location* ist das Verzeichnis, in dem Sie den JDBC-Client installiert haben. Mit diesem Schritt können Sie Shell-Skripts ausführen, die im installierten Client enthalten sind.

JDBC-Verbindungsparameter

Viele Anwendungen benötigen für die Verwendung des JDBC-Client-Treibers bestimmte Verbindungsparameter. Zu den gängigen Parametern gehören:

- Verbindungszeichenfolge oder Verbindungs-URL
- Klassenname

Die JDBC-Verbindungszeichenfolge (URL) hat folgendes Format:

```
jdbc:ca-elm://[CA-ELM_host_name]:[ODBC/JDBCport];ServerDataSource=Default;
```

Der JDBC-Treiber hat folgenden Klassennamen:

```
com.ca.jdbc.openaccess.OpenAccessDriver
```

Hinweise zur JDBC-URL

Wenn Sie mit dem JDBC-Client auf Ereignisdaten zugreifen, die in CA Enterprise Log Manager gespeichert sind, benötigen Sie sowohl den JDBC-Klassenpfad als auch eine JDBC-URL. Der JDBC-Klassenpfad gibt den Speicherort der JAR-Treiberdatei an. Die JDBC-URL definiert die Parameter, die von den Klassen in den JARs beim Laden verwendet werden.

Das folgende Beispiel zeigt eine vollständige JDBC-URL:

```
jdbc:ca-
elm://127.0.0.1:17002;encrypted=1;ServerDataSource=Default;CustomProperties=(querytimeout=600;que
ryfederated=true;queryfetchrows=1000;offsetmins=0;suppressNoncriticalErrors=false)
```

Die einzelnen URL-Komponenten sind im Folgenden erläutert:

jdbc.ca-elm:

Definiert die "Protokoll:Unterprotokoll"-Zeichenfolge, für den mit CA Enterprise Log Manager bereitgestellten JDBC-Treiber.

//IP Address:Port;

Gibt die IP-Adresse des CA Enterprise Log Manager-Servers an, auf dessen Daten zugegriffen werden soll. Die Portnummer bezieht sich auf den Port, der für die Kommunikation verwendet werden soll, und muss mit der Einstellung für die Konfiguration des ODBC-Dienstes in CA Enterprise Log Manager übereinstimmen. Wenn die Portnummern nicht identisch sind, schlägt der Verbindungsversuch fehl.

encrypted=0|1;

Gibt an, ob für die Kommunikation zwischen dem ODBC-Client und dem CA Enterprise Log Manager-Server SSL-Verschlüsselung verwendet wird. Der Standardwert ist 0 (nicht verschlüsselt). Diese Einstellung muss nicht in der URL angegeben werden. Mit der Einstellung "encrypted=1" wird die Verschlüsselung aktiviert. Die Verschlüsselung der Verbindung muss explizit festgelegt werden. Außerdem muss diese Einstellung mit der Konfiguration im Dialogfeld für den ODBC-Dienst in CA Enterprise Log Manager übereinstimmen, da der Verbindungsversuch andernfalls fehlschlägt.

ServerDataSource=Default

Gibt den Namen der Datenquelle an. Stellen Sie diesen Wert für den Zugriff auf den CA Enterprise Log Manager-Ereignisprotokollspeicher auf "*Default*" ein.

CustomProperties=(x;y;z)

Diese Eigenschaften entsprechen den benutzerdefinierten ODBC-Eigenschaften. Wenn Sie diese nicht explizit angeben, werden die in der Beispiel-URL gezeigten Standardwerte verwendet.

Weitere Informationen

Hinweise zur ODBC-Datenquelle (siehe Seite 114)

Fehlerbehebung bei der Installation

Sie können zunächst folgende Protokolldateien der Installation überprüfen, falls Sie bei der Installation aufgetretene Fehler beheben müssen:

Produkt	Speicherort der Protokolldatei
CA Enterprise Log Manager	/tmp/pre-install_ca-elm.log /tmp/install_ca-elm.<*Zeitstempel*>.log /tmp/install_ca-elmagent.<*Zeitstempel*>.log
CA Embedded Entitlements Manager	/opt/CA/SharedComponents/EmbeddedIAM/eiam-install.log
CA Directory	/tmp/etrdir_install.log

Bei der CA Enterprise Log Manager-Installation werden Inhaltsdateien und andere Dateien zur Verwaltung auf den CA EEM-Server kopiert. Aus Sicht des CA EEM-Servers werden die CA Enterprise Log Manager-Berichte und anderen Dateien *importiert*. Falls bei der Installation keine Verbindung mit dem CA EEM-Server hergestellt werden kann, wird die Installation von CA Enterprise Log Manager fortgesetzt, ohne dass Inhaltsdateien importiert werden. Sie können die Inhaltsdateien nach Abschluss der Installation manuell importieren.

Falls während der Installation Fehler auftreten, müssen Sie ggf. eine oder mehrere der folgenden Aktionen durchführen, um die Installation abschließen zu können. Bei jeder dieser Aktionen müssen Sie sich unter dem Standardkonto "caelmadmin" beim CA Enterprise Log Manager-Server anmelden und dann Benutzer auf das "root"-Konto umschalten.

- Beheben von Fehlern bei der Netzwerkschnittstellenkonfiguration
- Überprüfen, dass das rpm-Paket installiert wurde
- Überprüfen, dass der iGateway-Daemon ausgeführt wird
- Registrieren der CA Enterprise Log Manager-Anwendung beim CA EEM-Server
- Beziehen digitaler Zertifikate
- Importieren von CA Enterprise Log Manager-Berichten
- Importieren von Datenzuordnungsdateien
- Importieren von Nachrichtenanalysedateien
- Importieren von Dateien für die ELM-Schemadefinition
- Importieren von Dateien für die allgemeine Agentenverwaltung

Beheben von Fehlern bei der Netzwerkschnittstellenkonfiguration

Falls Sie nach der Installation nicht auf die Benutzeroberfläche des CA Enterprise Log Manager-Servers zugreifen können, liegt eventuell ein Fehler bei der Netzwerkschnittstellenkonfiguration vor. Sie können den Fehler auf zweierlei Weise beheben:

- Entfernen Sie das physische Netzwerkkabel, und schließen Sie es an einen anderen Port an.
- Konfigurieren Sie die logischen Netzwerkschnittstellenadapter über eine Befehlszeile neu.

So konfigurieren Sie die Netzwerkadapterports über eine Befehlszeile:

1. Melden Sie sich als "caelmadmin"-Benutzer bei der Software-Appliance an, und rufen Sie eine Eingabeaufforderung auf.
2. Schalten Sie Benutzer mit folgendem Befehl auf den "root"-Benutzer um:

   ```
   su -
   ```

3. Geben Sie das Kennwort für den "root"-Benutzer ein, um den Zugriff auf das System zu bestätigen.
4. Geben Sie folgenden Befehl ein:

   ```
   system-config-network
   ```

   Die Benutzeroberfläche zur Konfiguration der Netzwerkadapter wird angezeigt.
5. Legen Sie die Portkonfigurationen wie gewünscht fest, und beenden Sie die Anzeige.
6. Starten Sie die Netzwerkdienste mit folgendem Befehl neu, damit die Änderungen in Kraft treten können:

   ```
   service network restart
   ```

Überprüfen der Installation des RPM-Pakets

Sie können eine schnelle Überprüfung der Installation vornehmen, indem Sie überprüfen, ob das richtige RPM-Paket installiert wurde.

So überprüfen Sie das RPM-Paket:

1. Rufen Sie auf dem CA Enterprise Log Manager-Server eine Befehlszeile auf.
2. Melden Sie sich mit den Anmeldedaten des "caelmadmin"-Kontos an.
3. Schalten Sie Benutzer mit folgendem Befehl auf das "root"-Konto um:

   ```
   su - root
   ```

4. Überprüfen Sie mit den folgenden Befehlen, ob das Paket "ca-elm-<Version>.i386.rpm" installiert ist:

   ```
   rpm -q ca-elm
   rpm -q ca-elmagent
   ```

   Das Betriebssystem gibt den vollständigen Namen des Pakets zurück, sofern es installiert wurde.

Registrieren des CA Enterprise Log Manager-Servers beim CA EEM-Server

Symptom:

Während der Installation wurde die CA Enterprise Log Manager-Anwendung nicht ordnungsgemäß beim CA EEM-Server registriert. Die CA Enterprise Log Manager-Anwendung benötigt den CA EEM-Server für die Verwaltung von Benutzerkonten und Servicekonfigurationen. Falls die CA Enterprise Log Manager-Anwendung nicht registriert wird, funktioniert die Software nicht ordnungsgemäß.

Das in den folgenden Anleitungen erwähnte Shell-Skript wird während der Installation automatisch in das benannte Verzeichnis kopiert.

Lösung:

Registrieren Sie die CA Enterprise Log Manager-Anwendung manuell beim CA EEM-Server.

So registrieren Sie die CA Enterprise Log Manager-Anwendung:

1. Rufen Sie auf dem CA Enterprise Log Manager-Server eine Befehlszeile auf.
2. Melden Sie sich mit den Anmeldedaten des "caelmadmin"-Kontos an.
3. Schalten Sie Benutzer mit folgendem Befehl auf den "root"-Benutzer um:

   ```
   su -
   ```

4. Navigieren Sie zu dem Verzeichnis "/opt/CA/LogManager/EEM".
5. Führen Sie folgenden Befehl aus:

   ```
   ./EEMRegister.sh
   ```

   Das Shell-Skript registriert die CA Enterprise Log Manager-Anwendung beim CA EEM-Server.

Beziehen von Zertifikaten vom CA EEM-Server

Symptom:

Während der Installation wurden die digitalen Zertifikate nicht ordnungsgemäß vom CA EEM-Server bezogen. Digitale Zertifikate werden zum Starten und Ausführen der CA Enterprise Log Manager-Anwendung benötigt.

Das in den folgenden Anleitungen erwähnte Shell-Skript wird während der Installation automatisch in das benannte Verzeichnis kopiert.

Lösung:

Beziehen Sie die Zertifikate manuell vom CA EEM-Server.

So beziehen Sie digitale Zertifikate:

1. Rufen Sie auf dem CA Enterprise Log Manager-Server eine Befehlszeile auf.
2. Melden Sie sich mit den Anmeldedaten des "caelmadmin"-Kontos an.
3. Schalten Sie Benutzer mit folgendem Befehl auf den "root"-Benutzer um:

   ```
   su -
   ```

4. Navigieren Sie zu dem Verzeichnis "/opt/CA/LogManager/EEM".
5. Führen Sie folgenden Befehl aus:

   ```
   ./EEMAcqCert.sh
   ```

   Das Shell-Skript führt die zum Beziehen der erforderlichen digitalen Zertifikate notwendige Verarbeitung durch.

Importieren von CA Enterprise Log Manager-Berichten

Symptom:

Während der Installation wurden Berichtsinhalte nicht richtig vom CA EEM-Server importiert. Sie müssen die Berichtsinhalte importieren, damit Ereignisdaten angezeigt werden, nachdem sie im Ereignisprotokollspeicher gespeichert wurden.

Das in den folgenden Anleitungen erwähnte Shell-Skript wird während der Installation automatisch in das benannte Verzeichnis kopiert.

Lösung:

Importieren Sie die Berichtsinhalte manuell.

So importieren Sie Berichtsinhalte:

1. Rufen Sie auf dem CA Enterprise Log Manager-Server eine Befehlszeile auf.
2. Melden Sie sich mit den Anmeldedaten des "caelmadmin"-Kontos an.
3. Schalten Sie Benutzer mit folgendem Befehl auf den "root"-Benutzer um:

   ```
   su -
   ```

4. Navigieren Sie zu dem Verzeichnis "/opt/CA/LogManager/EEM/content".
5. Führen Sie folgenden Befehl aus:

   ```
   ./ImportCALMContent.sh
   ```

   Das Shell-Skript lädt die Berichtsinhalte vom CA EEM-Server herunter.

Importieren von CA Enterprise Log Manager-Datenzuordnungsdateien

Symptom:

Während der Installation wurden die Datenzuordnungsdateien nicht richtig vom CA EEM-Server importiert. Die Datenzuordnungsdateien werden für die Zuordnung der eintreffenden Ereignisdaten im Ereignisprotokollspeicher benötigt.

Das in den folgenden Anleitungen erwähnte Shell-Skript wird während der Installation automatisch in das benannte Verzeichnis kopiert.

Lösung:

Importieren Sie die Datenzuordnungsdateien manuell.

So importieren Sie Datenzuordnungsdateien:

1. Rufen Sie auf dem CA Enterprise Log Manager-Server eine Befehlszeile auf.
2. Melden Sie sich mit den Anmeldedaten des "caelmadmin"-Kontos an.
3. Schalten Sie Benutzer mit folgendem Befehl auf den "root"-Benutzer um:

   ```
   su -
   ```

4. Navigieren Sie zu dem Verzeichnis "/opt/CA/LogManager/EEM/content".
5. Führen Sie folgenden Befehl aus:

   ```
   ./ImportCALMDM.sh
   ```

   Das Shell-Skript importiert die Datenzuordnungsdateien vom CA EEM-Server.

Importieren von CA Enterprise Log Manager-Nachrichtenanalysedateien

Symptom:

Während der Installation wurden die Nachrichtenanalysedateien (.xmp) nicht richtig vom CA EEM-Server importiert. Die Nachrichtenanalysedateien sind für die Verarbeitung der Ereignisprotokolle aus den verschiedenen Quellen im Netzwerk erforderlich. Sie werden benötigt, um Ereignisse in den CA Enterprise Log Manager-Ereignisprotokollspeicher einzufügen.

Das in den folgenden Anleitungen erwähnte Shell-Skript wird während der Installation automatisch in das benannte Verzeichnis kopiert.

Lösung:

Importieren Sie die Nachrichtenanalysedateien manuell.

So importieren Sie Nachrichtenanalysedateien:

1. Rufen Sie auf dem CA Enterprise Log Manager-Server eine Befehlszeile auf.
2. Melden Sie sich mit den Anmeldedaten des "caelmadmin"-Kontos an.
3. Schalten Sie Benutzer mit folgendem Befehl auf den "root"-Benutzer um:

   ```
   su -
   ```

4. Navigieren Sie zu dem Verzeichnis "/opt/CA/LogManager/EEM/content".
5. Führen Sie folgenden Befehl aus:

   ```
   ./ImportCALMMP.sh
   ```

   Das Shell-Skript importiert die Nachrichtenanalysedateien vom CA EEM-Server.

Importieren der Dateien für die ELM-Schemadefinition

Symptom:

Während der Installation wurden die Dateien für die ELM-Schemadefinition nicht richtig vom CA EEM-Server importiert. Die ELM-Schemadefinition ist das zugrunde liegende Datenbankschema für den Ereignisprotokollspeicher. Ohne die Dateien für die ELM-Schemadefinition können keine Ereignisse im CA Enterprise Log Manager-Ereignisprotokollspeicher gespeichert werden.

Das in den folgenden Anleitungen erwähnte Shell-Skript wird während der Installation automatisch in das benannte Verzeichnis kopiert.

Lösung:

Importieren Sie die Dateien für die ELM-Schemadefinition manuell.

So importieren Sie die Dateien für die ELM-Schemadefinition:

1. Rufen Sie auf dem CA Enterprise Log Manager-Server eine Befehlszeile auf.
2. Melden Sie sich mit den Anmeldedaten des "caelmadmin"-Kontos an.
3. Schalten Sie Benutzer mit folgendem Befehl auf den "root"-Benutzer um:

   ```
   su -
   ```

4. Navigieren Sie zu dem Verzeichnis "/opt/CA/LogManager/EEM/content".
5. Führen Sie folgenden Befehl aus:

   ```
   ./ImportCALMCEG.sh
   ```

   Das Shell-Skript importiert die Dateien für die ELM-Schemadefinition.

Importieren von Dateien für die allgemeine Agentenverwaltung

Symptom:

Während der Installation wurden die Dateien für die allgemeine Agentenverwaltung nicht richtig vom CA EEM-Server importiert. Ohne diese Dateien können keine Agenten über die CA Enterprise Log Manager-Benutzeroberfläche verwaltet werden.

Das in den folgenden Anleitungen erwähnte Shell-Skript wird während der Installation automatisch in das benannte Verzeichnis kopiert.

Lösung:

Importieren Sie die Agentenverwaltungsdateien manuell.

So importieren Sie Dateien für die allgemeine Agentenverwaltung:

1. Greifen Sie auf eine Eingabeaufforderung auf dem CA Enterprise Log Manager-Server zu.
2. Melden Sie sich mit den Anmeldeinformationen für das "caelmadmin"-Konto an.
3. Schalten Sie Benutzer mit folgendem Befehl auf den "root"-Benutzer um:

   ```
   su -
   ```

4. Navigieren Sie zu dem Verzeichnis "/opt/CA/LogManager/EEM/content".
5. Führen Sie folgenden Befehl aus:

   ```
   ./ImportCALMAgentContent.sh
   ```

   Das Shell-Skript importiert die Dateien für die allgemeine Agentenverwaltung.

Importieren von CA Enterprise Log Manager-Konfigurationsdateien

Symptom:

Während der Installation wurden die Konfigurationsdateien nicht richtig vom CA EEM-Server importiert. Sie können CA Enterprise Log Manager starten, es fehlen jedoch bestimmte Einstellungen und Werte aus den Bereichen für die Service-Konfiguration, und ohne diese Dateien können Sie einzelne Hosts nicht zentral konfigurieren.

Das in den folgenden Anleitungen erwähnte Shell-Skript wird während der Installation automatisch in das benannte Verzeichnis kopiert.

Lösung:

Importieren Sie die Konfigurationsdateien manuell.

So importieren Sie die Konfigurationsdateien:

1. Greifen Sie auf eine Eingabeaufforderung auf dem CA Enterprise Log Manager-Server zu.
2. Melden Sie sich mit den Anmeldeinformationen für das "caelmadmin"-Konto an.
3. Schalten Sie Benutzer mit folgendem Befehl auf den "root"-Benutzer um:

   ```
   su -
   ```

4. Navigieren Sie zu dem Verzeichnis "/opt/CA/LogManager/EEM/content".
5. Führen Sie folgenden Befehl aus:

   ```
   ./ImportCALMConfig.sh
   ```

   Das Shell-Skript importiert die Konfigurationsdateien.

Importieren von Unterdrückungs- und Zusammenfassungsdateien

Symptom:

Während der Installation wurden die Unterdrückungs- und Zusammenfassungsdateien nicht richtig vom CA EEM-Server importiert. Ohne diese Dateien können Sie die Standard-Unterdrückungs- und Standard-Zusammenfassungsregeln nicht in der CA Enterprise Log Manager-Benutzeroberfläche verwenden.

Das in den folgenden Anleitungen erwähnte Shell-Skript wird während der Installation automatisch in das benannte Verzeichnis kopiert.

Lösung:

Importieren Sie die Unterdrückungs- und Zusammenfassungsregeln manuell.

So importieren Sie Unterdrückungs- und Zusammenfassungsdateien:

1. Greifen Sie auf eine Eingabeaufforderung auf dem CA Enterprise Log Manager-Server zu.
2. Melden Sie sich mit den Anmeldeinformationen für das "caelmadmin"-Konto an.
3. Schalten Sie Benutzer mit folgendem Befehl auf den "root"-Benutzer um:

   ```
   su -
   ```

4. Navigieren Sie zu dem Verzeichnis "/opt/CA/LogManager/EEM/content".
5. Führen Sie folgenden Befehl aus:

   ```
   ./ImportCALMSAS.sh
   ```

   Das Shell-Skript importiert die Unterdrückungs- und Zusammenfassungsdateien.

Importieren von Analyse-Token-Dateien

Symptom:

Während der Installation wurden die Analyse-Token-Dateien nicht richtig vom CA EEM-Server importiert. Ohne diese Dateien können Sie im Assistenten für Analysedateien keine Standard-Analyse-Tokens verwenden.

Das in den folgenden Anleitungen erwähnte Shell-Skript wird während der Installation automatisch in das benannte Verzeichnis kopiert.

Lösung:

Importieren Sie die Analyse-Token-Dateien manuell.

So importieren Sie Analyse-Token-Dateien:

1. Greifen Sie auf eine Eingabeaufforderung auf dem CA Enterprise Log Manager-Server zu.
2. Melden Sie sich mit den Anmeldeinformationen für das "caelmadmin"-Konto an.
3. Schalten Sie Benutzer mit folgendem Befehl auf den "root"-Benutzer um:

   ```
   su -
   ```

4. Navigieren Sie zu dem Verzeichnis "/opt/CA/LogManager/EEM/content".
5. Führen Sie folgenden Befehl aus:

   ```
   ./ImportCALMTOK.sh
   ```

   Das Shell-Skript importiert die Analyse-Token-Dateien.

Importieren von CA Enterprise Log Manager-Benutzeroberflächendateien

Symptom:

Während der Installation wurden die Benutzeroberflächendateien nicht richtig vom CA EEM-Server importiert. Ohne diese Dateien können Sie die Werte in den Dropdown-Feldern des dynamischen Zeitbereichs nicht anzeigen oder verwenden.

Das in den folgenden Anleitungen erwähnte Shell-Skript wird während der Installation automatisch in das benannte Verzeichnis kopiert.

Lösung:

Importieren Sie die Benutzeroberflächendateien manuell.

So importieren Benutzeroberflächendateien:

1. Greifen Sie auf eine Eingabeaufforderung auf dem CA Enterprise Log Manager-Server zu.
2. Melden Sie sich mit den Anmeldeinformationen für das "caelmadmin"-Konto an.
3. Schalten Sie Benutzer mit folgendem Befehl auf den "root"-Benutzer um:

   ```
   su -
   ```

4. Navigieren Sie zu dem Verzeichnis "/opt/CA/LogManager/EEM/content".
5. Führen Sie folgenden Befehl aus:

   ```
   ./ImportCALMFlexFiles.sh
   ```

   Das Shell-Skript importiert die Benutzeroberflächendateien.

Kapitel 4: Grundlagen zur Benutzer- und Zugriffskonfiguration

Dieses Kapitel enthält folgende Themen:

Grundlagen zu Benutzern und Zugriff

Die Konfiguration beginnt mit der Einrichtung des Benutzerspeichers, der Erstellung eines oder mehrerer Benutzer mit der vordefinierten Administratorrolle und der Konfiguration von Kennwortrichtlinien. In der Regel wird diese Konfiguration von der Person vorgenommen, die CA Enterprise Log Manager installiert hat, da dieser Benutzer sich mit den "EiamAdmin"-Anmeldedaten bei CA Enterprise Log Manager anmelden kann. Nach Abschluss dieser Konfiguration wird CA Enterprise Log Manager von den als Administratoren ausgewiesenen Benutzern weiter konfiguriert.

Falls die Konfiguration für den Standardbenutzerspeicher übernommen wird, muss der "EiamAdmin"-Benutzer zumindest noch das Konto für den ersten Administrator einrichten. Der erste Administrator kann Kennwortrichtlinien und dann die übrigen CA Enterprise Log Manager-Komponenten konfigurieren.

Hinweis: Genaue Informationen zum Erstellen anderer Benutzer und zum Erstellen benutzerdefinierter Rollen und Zugriffsrichtlinien finden Sie im *CA Enterprise Log Manager-Administrationshandbuch*.

Konfigurieren des Benutzerspeichers

Der Benutzerspeicher ist das Repository für globale Benutzerdaten. Sie können den Benutzerspeicher sofort nach der Installation eines CA Enterprise Log Manager-Servers konfigurieren. Der Benutzerspeicher kann nur vom "EiamAdmin"-Benutzer eingerichtet werden. Dies geschieht in der Regel sofort nach der ersten Anmeldung.

Konfigurieren Sie den Benutzerspeicher auf eine der folgenden Weisen:

- Übernehmen Sie die Standardoption, d. h. die Speicherung im internen Datenspeicher.

  Hinweis: Als Standardoption wird ggf. die CA-Verwaltungsdatenbank angezeigt, falls Sie während der Installation einen Zeiger auf einen eigenständigen CA EEM-Server eingerichtet haben.
- Wählen Sie die Option "Von externem Verzeichnis referenziert" aus. Dabei kann es sich um ein LDAP-Verzeichnis wie Microsoft Active Directory, Sun One oder Novell CA Directory handeln.
- Wählen Sie die Option "Von CA SiteMinder referenziert" aus.

Falls Sie den Benutzerspeicher als externes Verzeichnis einrichten, können Sie keine neuen Benutzer erstellen. Sie können dann nur vordefinierte und benutzerdefinierte Anwendungsgruppen bzw. Rollen zu den schreibgeschützten globalen Benutzerdatensätzen hinzufügen. Sie müssen neue Benutzer im externen Benutzerspeicher und dann die CA Enterprise Log Manager-Berechtigungen zu den globalen Benutzerdatensätzen hinzufügen.

Übernehmen des Standardbenutzerspeichers

Falls Sie den Standardbenutzerspeicher (also den internen Datenspeicher) übernehmen, müssen Sie den Benutzerspeicher nicht konfigurieren. Verwenden Sie diese Option, falls kein externer, zu referenzierender Benutzerspeicher vorhanden ist.

So überprüfen Sie, dass das Standard-Repository als Benutzerspeicher konfiguriert ist:

1. Melden Sie sich als Benutzer mit Administratorrechten bzw. mit dem Namen und Kennwort des "EiamAdmin"-Benutzers bei einem CA Enterprise Log Manager-Server an.
2. Klicken Sie auf die Registerkarte "Verwaltung".

   Falls Sie sich als "EiamAdmin"-Benutzer anmelden, wird diese Registerkarte automatisch angezeigt.

3. Wählen Sie die untergeordnete Registerkarte "Benutzer- und Zugriffsverwaltung" aus, und klicken Sie im linken Teilfenster auf "Benutzerspeicher".

   Die EEM-Server-Konfiguration für globale Benutzer/globale Gruppen wird angezeigt.

4. Vergewissern Sie sich, dass die Option für die Speicherung im internen Datenspeicher aktiviert ist.

5. Klicken Sie auf "Speichern" und anschließend auf "Schließen".

Hinweis: Wenn Sie den Standardbenutzerspeicher verwenden, können Sie neue Benutzer erstellen, temporäre Kennwörter festlegen und Kennwortrichtlinien definieren.

Weitere Informationen

Planen des Benutzerspeichers (siehe Seite 40)

Verweisen auf ein LDAP-Verzeichnis

Konfigurieren Sie den Benutzerspeicher als Verweis auf ein LDAP-Verzeichnis, falls die globalen Benutzerdaten in Microsoft Active Directory, Sun One oder Novell Directory gespeichert sind.

Hinweis: Anwendungsdaten werden im Standard-Repository gespeichert. Durch den Verweis auf einen externen Benutzerspeicher wird dieser Benutzerspeicher nicht aktualisiert.

So verweisen Sie auf ein LDAP-Verzeichnis als Benutzerspeicher:

1. Melden Sie sich als Benutzer mit Administratorrechten bzw. als "EiamAdmin"-Benutzer bei einem CA Enterprise Log Manager-Server an.

2. Klicken Sie auf die Registerkarte "Verwaltung".

   Falls Sie sich als "EiamAdmin"-Benutzer anmelden, wird diese Registerkarte automatisch angezeigt.

3. Wählen Sie die untergeordnete Registerkarte "Benutzer- und Zugriffsverwaltung" aus, und klicken Sie im linken Teilfenster auf "Benutzerspeicher".

   Die CA EEM-Server-Konfiguration für den Benutzerspeicher wird angezeigt.

4. Aktivieren Sie die Option "Von externem Verzeichnis referenziert".

   Die Felder für die LDAP-Konfiguration werden angezeigt.

5. Füllen Sie die Felder wie auf dem Arbeitsblatt für ein externes Verzeichnis geplant aus.

   Halten Sie sich an das folgende Beispiel, um eine Bindung an Active-Directory-Objekte mit Hilfe der folgenden Bindungszeichenfolge herzustellen:

   Set objUser = Get Object ("LDAP://cn=Bob, cn=Users, ou=Sales, dc=MyDomain, dc=com"), wobei "cn" der allgemeine Name und "ou" die Organisationseinheit ist und "dc" aus den beiden Domänenkomponenten besteht, die den vollständigen DNS-Namen ergeben. Für den Benutzer-DN würden Sie Folgendes eingeben:

   ```
   cn=Bob,cn=Users,ou=Sales,dc=MyDomain,dc=com
   ```

6. Klicken Sie auf "Speichern".

   Wenn Sie diesen Verweis speichern, werden die Benutzerkontoinformationen in CA EEM geladen. So können Sie auf diese Benutzerdatensätze als globale Benutzer zugreifen und Anwendungsinformationen wie die Anwendungsbenutzergruppe und den Namen für die Benutzerrolle hinzufügen.

7. Überprüfen Sie den angezeigten Status, um sicherzustellen, dass die Bindung an das externe Verzeichnis ordnungsgemäß erfolgt ist und Daten geladen werden.

   Falls beim Status eine Warnung angezeigt wird, klicken Sie auf die Option zum Aktualisieren des Status. Falls beim Status ein Fehler angezeigt wird, korrigieren Sie die Konfiguration, klicken auf "Speichern" und wiederholen diesen Schritt.

8. Klicken Sie auf "Schließen".

Weitere Informationen

Planen des Benutzerspeichers (siehe Seite 40)
Arbeitsblatt für ein externes LDAP-Verzeichnis (siehe Seite 41)

Verweisen auf CA SiteMinder als Benutzerspeicher

Falls Ihre Benutzerkonten bereits für CA SiteMinder definiert sind, verweisen Sie bei der Konfiguration des Benutzerspeichers auf dieses externe Verzeichnis.

So verweisen Sie auf CA SiteMinder als Benutzerspeicher:

1. Melden Sie sich als Benutzer mit Administratorrechten bzw. als "EiamAdmin"-Benutzer bei einem CA Enterprise Log Manager-Server an.
2. Klicken Sie auf die Registerkarte "Verwaltung".

   Falls Sie sich als "EiamAdmin"-Benutzer anmelden, wird diese Registerkarte automatisch angezeigt.
3. Wählen Sie die untergeordnete Registerkarte "Benutzer- und Zugriffsverwaltung" aus, und klicken Sie im linken Teilfenster auf "Benutzerspeicher".

   Die CA EEM-Server-Konfiguration für den Benutzerspeicher wird angezeigt.
4. Wählen Sie die Option für den Verweis aus CA SiteMinder.

   CA SiteMinder-spezifische Felder werden angezeigt.

   a. Füllen Sie die Felder wie auf dem Arbeitsblatt für SiteMinder geplant aus.

   b. Um die von CA SiteMinder verwendeten Verbindungen und Ports anzuzeigen bzw. zu ändern, klicken Sie auf die Auslassungspunkte, um das Fenster für die Verbindungsattribute einzublenden.
5. Klicken Sie auf "Speichern".

   Wenn Sie diesen Verweis speichern, werden die Benutzerkontoinformationen in CA EEM geladen. So können Sie auf diese Benutzerdatensätze als globale Benutzer zugreifen und Anwendungsinformationen wie die Anwendungsbenutzergruppe und den Namen für die Benutzerrolle hinzufügen.
6. Überprüfen Sie den angezeigten Status, um sicherzustellen, dass die Bindung an das externe Verzeichnis ordnungsgemäß erfolgt ist und Daten geladen werden.

   Falls beim Status eine Warnung angezeigt wird, klicken Sie auf die Option zum Aktualisieren des Status. Falls beim Status ein Fehler angezeigt wird, korrigieren Sie die Konfiguration, klicken auf "Speichern" und wiederholen diesen Schritt.
7. Klicken Sie auf "Schließen".

Weitere Informationen

Planen des Benutzerspeichers (siehe Seite 40)
Arbeitsblatt für CA SiteMinder (siehe Seite 43)

Konfigurieren von Kennwortrichtlinien

Sie können Kennwortrichtlinien festlegen, um sicherzustellen, dass die von Benutzern selbst erstellten Kennwörter den festgelegten Vorgaben entsprechen und mit der vorgegebenen Häufigkeit geändert werden. Legen Sie die Kennwortrichtlinien fest, nachdem Sie den internen Benutzerspeicher eingerichtet haben. Kennwortrichtlinien können nur vom "EiamAdmin"-Benutzer bzw. einem Benutzer mit Administratorrolle festgelegt oder geändert werden.

Hinweis: Die Kennwortrichtlinien für CA Enterprise Log Manager gelten nicht für Benutzerkonten, die in einem externen Benutzerspeicher erstellt wurden.

So konfigurieren Sie Kennwortrichtlinien:

1. Melden Sie sich als Benutzer mit Administratorrechten bzw. als "EiamAdmin"-Benutzer bei einem CA Enterprise Log Manager-Server an.
2. Klicken Sie auf die Registerkarte "Verwaltung".

   Falls Sie sich als "EiamAdmin"-Benutzer anmelden, wird diese Registerkarte automatisch angezeigt.
3. Wählen Sie die untergeordnete Registerkarte "Benutzer- und Zugriffsverwaltung" aus, und klicken Sie im linken Teilfenster auf die Schaltfläche "Kennwortrichtlinie".

   Das Fenster "Kennwortrichtlinie" wird angezeigt.
4. Legen Sie fest, ob Kennwörter mit dem Benutzernamen identisch sein dürfen.
5. Legen Sie fest, ob Längenbeschränkungen gelten sollen.
6. Legen Sie fest, ob gemäß den Richtlinien eine maximale Anzahl gleicher Zeichen enthalten sein darf oder eine Mindestanzahl von Zahlen bzw. Ziffern enthalten sein muss.
7. Legen Sie Richtlinien für das Kennwortalter und die Wiederverwendung von Kennwörtern fest.
8. Überprüfen Sie die Einstellungen, und klicken Sie auf "Speichern".
9. Klicken Sie auf "Schließen".

   Die konfigurierten Kennwortrichtlinien gelten für alle CA Enterprise Log Manager-Benutzer.

Weitere Informationen

Planen der Kennwortrichtlinien (siehe Seite 44)
Benutzername als Kennwort (siehe Seite 45)
Kennwortalter und Wiederverwendung von Kennwörtern (siehe Seite 45)
Länge und Format von Kennwörtern (siehe Seite 46)

Aufbewahren vordefinierter Zugriffsrichtlinien

Falls Sie beabsichtigen, ausschließlich vordefinierte Anwendungsbenutzergruppen oder -rollen mit den zugehörigen vordefinierten Richtlinien zu verwenden, besteht ein gewisses Risiko, dass die vordefinierten Richtlinien versehentlich gelöscht oder unbrauchbar werden. Falls Ihre Administratoren beabsichtigen, eigene Rollen mit den zugehörigen Zugriffsrichtlinien zu verwenden, werden die vordefinierten Richtlinien bearbeitet, wobei es zu unbeabsichtigten Änderungen kommen kann. Daher empfiehlt es sich, eine Sicherungskopie der ursprünglichen vordefinierten Richtlinien zu erstellen, so dass die Richtlinien ggf. wiederhergestellt werden können.

Erstellen Sie mit der Exportfunktion eine Sicherungsdatei, die alle Arten von vordefinierten Richtlinien enthält. Sie können diese Dateien dann auf einem externen Datenträger speichern oder auf der Festplatte des Servers, auf dem der Export durchgeführt wurde, belassen.

Hinweis: Vorgehensweisen zum Sichern vordefinierter Richtlinien finden Sie im *CA Enterprise Log Manager-Administrationshandbuch*.

Erstellen des ersten Administrators

Dem ersten erstellten Benutzer muss die Administratorrolle zugewiesen werden. Nur Benutzer mit Administratorrolle können Konfigurationen vornehmen. Sie können die Administratorrolle einem neuen, von Ihnen erstellten Benutzerkonto oder einem bereits vorhandenen, in CA Enterprise Log Manager geladenen Benutzerkonto zuweisen.

Gehen Sie wie folgt vor:

1. Melden Sie sich als Standardbenutzer "EiamAdmin" beim CA Enterprise Log Manager-Server an.
2. Erstellen Sie den ersten Administrator.

   Auf welche Weise Sie den ersten CA Enterprise Log Manager-Administrator erstellen, ist davon abhängig, wie Sie den Benutzerspeicher konfigurieren.

   - Falls CA Enterprise Log Manager den internen Benutzerspeicher verwendet, erstellen Sie ein neues Benutzerkonto mit Administratorrolle.
   - Falls CA Enterprise Log Manager einen externen Benutzerspeicher verwendet, binden Sie einen bestehenden LDAP-Benutzer an das Verzeichnis. Nachdem Sie die Bindung zum externen Verzeichnis erstellt haben, rufen Sie aus dem externen Benutzerspeicher das Konto des Benutzers ab, dem eine CA Enterprise Log Manager-Rolle zugewiesen werden soll. Benutzerkonten aus externen Benutzerspeichern werden als globale Benutzer abgerufen. Sie können die bestehenden Benutzerkontodaten zwar nicht ändern, aber eine neue CAELM-Anwendungsbenutzergruppe oder -Rolle erstellen. Dem ersten Benutzer weisen Sie die Rolle des Administrators zu.

   Hinweis: Sie können in CA Enterprise Log Manager keine neuen Benutzer erstellen, wenn Sie einen externen Benutzerspeicher konfigurieren.
3. Melden Sie sich vom CA Enterprise Log Manager-Server ab.
4. Melden Sie sich erneut mit den Anmeldedaten des neuen Benutzerkontos beim CA Enterprise Log Manager-Server an.

   Jetzt können Sie Konfigurationsaufgaben vornehmen.

Erstellen eines neuen Benutzerkontos

Sie können für jede Person, die CA Enterprise Log Manager verwenden soll, ein Benutzerkonto erstellen. Sie stellen die Anmeldeinformationen für die erste Anmeldung des Benutzers bereit und legen die jeweilige Rolle fest. Zu den drei vordefinierten Rollen gehören "Administrator", "Analyst" und "Auditor". Wenn sich Benutzer mit der Rolle "Analyst" bzw. "Auditor" anmelden, werden sie von CA Enterprise Log Manager anhand der gespeicherten Anmeldeinformationen authentifiziert und erhalten basierend auf der zugewiesenen Rolle Zugang zu verschiedenen Funktionen.

So erstellen Sie einen neuen Benutzer:

1. Melden Sie sich als Standardbenutzer "EiamAdmin" beim CA Enterprise Log Manager-Server an.

   Die Registerkarte "Verwaltung" und die untergeordnete Registerkarte "Benutzer- und Zugriffsverwaltung" werden angezeigt.

2. Klicken Sie im linken Teilfenster auf "Benutzer".
3. Klicken Sie links neben dem Ordner "Benutzer" auf die Option "Neuer Benutzer".

   Rechts im Fenster werden Detailinformationen zum neuen Benutzer angezeigt.

4. Geben Sie im Feld "Name" einen Benutzernamen ein. Bei Benutzernamen wird nicht zwischen Groß- und Kleinschreibung unterschieden.
5. Klicken Sie auf die Option zum Hinzufügen von Benutzerdetails für die Anwendung.
6. Wählen Sie die Rolle aus, die den künftigen Aufgaben dieses Benutzers entspricht. Verschieben Sie sie mit dem Wechselsteuerelement in die Liste für die ausgewählten Benutzergruppen.
7. Stellen Sie für die übrigen Felder die gewünschten Werte bereit. Im Gruppenfeld für die Authentifizierung müssen Sie ein Kennwort (hier werden Groß und Kleinschreibung unterschieden) mit Bestätigung eingeben.
8. Klicken Sie auf "Speichern" und anschließend auf "Schließen".

Weitere Informationen

Zuweisen einer Rolle zu einem globalen Benutzer (siehe Seite 140)

Zuweisen einer Rolle zu einem globalen Benutzer

Sie können nach einem vorhandenen Benutzerkonto suchen und die Anwendungsbenutzergruppe für die Rolle zuweisen, die der einzelne Benutzer ausführen soll. Wenn Sie auf einen externen Benutzerspeicher verweisen, gibt die Suche globale Datensätze zurück, die aus diesem Benutzerspeicher geladen wurden. Wenn Ihr konfigurierter Benutzerspeicher der CA Enterprise Log Manager-Benutzerspeicher ist, gibt die Suche Datensätze zurück, die für Benutzer in CA Enterprise Log Manager erstellt wurden.

Nur Administratoren können Benutzerkonten bearbeiten.

So weisen Sie einem vorhandenen Benutzer eine Rolle oder Anwendungsbenutzergruppe zu:

1. Klicken Sie auf die Registerkarte "Verwaltung" und auf die Unterregisterkarte "Benutzer- und Zugriffsverwaltung".
2. Klicken Sie im linken Fensterbereich auf "Benutzer".

   Die Fensterbereiche "Benutzer suchen" und "Benutzer" werden eingeblendet.
3. Wählen Sie "Globale Benutzer" aus, geben Sie Suchkriterien ein, und klicken Sie auf "Los".

   Wenn Sie nach geladenen Benutzerkonten suchen, wird im Fenster "Benutzer" der Pfad angezeigt, und die Bezeichnung für den Pfad gibt das externe Verzeichnis an, auf das verwiesen wurde.

   Wichtig! Geben Sie bei der Suche immer Kriterien ein, damit nicht alle Einträge in einem externen Benutzerspeicher angezeigt werden.
4. Wählen Sie einen globalen Benutzer aus, der kein Mitglied einer CA Enterprise Log Manager-Anwendungsgruppe ist.

   Auf der Seite "Benutzer" werden der Ordnername, Details zum globalen Benutzer und ggf. Angaben zu einer Mitgliedschaft in einer globalen Gruppe angezeigt.
5. Klicken Sie auf "Anwendungsbenutzerdetails hinzufügen".

   Das "CAELM"-Fenster mit Benutzerdetails wird erweitert.
6. Wählen Sie unter "Verfügbare Benutzergruppen" die gewünschte Gruppe aus, und klicken Sie auf den Pfeil nach rechts.

   Die ausgewählte Gruppe wird im Feld "Ausgewählte Benutzergruppen" angezeigt.
7. Klicken Sie auf "Speichern".

8. Überprüfen Sie die hinzugefügte Gruppe.
    a. Klicken Sie im Fenster "Benutzer suchen" auf "Anwendungsbenutzerdetails", und klicken Sie auf "Los".
    b. Überprüfen Sie, ob der Name des neuen Anwendungsbenutzers in den angezeigten Ergebnissen angezeigt wird.
9. Klicken Sie auf "Schließen".

Kapitel 5: Konfigurieren von Services

Dieses Kapitel enthält folgende Themen:

Ereignisquellen und Konfigurationen

Die meisten Netzwerke arbeiten mit einigen Windows- und einigen Syslog-basierten Geräten, deren Ereignisprotokolle erfasst, gespeichert, überwacht und überprüft werden müssen. Eventuell sind in Ihrem Netzwerk noch andere Geräte- und Systemtypen installiert, wie Anwendungen, Datenbanken, Kartenlesegeräte, biometrische Systeme oder CA Audit-Recorder und -iRecorder. Die CA Enterprise Log Manager-Services, -Adapter, -Agenten und -Connectors stehen für diese Konfigurationen, die erforderlich sind, damit eine Verbindung mit diesen Ereignisquellen hergestellt werden kann und Ereignisdaten empfangen werden können.

Die CA Enterprise Log Manager-Services umfassen die folgenden Bereiche für Konfigurationen und Einstellungen:

- Globale Konfigurationen
- Globale Filter und Einstellungen
- Einstellungen für den Ereignisprotokollspeicher
- ODBC-Server-Einstellungen
- Einstellungen für den Berichtsserver
- Konfiguration des Moduls für automatische Software-Updates
- Zugriffsbereich "Systemstatus"

Die Servicekonfigurationen können global sein, das heißt, dass sie für alle unter dem gleichen Anwendungsinstanznamen auf dem Verwaltungsserver installierten CA Enterprise Log Manager-Server gelten. Konfigurationen können allerdings auch lokal sein, dann gelten sie nur für einen ausgewählten Server. Konfigurationen werden auf dem Verwaltungsserver gespeichert, wobei eine lokale Kopie auf dem CA Enterprise Log Manager-Quellserver verbleibt. So kann die Ereigniserfassung auf den (agentenlosen) Quellservern für Protokolldateien auch dann ohne Unterbrechung fortgesetzt werden, falls die Netzwerkverbindung unterbrochen wird oder der Verwaltungsserver ausfällt.

Der Zugriffsbereich "Systemstatus" enthält Tools, die für einen CA Enterprise Log Manager-Server und dessen Dienste gelten und mit denen Informationen für den Support gesammelt werden können. Zusätzliche Informationen zu diesem Bereich finden Sie im Administrationshandbuch und in der Online-Hilfe.

Bearbeiten globaler Konfigurationen

Sie können globale Konfigurationen für alle Services festlegen. Beim Versuch, Werte außerhalb des zulässigen Bereichs zu speichern, wird CA Enterprise Log Manager standardmäßig je nachdem auf den minimalen oder maximalen Wert gesetzt. Einige Einstellungen hängen voneinander ab.

So bearbeiten Sie globale Einstellungen:

1. Klicken Sie auf die Registerkarte "Verwaltung" und auf die Unterregisterkarte "Services".

   Die Service-Liste wird angezeigt.

2. Klicken Sie in der Service-Liste auf "Globale Konfiguration".

   Das Detailfenster "Globale Service-Konfiguration" wird geöffnet.

3. Folgende Konfigurationseinstellungen können geändert werden:

   Aktualisierungsintervall

   Gibt die Häufigkeit (Sekunden) an, mit der die Serverkomponenten Konfigurationsaktualisierungen anwenden.

   Minimum: 30

   Maximum: 86400

   Sitzungszeitlimit

   Gibt die maximale Länge einer inaktiven Sitzung an. Ist die Option zur automatischen Aktualisierung aktiviert, laufen die Sitzungen nie ab.

   Minimum: 10

   Maximum: 60

Automatische Aktualisierung zulassen

Berechtigt den Benutzer zum automatischen Aktualisieren von Berichten und Abfragen. Mit dieser Einstellung können Administratoren die automatische Aktualisierung global deaktivieren.

Häufigkeit der automatischen Aktualisierung

Gibt an, in welchen minütlichen Abständen die Berichtsansicht aktualisiert wird. Diese Einstellung ist von der Auswahl der Option "Automatische Aktualisierung zulassen" abhängig.

Minimum: 1

Maximum: 600

Automatische Aktualisierung zulassen

Legt die automatische Aktualisierung in allen Sitzungen fest. Standardmäßig ist die Funktion nicht aktiviert.

Zum Anzeigen von Aktionsalarmen ist eine Authentifizierung erforderlich

Verhindert die Anzeige von Aktionsalarm-RSS-Feeds für Auditoren oder Produkte anderer Hersteller. Diese Einstellung ist standardmäßig aktiviert.

Standardbericht

Legt den Standardbericht fest.

Start des Standardberichts aktivieren

Zeigt den Standardbericht an, wenn Sie auf die Registerkarte "Berichte" klicken. Diese Einstellung ist standardmäßig aktiviert.

4. Folgende Einstellungen für Berichts- und Abfragekennung können geändert werden:

Berichtskennungen ausblenden

Verhindert, dass die angegebenen Kennungen in einer Kennungsliste angezeigt werden. Durch das Ausblenden von Kennungen wird die Anzeige der verfügbaren Berichte vereinfacht.

Abfragekennungen ausblenden

Dient zum Ausblenden ausgewählter Kennungen. Ausgeblendete Kennungen werden nicht in der Hauptabfrageliste oder der Abfrageliste für die Aktionsalarmplanung angezeigt. Beim Ausblenden von Abfragekennungen wird die Anzeige der verfügbaren Abfragen angepasst.

5. Folgende Profileinstellungen können geändert werden:

   Standardprofil aktivieren

   Dient zum Festlegen des Standardprofils.

   Standardprofil

   Legt das Standardprofil fest.

   Profile ausblenden

   Dient zum Ausblenden ausgewählter Profile. Wenn die Oberfläche aktualisiert wird oder das Aktualisierungsintervall abläuft, werden keine ausgeblendeten Profile angezeigt. Beim Ausblenden von Profilen wird die Anzeige der verfügbaren Profile angepasst.

   Hinweis: Klicken Sie auf "Zurücksetzen", um die zuletzt gespeicherten Werte wiederherzustellen. Sie können eine einzelne Änderung oder mehrere Änderungen zurücksetzen, solange Sie die Änderungen noch nicht gespeichert haben. Nach dem Speichern von Änderungen können Sie diese nur einzeln zurücksetzen.

6. Klicken Sie auf "Speichern".

Arbeiten mit globalen Filtern und Einstellungen

Sie können bei der Konfiguration Ihres CA Enterprise Log Manager-Servers globale Filter und Einstellungen festlegen. Globale Einstellungen werden nur für die aktuelle Sitzung gespeichert und gehen verloren, wenn Sie sich vom Server abmelden, außer Sie wählen die Option "Als Standard festlegen" aus.

Ein globaler *Schnellfilter* steuert das anfängliche Zeitintervall, für das Berichte erstellt werden, bietet einen einfachen Filter für den Textabgleich und ermöglicht Ihnen die Verwendung bestimmter Felder und Werte, um festzulegen, welche Daten in einem Bericht angezeigt werden.

Über einen globalen *erweiterten Filter* können Sie mittels SQL-Syntax und Operatoren die Berichtsdaten noch weiter auf Ihre Wünsche abstimmen. Über die globalen Einstellungen können Sie eine Zeitzone festlegen, spezielle Abfragen zum Abrufen von Daten auf anderen CA Enterprise Log Manager-Servern in einer Föderation verwenden und die automatische Aktualisierung von Berichten während der Anzeige aktivieren.

Sie sollten sinnvolle globale Filter festlegen, die in verschiedenen Berichtsbereichen verwendet werden können. Indem Sie Optionen definieren, durch die der globale Filter eingegrenzt wird, können Sie steuern, wie viele Daten in einem Bericht angezeigt werden. Zunächst müssen Sie für globale Filter und Einstellungen folgende Aufgaben durchführen:

- Konfigurieren globaler Schnellfilter, mit denen die anfängliche Zeit für die Berichte dieses CA Enterprise Log Manager-Servers festgelegt wird
- Auswählen föderierter Abfragen auf der Registerkarte "Einstellungen" zum Anzeigen von Daten für CA Enterprise Log Manager-Server, die sich in einer Föderation (Verbund) mit diesem Server befinden
- Festlegen, ob Berichte automatisch aktualisiert werden sollen
- Festlegen des Intervalls, mit dem die Berichtsdaten aktualisiert werden sollen

Hinweis: Falls Sie den globalen Filter zu eng oder zu spezifisch einstellen, werden bestimmte Daten unter Umständen in einigen Berichten nicht angezeigt.

Weitere Informationen zu globalen Filtern und ihrer Verwendung finden Sie in der Online-Hilfe.

Weitere Informationen

Bearbeiten globaler Konfigurationen (siehe Seite 144)

Verwenden föderierter Abfragen

Sie können wählen, ob Sie Abfragen an föderierten Daten ausführen möchten. Falls Sie planen, mehrere CA Enterprise Log Manager-Server in einem Verbundnetzwerk zu verwenden, können Sie das Kontrollkästchen "Föderierte Abfragen ausführen" aktivieren. Mit dieser Option können Sie Ereignisdaten für die Berichterstellung von allen CA Enterprise Log Manager-Servern einholen, die sich mit diesem CA Enterprise Log Manager-Server in einem Verbund befinden (d. h. als untergeordnete Server dieses Servers fungieren).

Sie können die föderierten Abfragen auch für eine bestimmte Abfrage deaktivieren, falls nur die Daten des aktuellen CA Enterprise Log Manager-Servers angezeigt werden sollen.

So aktivieren Sie föderierte Abfragen:

1. Melden Sie sich beim CA Enterprise Log Manager-Server an.
2. Klicken Sie auf die Schaltfläche "Globale Filter anzeigen/bearbeiten".

   Die Schaltfläche befindet sich rechts neben dem Namen des aktuellen CA Enterprise Log Manager-Servers, direkt über den Hauptregisterkarten.
3. Klicken Sie auf die Registerkarte "Einstellungen".
4. Legen Sie fest, ob föderierte Abfragen verwendet werden sollen.

   Falls Sie die Option für föderierte Abfragen deaktivieren, enthalten die angezeigten Berichte *keine* Ereignisdaten der Server, die als untergeordnete Server dieses Servers konfiguriert wurden.

Weitere Informationen

Konfigurieren einer CA Enterprise Log Manager-Föderation (siehe Seite 215)
Konfigurieren eines CA Enterprise Log Manager-Servers als untergeordneter Server (siehe Seite 216)

Konfigurieren des globalen Aktualisierungsintervalls

Sie können das Intervall festlegen, mit dem die CA Enterprise Log Manager-Services nach Konfigurationsänderungen suchen sollen. Der bei der Installation festgelegte Standardwert beträgt fünf Minuten und wird in Sekunden angegeben. Falls Sie sehr lange Intervalle festlegen, kann es vorkommen, dass notwendige Konfigurationsänderungen erst sehr zeitverzögert zur Anwendung kommen.

So konfigurieren Sie das Aktualisierungsintervall:

1. Melden Sie sich beim CA Enterprise Log Manager-Server an, und wählen Sie die Registerkarte "Verwaltung" aus.
2. Klicken Sie zuerst auf die Registerkarte "Services" und dann auf den Knoten "Globale Service-Konfiguration".
3. Geben Sie einen neuen Wert für das Aktualisierungsintervall ein.

   Der empfohlene Standardwert ist 300 Sekunden.

Wissenswertes über lokale Filter

Lokale Filter gelten für einen Live-Bericht während dessen Anzeige und setzen die globalen Einstellungen vorübergehend außer Kraft. Sie können mit lokalen Filtern die Daten in einem Bericht verfeinern und so Sicherheitsmängel beheben oder nach einem bestimmten Bericht in einer Liste der erstellten Berichte suchen. Die lokalen Konfigurationsaufgaben beinhalten Folgendes:

- Festlegen eines neuen Filters für einen angezeigten Live-Bericht
- Festlegen eines Filters für eine Liste mit erstellten Berichten zum Anzeigen einer Untergruppe der Liste anhand von Zeit oder Berichtstyp

Weitere Informationen zum Festlegen lokaler Filter während der Anzeige eines Berichts oder einer Berichtsliste finden Sie in der Online-Hilfe.

Konfigurieren des Ereignisprotokollspeichers

Der Ereignisprotokollspeicher ist die zugrunde liegende proprietäre Datenbank, die die erfassten Ereignisprotokolle enthält. Sie können globale und lokale Konfigurationsoptionen für den Ereignisprotokollspeicherservice festlegen, die die Speicherung und Archivierung von Ereignissen auf den CA Enterprise Log Manager-Servern betreffen. Die Konfiguration des Ereignisprotokollspeichers beinhaltet Folgendes:

- Kenntnisse zum Ereignisprotokollspeicherservice
- Kenntnisse zur Verarbeitung von Archivdateien durch den Ereignisprotokollspeicher
- Konfigurieren der globalen und lokalen Werte für den Ereignisprotokollspeicher

  Hierzu gehört das Festlegen der Datenbankgröße, der grundlegenden Werte für die Aufbewahrung von Archivdateien, der Zusammenfassungsregeln für die Aggregierung ähnlicher Ereignisse, der Unterdrückungsregeln, mit denen verhindert wird, dass bestimmte Ereignisse in der Datenbank gespeichert werden, der Föderationsbeziehungen und der Optionen für die automatische Archivierung.

CA Enterprise Log Manager schließt automatisch aktive Datenbankdateien und erstellt Archivdateien, wenn die aktiven Datenbanken die für diesen Service festgelegte Kapazität erreicht haben. Anschließend öffnet CA Enterprise Log Manager neue, aktive Dateien und setzt die Ereigniserfassung fort. Sie können Optionen für die automatische Archivierung für diese Dateien festlegen, allerdings nur als lokale Konfiguration für jeden einzelnen CA Enterprise Log Manager-Server.

Wissenswertes über den Ereignisprotokollspeicherservice

Der Ereignisprotokollspeicherservice verarbeitet Datenbankinteraktionen wie etwa die folgenden:

- Einfügen neuer Ereignisse in die aktuelle (Online)-Datenbank
- Abrufen von Ereignissen aus lokalen oder standortfernen föderierten Datenbanken für Abfragen und Berichte
- Erstellen neuer Datenbanken, wenn die aktuelle Datenbank vollständig belegt ist
- Erstellen neuer und Löschen alter Archivdateien
- Verwalten des Cache für Archivabfragen
- Anwenden ausgewählter Zusammenfassungs- und Unterdrückungsregeln
- Anwenden ausgewählter Ereignisweiterleitungsregeln
- Definieren der CA Enterprise Log Manager-Server, die als untergeordnete Verbundserver für diesen CA Enterprise Log Manager-Server fungieren

Wissenswertes über Archivdateien

Der CA Enterprise Log Manager-Server erstellt automatisch Standby-Datenbankdateien, auch *Archiv*dateien genannt, wenn eine Online-Datenbank die im Ereignisprotokollspeicherservice angegebene Einstellung "Maximale Zeilenanzahl" erreicht. Online-Datenbankdateien werden nicht komprimiert.

Wenn Sie die automatische Archivierung von einem (agentenlosen) Quellserver auf einen Berichtsserver einrichten, werden die Standby-Datenbanken auf dem Quellserver gelöscht, nachdem sie auf den Berichtsserver kopiert wurden. In diesem Fall hat die Einstellung "Maximale Anzahl an Archivtagen" keine Gültigkeit.

Wenn Sie die automatische Archivierung von einem Berichtsserver auf einen Remote-Speicherserver einrichten, werden die Standby-Datenbanken auf dem Berichtsserver nicht gelöscht, nachdem sie auf den Remote-Speicherserver kopiert wurden. Die Standby-Datenbanken verbleiben auf dem Berichtsserver, bis der für die Einstellung "Maximale Anzahl an Archivtagen" festgelegte Wert erreicht wurde. Dann werden sie *gelöscht*. Es wird allerdings eine Aufzeichnung dieser gelöschten Offline-Datenbanken aufbewahrt, so dass Sie Daten in der Archivdatenbank abfragen können, falls diese Informationen einmal für eine Wiederherstellung benötigt werden.

Bei der Festlegung des Werts für "Maximale Anzahl an Archivtagen" ziehen Sie den verfügbaren Speicherplatz auf dem Berichtsserver in Betracht. Der Grenzwert wird durch die Konfiguration der Einstellung "Festplattenspeicher für Archiv" vorgegeben. Falls der verfügbare Speicherplatz unter den festgelegten Prozentsatz fällt, werden Ereignisprotokolldaten gelöscht, um Platz zu schaffen, auch wenn die "Maximale Anzahl an Archivtagen" für diese Daten noch nicht abgelaufen ist.

Falls Sie keine automatische Archivierung von einem Berichtsserver auf einen Remote-Speicherserver verwenden, müssen Sie die Standby-Datenbanken manuell sichern und die Kopie manuell an den Remote-Speicherort verschieben, und zwar häufiger als die festgelegte "Maximale Anzahl an Archivtagen". Andernfalls können Daten verloren gehen. Es wird empfohlen, Archivdateien täglich zu sichern, um Datenverluste zu vermeiden und ausreichend Speicherplatz zu gewährleisten. Der Ereignisprotokollspeicherservice verwaltet seinen eigenen internen Cache für Abfragen in archivierten Datenbanken. So lässt sich die Leistung verbessern, falls wiederholte oder sehr weit gefasste Abfragen durchgeführt werden.

Weitere Informationen zur Arbeit mit Archivdateien finden Sie im *CA Enterprise Log Manager-Administrationshandbuch*.

Weitere Informationen

Beispiel: Automatische Archivierung über drei Server hinweg (siehe Seite 164)

Wissenswertes über die automatische Archivierung

Die Verwaltung gespeicherter Ereignisprotokolle erfordert einen sorgfältigen Umgang mit Sicherungen und wiederhergestellten Dateien. Die Konfiguration des Ereignisprotokollspeicherservice bietet Ihnen einen zentralen Ort für die Konfiguration und Optimierung von internen Datenbankgrößen und Aufbewahrungszeiten sowie für die Festlegung von Optionen für die automatische Archivierung. CA Enterprise Log Manager unterstützt Sie mit folgenden Skripten bei diesen Aufgaben:

- backup-ca-elm.sh
- restore-ca-elm.sh
- monitor-backup-ca-elm.sh

Hinweis: Die Verwendung dieser Skripten setzt voraus, dass Sie die nicht interaktive Authentifizierung zwischen den beiden Servern mittels RSA-Schlüsseln eingerichtet haben.

Die *Sicherungs*- und *Wiederherstellungs*skripten verwenden das Hilfsprogramm "LMArchive", um Ihnen das Kopieren von Standby-Datenbanken auf und von Remote-Hosts zu erleichtern. Die entsprechenden Katalogdateien werden nach Abschluss der Aufgaben automatisch von den Skripten aktualisiert. Sie können auf Remote-Server oder auf andere CA Enterprise Log Manager-Server kopieren. Falls es sich bei dem Remote-Host, an den Sie Dateien senden, um einen CA Enterprise Log Manager-Server handelt, werden die Katalogdateien auch auf dem empfangenden Server automatisch von den Skripten aktualisiert. Die Skripten löschen ferner die Archivdateien vom lokalen Rechner, um doppelte Einträge in Föderationsberichten zu vermeiden. So wird sichergestellt, dass Daten für Abfragen und Berichte verfügbar sind. Die Speicherung außerhalb des Systems wird Offline-Speicherung genannt. Sie können Dateien, die in einen Offline-Speicher verschoben wurden, für Abfragen und Berichte wiederherstellen.

Das *Überwachungs*skript führt das Sicherungsskript automatisch mit den Einstellungen aus, die Sie im Abschnitt für die automatische Archivierung während der Konfiguration des Ereignisprotokollspeicherservice festgelegt haben.

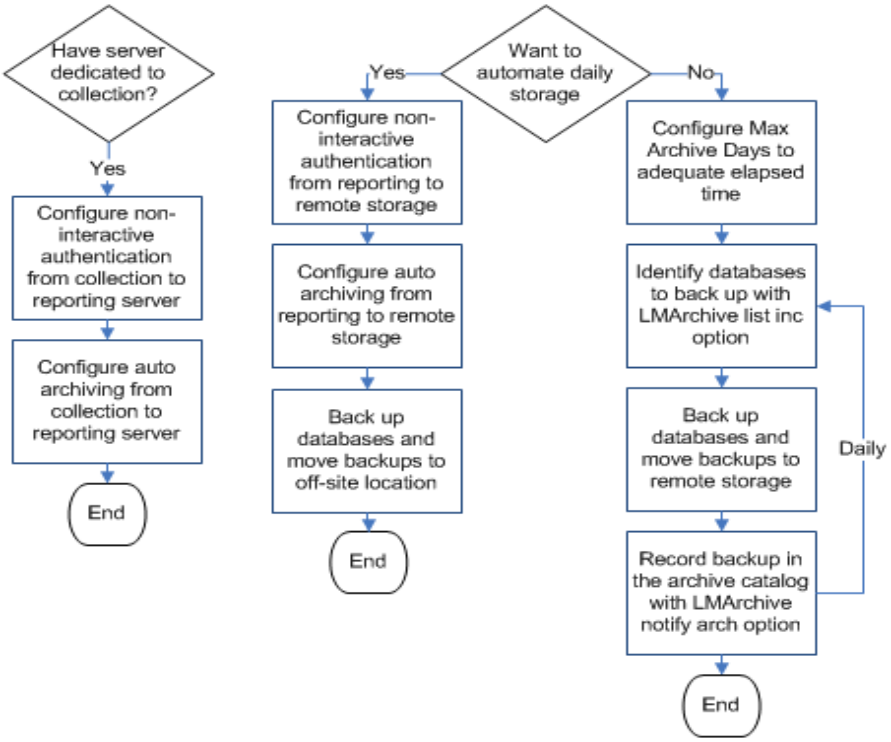
Weitere Informationen

Beispiel: Automatische Archivierung über drei Server hinweg (siehe Seite 164)

Flussdiagramm zum Verschieben der Datenbanken und Sicherungsstrategie

Sie können sowohl die Ereigniserfassung als auch die Berichterstellung auf den einzelnen CA Enterprise Log Manager-Server ausführen oder verschiedene Server für Ereigniserfassung und Berichterstellung festlegen. Wenn Sie Server für die Ereigniserfassung festlegen, sind stündliche, automatisierte Verschiebungen vom Sammelserver auf den Berichtsserver zu programmieren. Wenn Sie keinen Server spezifisch für die Ereigniserfassung festlegen, ist diese Automatisierung nicht nötig. Wenn über Sie keine dedizierten Serverrollen verfügen, legen Sie die Bezeichnung im Flussdiagramm "von Berichtsserver auf Remote-Speicher" als "von einem nicht dedizierten CA Enterprise Log Manager-Server auf Remote-Speicher" aus.

Die Sicherungsstrategie impliziert, dass zwei Kopien jeder Datenbank vorhanden sein müssen, wobei eine davon als Sicherung. Sie können dies mit oder ohne automatische Archivierung auf einem Remote-Speicherserver erreichen. Die Sicherungsstrategie mit automatischer Archivierung sieht die ursprünglichen Datenbanken auf dem Remote-Speicherserver und die Sicherungen an einem externen Speicherort vor. Die Sicherungsstrategie ohne automatische Archivierung sieht die ursprünglichen Datenbanken auf dem CA Enterprise Log Manager-Server und die Sicherungen auf einem Remote-Speicherserver vor. Ob Sie die ursprünglichen Datenbanken auf dem CA Enterprise Log Manager-Server speichern können, wo sie anfänglich archiviert wurden, hängt vom verfügbaren Platz für langfristige Speicherungen sowie den Speicherrichtlinien ab. Wenn diesen Kriterien entsprochen wird, hängt die Entscheidung von persönlicher Präferenz ab.



Konfigurieren von nicht interaktiver Authentifizierung für die automatische Archivierung

Sie können festlegen, dass die automatische Archivierung zwischen Servern unterschiedliche Rollen haben kann. Beispiel:

- Von einem oder mehreren Sammelservern zu einem einzelnen Berichtsserver
- Von einem oder mehreren Berichtsservern zu einem einzelnen Remote-Speicherserver.

Bevor Sie die automatische Archivierung von einem Server zu einem anderen konfigurieren, konfigurieren Sie nicht interaktive *ssh*-Authentifizierung vom Quellserver zum Zielserver. *Nicht interaktiv* bedeutet, dass ein Server Dateien auf den anderen Server verschieben kann, ohne dass Kennwörter erforderlich sind.

- Wenn Sie nur drei Server haben, einen Sammelserver, einen Berichtsserver und einen Remote-Speicherserver, konfigurieren Sie die nicht interaktive Authentifizierung zweimal:
  - Vom Sammelserver zum Berichtsserver
  - Vom Berichtsserver zum Remote-Speicherserver
- Wenn Sie sechs Server haben, vier Sammelserver, einen Berichtsserver und einen Remote-Speicherserver, konfigurieren Sie die nicht interaktive Authentifizierung fünfmal:
  - Vom Sammelserver 1 zum Berichtsserver
  - Vom Sammelserver 2 zum Berichtsserver
  - Vom Sammelserver 3 zum Berichtsserver
  - Vom Sammelserver 4 zum Berichtsserver
  - Vom Berichtsserver zum Remote-Speicherserver

Zur Konfiguration von nicht interaktiver ssh-Authentifizierung zwischen zwei Servern werden RSA-Schlüsselpaare, ein privater Schlüssel und ein öffentlicher Schlüssel verwendet. Sie kopieren den ersten öffentlichen Schlüssel, den Sie generieren, als "authorized_keys" zum Zielserver. Wenn Sie mehrere Instanzen von nicht interaktiver Authentifizierung für den gleichen Zielberichtsserver konfigurieren, kopieren Sie die zusätzlichen öffentlichen Schlüssel in die eindeutigen Dateinamen, um somit zu vermeiden, dass der ursprüngliche "authorized_keys" überschrieben wird. Verbinden Sie diese Dateinamen mit "authorized_keys". Zum Beispiel würden Sie "authorized_keys_ELM-C2" und "authorized_keys_ELM-C3" zu Datei "authorized_keys" aus ELM-C1 anhängen.

Beispiel: Konfigurieren von nicht interaktiver Authentifizierung für Hub-and-Spoke

Die Existenz von nicht interaktiver Authentifizierung zwischen zwei Servern gilt als Voraussetzung für die automatische Archivierung von der Quelle zum Zielserver. Beim Konfigurieren der nicht interaktiven Authentifizierung ist es üblich, dass mehrere Quellserver, die für die Erfassung festgelegt wurden, einen gemeinsamen Zielserver zur Berichterstellung/Verwaltung haben. Dieses Beispiel geht von einer mittelgroßen CA Enterprise Log Manager-Föderation aus, mit einem Server zur Berichterstellung/Verwaltung (Hub), vier Sammelservern (Spoke) und einem Remote-Speicherserver. Die Namenskonventionen für Server jeder Serverrolle lauten wie folgt:

- CA Enterprise Log Manager-Server zur Berichterstellung/Verwaltung: ELM-RPT
- CA Enterprise Log Manager-Sammelserver: ELM-C1, ELM-C2, ELM-C3, ELM-C4
- Remote-Speicherserver: RSS

Die Vorgehensweisen für das Aktivieren der nicht interaktiven Authentifizierung für die CA Enterprise Log Manager-Föderation lauten wie folgt:

1. Generieren Sie vom ersten Sammelserver ein RSA-Schlüsselpaar als "caelmservice" und kopieren Sie den öffentlichen Schlüssel als "authorized_keys" in das Verzeichnis "/tmp" auf dem Zielberichtsserver.
2. Generieren Sie bei Bedarf von jedem zusätzlichen Sammelserver ein RSA-Schlüsselpaar und kopieren Sie den öffentlichen Schlüssel als "authorized_keys_n", wobei "n" die Quelle angibt.
3. Verbinden Sie den Inhalt dieser öffentlichen Schlüsseldateien vom Verzeichnis "/tmp" des Berichtsservers zum ursprünglichen "authorized_keys". Erstellen Sie ein ".ssh"-Verzeichnis und ändern Sie die Besitzerrechte des Verzeichnisses auf "caelmservice", verschieben Sie "authorized_keys" in das ".ssh"-Verzeichnis und legen Sie die Eigentümerschaft für die Schlüsseldatei sowie die entsprechenden Berechtigungen fest.
4. Überprüfen Sie, dass nicht interaktive Authentifizierung zwischen jedem Sammelserver und dem Berichtsserver vorhanden ist.
5. Erstellen Sie vom Remote-Speicherserver eine Verzeichnisstruktur für das ".ssh"-Verzeichnis, wobei der Standard "/opt/CA/LogManager" lautet. Erstellen Sie ein ".ssh"-Verzeichnis auf dem Ziel und ändern Sie die Besitzerrechte auf "caelmservice".
6. Generieren Sie vom Berichtserver ein RSA-Schlüsselpaar als "caelmservice" und kopieren Sie den öffentlichen Schlüssel als "authorized_keys" in das Verzeichnis "/tmp" auf dem Remote-Speicherserver.

7. Verschieben Sie vom Remote-Speicherserver aus "authorized_keys" von "/tmp" in das ".ssh"-Verzeichnis und legen Sie die Eigentümerschaft für die Schlüsseldatei mit den erforderlichen Berechtigungen auf "caelmservice" fest.
8. Überprüfen Sie, dass nicht interaktive Authentifizierung zwischen dem Berichtsserver und dem Remote-Speicherserver vorhanden ist.

Konfigurieren der Schlüssel für das Paar "Erster Sammelserver-Berichterstellungsserver"

Für die Konfiguration von nicht interaktiver Authentifizierung der Hub-and-Spoke-Architektur muss ein Paar öffentlicher RSA-Schlüssel oder -Privatschlüssel auf dem Sammelserver generiert werden. Der öffentliche Schlüssel muss auf seinen Berichtsserver kopiert werden. Kopieren Sie die öffentliche Schlüsseldatei mit dem Namen *authorized_keys.* Nehmen Sie an, dass dieser Schlüssel der erste öffentliche Schlüssel ist, der auf den angegebenen Berichtsserver kopiert wird.

So generieren Sie ein RSA-Schlüsselpaar auf dem ersten Sammelserver und kopieren den öffentlichen Schlüssel auf den Berichtsserver

1. Melden Sie sich über "ssh" als "caelmadmin"-Benutzer bei ELM-C1 an.
2. Wechseln Sie die Benutzer zu "root".

   ```
   su –
   ```

3. Schalten Sie Benutzer auf das "caelmservice"-Konto um.

   ```
   su – caelmservice
   ```

4. Erzeugen Sie mit dem folgenden Befehl ein RSA-Schlüsselpaar:

   ```
   ssh-keygen –t rsa
   ```

5. Drücken Sie die Eingabetaste, um die Standardangaben zu bestätigen, wenn die folgenden Eingabeaufforderungen angezeigt werden:
   - Geben Sie die Datei ein, in der der Schlüssel gespeichert werden soll (/opt/CA/LogManager/.ssh/id_rsa):
   - Geben Sie eine Passphrase ein (leer bei keiner Passphrase):
   - Geben Sie die gleiche Passphrase erneut ein:
6. Wechseln Sie zu folgendem Verzeichnis: opt/CA/LogManager.
7. Ändern Sie die Berechtigungen für das Verzeichnis ".ssh" mit folgendem Befehl:

   ```
   chmod 755 .ssh
   ```

8. Gehen Sie zu ".ssh", wo der Schlüssel "id_rsa.pub" gespeichert ist.

   ```
   cd .ssh
   ```

9. Kopieren Sie die Datei "id_rsa.pub" mit dem folgenden Befehl auf ELM-RPT, den CA Enterprise Log Manager-Zielserver:

   ```
   scp id_rsa.pub caelmadmin@ELM-RPT:/tmp/authorized_keys
   ```

   Damit wird die Datei "authorized_keys" auf dem Berichtsserver mit dem Inhalt des öffentlichen Schlüssels erstellt.

Konfigurieren der Schlüssel für zusätzliche Paare "Sammelserver-Berichterstellungsserver"

Der zweite Schritt der Konfiguration nicht interaktiver Authentifizierung für eine Hub-and-Spoke-Architektur ist die Erstellung eines RSA-Schlüsselpaares auf jedem zusätzlichen Sammelserver. Dieses Paar muss anschließend in das Verzeichnis "/tmp" des gemeinsamen Berichtservers als "authorized_keys_n" kopiert werden, wobei "n" den Quellsammelserver angibt.

So generieren Sie ein RSA-Schlüsselpaar auf zusätzlichen Sammelservern und kopieren den öffentlichen Schlüssel auf einen gemeinsamen Berichtsserver

1. Melden Sie sich über ssh am Sammelserver ELM-C2 als "caelmadmin" an.
2. Wechseln Sie die Benutzer zu "root".
3. Schalten Sie Benutzer auf das "caelmservice"-Konto um.

   ```
   su – caelmservice
   ```

4. Erzeugen Sie mit dem folgenden Befehl ein RSA-Schlüsselpaar:

   ```
   ssh-keygen –t rsa
   ```

5. Drücken Sie die Eingabetaste, um die Standardangaben zu bestätigen, wenn die folgenden Eingabeaufforderungen angezeigt werden:
   - Geben Sie die Datei ein, in der der Schlüssel gespeichert werden soll (/opt/CA/LogManager/.ssh/id_rsa):
   - Geben Sie eine Passphrase ein (leer bei keiner Passphrase):
   - Geben Sie die gleiche Passphrase erneut ein:
6. Wechseln Sie zu folgendem Verzeichnis: /opt/CA/LogManager.
7. Ändern Sie die Berechtigungen für das Verzeichnis ".ssh" mit folgendem Befehl:

   ```
   chmod 755 .ssh
   ```

8. Gehen Sie zu ".ssh", wo der Schlüssel "id_rsa.pub" gespeichert ist.

9. Kopieren Sie die Datei "id_rsa.pub" mit dem folgenden Befehl auf ELM-RPT, den CA Enterprise Log Manager-Zielserver:

   ```
   scp id_rsa.pub caelmadmin@ELM-RPT:/tmp/authorized_keys_ELM-C2
   ```

   Damit wird die Datei "authorized_keys_ELM-C2" auf dem Berichtsserver mit dem Inhalt des öffentlichen Schlüssels erstellt.

10. Geben Sie "Ja" ein, gefolgt von dem "caelmadmin"-Kennwort des ELM-RPT
11. Geben Sie "Beenden" ein.
12. Wiederholen Sie die Schritte 1-11 dieser Vorgehensweise für den Sammelserver ELM-C3. Für Schritt 9 geben Sie Folgendes an:

    ```
    scp id_rsa.pub caelmadmin@ELM-RPT:/tmp/authorized_keys_ELM-C3
    ```

13. Wiederholen Sie die Schritte 1-11 dieser Vorgehensweise für den Sammelserver ELM-C4. Für Schritt 9 geben Sie Folgendes an:

    ```
    scp id_rsa.pub caelmadmin@ELM-RPT:/tmp/authorized_keys_ELM-C4
    ```

Erstellen einer einzelnen öffentlichen Schlüsseldatei auf dem Berichtsserver und Festlegen der Eigentumsrechte an der Datei

In unserem Szenario haben wir bisher Schlüsselpaare auf allen Sammelservern generiert und den Teil des öffentlichen Schlüssels in Form der folgenden Dateien auf den Berichtsserver kopiert:

- authorized_keys
- authorized_keys_ELM-C2
- authorized_keys_ELM-C3
- authorized_keys_ELM-C4

In Schritt 3 wird beschrieben, wie diese Dateien verknüpft werden, wie die entstandene öffentliche RSA-Schlüsseldatei in das richtige Verzeichnis verschoben und Verzeichnis- sowie Eigentumsrechte an der Datei auf "caelmservice" festgelegt werden.

So erstellen Sie die kombinierte, öffentliche Schlüsseldatei an dem richtigen Speicherort auf dem Berichtsserver und legen die Eigentümerschaft für die Datei fest:

1. Melden Sie sich mittels "ssh" als "caelmadmin"-Benutzer auf dem CA Enterprise Log Manager-Berichtsserver an.
2. Wechseln Sie die Benutzer zu "root".

3. Wechseln Sie zum Verzeichnis des CA Enterprise Log Manager-Ordners:

   ```
   cd /opt/CA/LogManager
   ```

4. Erstellen Sie dem Ordner ".ssh".

   ```
   mkdir .ssh
   ```

5. Übertragen Sie die Eigentümerschaft für den neuen Ordner mit folgendem Befehl auf den "caelmservice"-Benutzer und die "caelmservice"-Gruppe:

   ```
   chown caelmservice:caelmservice .ssh
   ```

6. Wechseln Sie zum Verzeichnis "/tmp"

7. Fügen Sie der Datei "authorized_keys", die den öffentlichen Schlüssel von EML-C1 enthält, die Inhalte der öffentlichen Schlüssel der Sammelserver ELM-C2, ELM-C3 und ELM-C4 hinzu.

   ```
   cat authorized_keys_ELM-C2 >> authorized_keys
   ```

   ```
   cat authorized_keys_ELM-C3 >> authorized_keys
   ```

   ```
   cat authorized_keys_ELM-C4 >> authorized_keys
   ```

8. Wechseln Sie zum Verzeichnis "opt/CA/LogManager/.ssh"

9. Kopieren Sie die Datei "authorized_keys" vom Ordner "/tmp" in den aktuellen Ordner ".ssh":

   ```
   cp /tmp/authorized_keys .
   ```

10. Übertragen Sie die Eigentümerschaft für die Datei "authorized_keys" auf das "caelmservice"-Konto:

    ```
    chown caelmservice:caelmservice authorized_keys
    ```

11. Ändern Sie die Berechtigungen für die Datei:

    ```
    chmod 755 authorized_keys
    ```

    755 steht für die Berechtigungen "Lesen und Ausführen" für alle Benutzer und "Lesen, Schreiben und Ausführen" für den Eigentümer der Datei

Hiermit ist die Konfiguration der kennwortlosen Authentifizierung zwischen den Sammelserver und dem Berichtsserver abgeschlossen.

Validieren von nicht interaktiver Authentifizierung zwischen Sammelserver und Berichtsserver

Sie können die Konfiguration der nicht interaktiven Authentifizierung zwischen dem Ausgangs- und dem Zielserver für beide Phasen der automatischen Archivierung überprüfen.

So validieren Sie die Konfiguration zwischen dem Quell- und dem Berichtsserver:

1. Melden Sie sich über ssh am Sammelserver ELM-C1 als "caelmadmin" an.
2. Wechseln Sie die Benutzer zu "root".
3. Schalten Sie Benutzer auf das "caelmservice"-Konto um.

   ```
   su – caelmservice
   ```

4. Geben Sie folgenden Befehl ein:

   ```
   ssh caelmservice@ELM-RPT
   ```

   Wenn Sie sich bei ELM-RPT anmelden, ohne eine Passphrase einzugeben, wird die nicht interaktive Authentifizierung zwischen ELM-C1 und ELM-RPT bestätigt.
5. Melden Sie sich bei ELM-C2 an und wiederholen Sie den Vorgang.
6. Melden Sie sich bei ELM-C3 an und wiederholen Sie den Vorgang.
7. Melden Sie sich bei ELM-C4 an und wiederholen Sie den Vorgang.

Erstellen einer Verzeichnisstruktur mit Eigentumsrechten auf dem Remote-Speicherserver

Bei dieser Vorgehensweise wird vorausgesetzt, dass der Remote-Speicherserver kein CA Enterprise Log Manager-Server ist und dass Sie neue Benutzer, eine Gruppe und eine Verzeichnisstruktur, die der Struktur eines CA Enterprise Log Manager-Servers entspricht, erstellen müssen. Diese Prozedur müssen Sie abschließen, bevor Sie den Schlüssel vom Berichtsserver aus versenden, da Sie das erstellte caelmadmin-Konto dazu verwenden, mit dem Berichtsserver zu kommunizieren.

So erstellen Sie eine Dateistruktur und legen Eigentumsrechte für Dateien auf dem Remote-Speicherserver fest

1. Melden Sie sich beim Remote-Speicherserver, RSS, über ssh als "root" an.
2. Erstellen Sie den neuen Benutzer "caelmadmin".
3. Erstellen Sie die Gruppe "caelmservice", und erstellen Sie dann den neuen Benutzer "caelmservice".
4. Erstellen Sie das Verzeichnis, das als Remote-Speicherort dient, wobei der Standard "/opt/CA/LogManager" lautet.

   Hinweis: Wenn Sie ein anderes Verzeichnis verwenden möchten, stellen Sie sicher, dass Sie das Verzeichnis angeben, wenn Sie den Remote-Speicherort für die automatische Archivierung konfigurieren.

5. Ändern Sie das Stammverzeichnis für "caelmservice" auf "/opt/CA/LogManager" oder das Verzeichnis des Remote-Speicherorts. Für das folgende Beispiel wird das Standardverzeichnis verwendet:

   ```
   usermod -d /opt/CA/LogManager caelmservice
   ```

6. Legen Sie die Dateiberechtigungen für "caelmservice" fest. Für das folgende Beispiel wird das Verzeichnis des Remote-Speicherorts verwendet:

   ```
   chown -R caelmservice:caelmservice /opt/CA/LogManager
   ```

7. Wechseln Sie zum Verzeichnis "/opt/CA/LogManager" oder zum Verzeichnis des Remote-Speicherorts.
8. Erstellen Sie dem Ordner ".ssh".
9. Übertragen Sie die Eigentümerschaft für den Ordner ".ssh" mit folgendem Befehl auf den "caelmservice"-Benutzer und die "caelmservice"-Gruppe:

   ```
   chown caelmservice:caelmservice .ssh
   ```

10. Melden Sie sich vom Remote-Speicherservers ab.

Konfigurieren der Schlüssel für das Paar "Berichtsserver – Remote-Speicherserver"

Nachdem Sie die nicht interaktive Authentifizierung von allen Sammelservern zum Berichtsserver konfiguriert und validiert haben, konfigurieren und validieren Sie die nicht interaktive Authentifizierung vom Berichtsserver zum Remote-Speicherserver.

In unserem Beispielszenario ist der erste Schritt der Konfiguration die Erstellung eines neuen RSA-Schlüsselpaars auf dem Berichtsserver, ELM-RPT. Anschließend wird der öffentliche Schlüssel als "authorized_keys" in das Verzeichnis "/tmp" des Remote-Speicherservers, RSS, kopiert.

So generieren Sie ein RSA-Schlüsselpaar auf dem Berichtsserver und kopieren es auf den Remote-Speicherserver

1. Melden Sie sich am Berichtsserver als "caelmadmin" an.
2. Wechseln Sie die Benutzer zu "root".
3. Schalten Sie Benutzer auf das "caelmservice"-Konto um.

   ```
   su – caelmservice
   ```

4. Erzeugen Sie mit dem folgenden Befehl ein RSA-Schlüsselpaar:

   ```
   ssh-keygen –t rsa
   ```

5. Drücken Sie die Eingabetaste, um die Standardangaben zu bestätigen, wenn die folgenden Eingabeaufforderungen angezeigt werden:
   - Geben Sie die Datei ein, in der der Schlüssel gespeichert werden soll (/opt/CA/LogManager/.ssh/id_rsa):
   - Geben Sie eine Passphrase ein (leer bei keiner Passphrase):
   - Geben Sie die gleiche Passphrase erneut ein:
6. Wechseln Sie zu folgendem Verzeichnis: opt/CA/LogManager.
7. Ändern Sie die Berechtigungen für das Verzeichnis ".ssh" mit folgendem Befehl:

   ```
   chmod 755 .ssh
   ```

8. Navigieren Sie zu dem Verzeichnis ".ssh".
9. Kopieren Sie die Datei "id_rsa.pub" mit dem folgenden Befehl auf RSS, den Remote-Zielspeicherserver:

   ```
   scp id_rsa.pub caelmadmin@RSS:/tmp/authorized_keys
   ```

   Dadurch wird die Datei "authorized_keys" im Verzeichnis "/tmp" auf dem Remote-Speicherserver mit dem Inhalt des öffentlichen Schlüssels erstellt.

Festlegen der Eigentumsrechte an der Schlüsseldatei auf dem Remote-Speicherserver

Sie können die Eigentümerschaft für eine Schlüsseldatei und Berechtigungen auf einem Remote-Speicherserver festlegen, nachdem Sie ein Schlüsselpaar auf dem Berichtsserver generiert und den öffentlichen Schlüssel auf diesen Remote-Speicherserver kopiert haben.

So verschieben Sie die öffentliche Schlüsseldatei an den richtigen Speicherort auf dem Remote-Speicherserver und legen die Eigentümerschaft für die Datei fest:

1. Melden Sie sich am Remote-Speicherserver als "caelmadmin" an.
2. Wechseln Sie die Benutzer zu "root".
3. Wechseln Sie zum Verzeichnis "/opt/CA/LogManager/.ssh".
4. Kopieren Sie die Datei "authorized_keys" vom Verzeichnis "/tmp" in das aktuelle Verzeichnis ".ssh":

   ```
   cp /tmp/authorized_keys .
   ```

5. Ändern Sie die Eigentümerschaft für die Datei "authorized_keys" mit folgendem Befehl:

   ```
   chown caelmservice:caelmservice authorized_keys
   ```

6. Ändern Sie die Berechtigungen für die Datei "authorized_keys":

   ```
   chmod 755 authorized_keys
   ```

   Jetzt ist die nicht interaktive Authentifizierung zwischen einem CA Enterprise Log Manager-Berichtsserver und dem für die Speicherung verwendeten Remote-Host eingerichtet.

Validieren von nicht interaktiver Authentifizierung zwischen Berichtsserver und Speicherserver

Bestätigen Sie, dass nicht interaktive Authentifizierung zwischen dem Berichtsserver und dem Remote-Speicherserver festgelegt wurde. Im Beispielszenario wird der Remote-Speicherserver RSS genannt.

So validieren Sie nicht interaktive Authentifizierung zwischen dem CA Enterprise Log Manager-Berichtsserver und dem Speicherserver

1. Melden Sie sich am Berichtsserver als "root" an.
2. Schalten Sie Benutzer auf das "caelmservice" um.

   ```
   su – caelmservice
   ```

3. Geben Sie folgenden Befehl ein:

   ```
   ssh caelmservice@RSS
   ```

   Somit können Sie sich am Remote-Speicherserver anmelden, ohne eine Passphrase einzugeben.

Beispiel: Konfigurieren von nicht interaktiver Authentifizierung über drei Server

Die einfachste Szenario zur Konfiguration einer nicht interaktiven Authentifizierung – Voraussetzung für die automatische Archivierung – besteht aus zwei CA Enterprise Log Manager-Server, einem Sammelserver und einem Berichts-/Verwaltungsserver sowie einem Remote-Speichersystem auf einem UNIX oder Linux-Server. In diesem Beispiel werden die drei für die automatische Archivierung vorbereiteten Server wie folgt genannt:

- NY-Sammel-ELM
- NY-Berichts-ELM
- NY-Speicherserver

Die Vorgehensweise zum Aktivieren der nicht interaktiven Authentifizierung lautet wie folgt:

1. Generieren Sie vom NY-Sammel-ELM das RSA-Schlüsselpaar als "caelmservice" und kopieren Sie den öffentlichen Schlüssel dieses Paares als "authorized_keys" in das Verzeichnis "/tmp" auf dem NY-Berichts-ELM.
2. Erstellen Sie ein ".ssh"-Verzeichnis auf NY-Berichts-ELM, ändern Sie die Eigentumsrechte auf "caelmservice", verschieben Sie "authorized_keys" vom Verzeichnis "/tmp" in das ".ssh"-Verzeichnis und legen Sie die Eigentumsrechte an der Schlüsseldatei mit den erforderlichen Berechtigungen auf "caelmservice" fest.
3. Validieren Sie nicht interaktive Authentifizierung zwischen NY-Sammel-ELM und NY-Berichts-ELM.
4. Generieren Sie vom NY-Berichts-ELM ein weiteres RSA-Schlüsselpaar als "caelmservice" und kopieren Sie den öffentlichen Schlüssel als "authorized_keys" in das Verzeichnis "/tmp" auf dem NY-Speicherserver.
5. Auf NY-Speicherserver erstellen Sie die Verzeichnisstruktur "/opt/CA/LogManager". Erstellen Sie in diesem Pfad ein ".ssh"-Verzeichnis, ändern Sie die Eigentumsrechte auf "caelmservice", verschieben Sie "authorized_keys" in dieses Verzeichnis und legen Sie die Eigentumsrechte an der Schlüsseldatei mit den erforderlichen Berechtigungen auf "caelmservice" fest.
6. Validieren Sie nicht interaktive Authentifizierung zwischen NY-Berichts-ELM und NY-Speicherserver.

Der Ablauf dieses Verfahrens ähnelt den Schritten des Hub-and-Spoke-Szenarios. Für ein Szenario mit drei Server überspringen Sie die Anweisungen in Schritt 2 für zusätzliche Paare "Sammelserver-Berichterstellungsserver" und die Anweisungen in Schritt 3 über das Verbinden der Dateien mit "authorized_keys".

Beispiel: Automatische Archivierung über drei Server hinweg

Wenn Sie die "Erfassen-Berichten-Architektur" verwenden, müssen Sie die automatische Archivierung von einem Erfassungs- auf einen Berichtsserver konfigurieren. Diese Konfiguration automatisiert das Verschieben einer warmen Datenbank erfasster und verfeinerter Daten auf den Berichtsserver, wo Sie darüber berichten können. Es ist gute Praxis, diese automatische Archivierung einmal pro Stunde einzuplanen anstatt einmal pro Tag; so lässt sich vermeiden, jeden Tag eine längere Zeit für umfangreiche Datentransfers aufwenden zu müssen. Wählen Sie einen Zeitplan aus auf der Basis Ihrer Auslastung sowie der Entscheidung, ob es besser ist, die Verarbeitung auf einmal oder über den Tag verteilt vorzunehmen. Wenn Datenbanken mit Hilfe der automatischen Archivierung von einem Erfassungsserver auf seinen Berichtsserver kopiert werden, dann werden diese Datenbanken auf dem Erfassungsserver gelöscht.

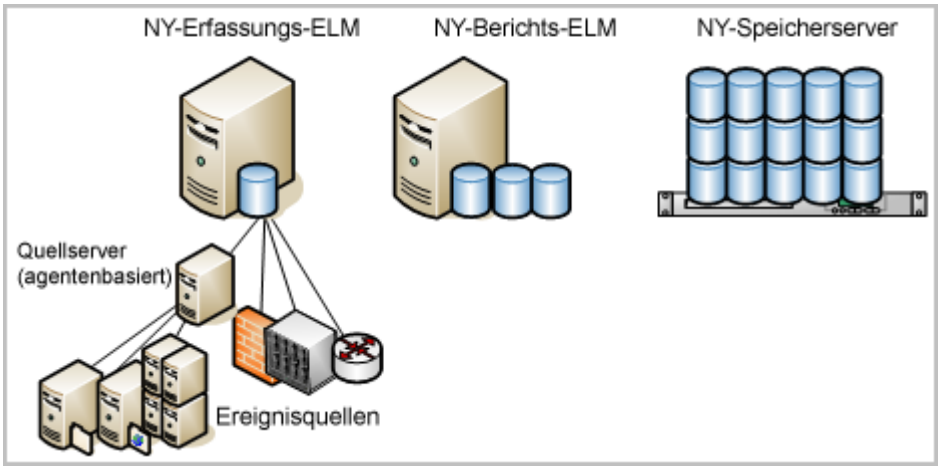
Wenn Sie einen lokalen Server mit viel Speicherplatz identifiziert haben, können Sie eine automatische Archivierung vom Berichtsserver auf einen solchen Remote-Speicherserver konfigurieren. Wenn Datenbanken mit Hilfe der automatischen Archivierung von einem Berichtsserver auf einen Remote-Speicherserver kopiert werden, bleiben diese Datenbanken auf dem Berichtsserver bestehen, bis der Zeitraum, den Sie als "Maximale Anzahl an Archivtagen" festgelegt haben, verstrichen ist. Dann werden sie gelöscht. Der Vorteil dieser Phase des automatischen Archivierens besteht darin, archivierte Datenbanken vor Verlust zu schützen, falls sie nicht manuell an einen Ablageort für die langfristige Speicherung verschoben werden, bevor das automatische Löschen erfolgt.

Hinweis: Bevor Sie einen Remote-Server für den Empfang automatisch archivierter Datenbanken konfigurieren, müssen Sie auf diesem Zielserver eine Verzeichnisstruktur einrichten, die der auf dem CA Enterprise Log Manager-Quellserver gleicht, und verschiedene Eigentumsrechte und Berechtigungen für die Authentifizierung zuweisen. Detaillierte Informationen finden Sie unter "Configuring Non-Interactive Authentication" ("Konfigurieren der nicht-interaktiven Authentifizierung") im *Implementation Guide (Implementierungsanleitung)*. Folgen Sie dabei den Anweisungen unter "Set Key File Ownership on a Remote Host" ("Schlüsseldatei-Eigentumsrechte auf einem Remote-Host festlegen").

Nehmen Sie bei diesem Beispiel an, Sie seien ein CA Enterprise Log Manager-Administrator in einem Datenzentrum in New York mit einem Netzwerk von CA Enterprise Log Manager-Servern, von denen jedem eine bestimmte Rolle zugeordnet ist, und einem Remote-Server mit umfangreicher Speicherkapazität. Die bei der automatischen Archivierung verwendeten Bezeichnungen der Server:

- NY-Erfassungs-ELM
- NY-Berichts-ELM
- NY-Speicherserver

Hinweis: In diesem Beispiel wird davon ausgegangen, dass ein Verwaltungsserver existiert, der ausschließlich für die Verwaltung des CA Enterprise Log Manager-Serversystems vorgesehen ist. Dieser Server wird hier nicht beschrieben, da er bei der automatischen Archivierung keine direkte Rolle spielt.

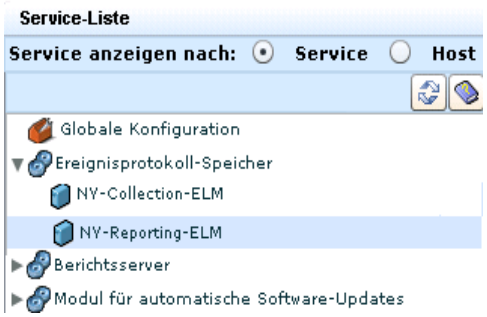


Für das Konfigurieren der automatischen Archivierung von einem Erfassungsserver auf einen Berichtsserver und dann von einem Berichtsserver auf einen Remote-Speicherserver können Sie das folgende Beispiel als Anleitung verwenden:

1. Klicken Sie auf die Registerkarte "Verwaltung" und auf die Unter-Registerkarte "Protokollerfassung".
2. Erweitern Sie den Ordner "Ereignisprotokollspeicher", und wählen Sie einen Erfassungsserver aus.

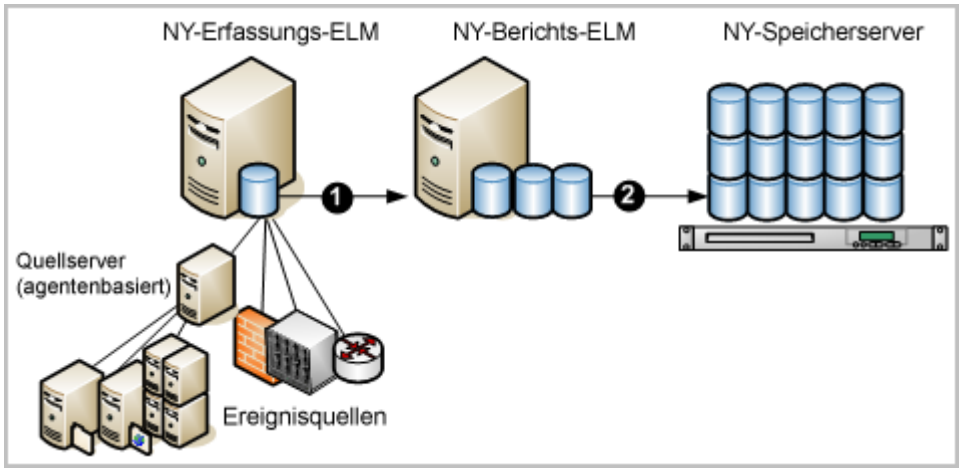
3. Legen Sie fest, dass die automatische Speicherung jede Stunde einmal erfolgen soll, mit dem Berichtsserver als Ziel Geben Sie die Berechtigungsnachweise eines CA Enterprise Log Manager-Benutzers mit Administratorrolle an. Wenn Sie benutzerdefinierte Richtlinien verwenden, muss dies ein Benutzer mit Bearbeitungsrechten für die Datenbankressource sein, da diese die Berechtigung einschließen, die archivierte Datenbank zu löschen.

4. Wählen Sie den Berichtsserver in der Liste "Services" aus.



5. Legen Sie fest, dass die automatische Speicherung einmal täglich erfolgen soll, wobei das Ziel der Speicherung der Remote-Server ist. Geben Sie die Berechtigungsnachweise eines CA Enterprise Log Manager-Benutzers mit Administratorrolle ein. Optional können Sie eine CALM-Zugriffsrichtlinie mit dem Recht zur Bearbeitung der Datenbankressource erstellen und einen Benutzer als Identität zuweisen. Geben Sie hier die Berechtigungsnachweise dieses Benutzers mit wenigen Berechtigungen ein.

Die Zahlen in der folgenden Grafik zeigen zwei Konfigurationen der automatischen Archivierung: eine vom Erfassungs- zum Berichtsserver und eine vom Berichts- zu einem Remote-Server im Netzwerk.

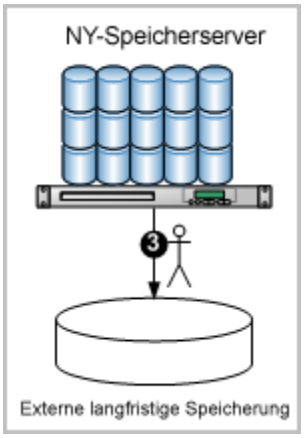


Mit solch einer Konfiguration läuft die automatische Archivierung folgendermaßen ab:

1. Der NY-Erfassungs-ELM, der CA Enterprise Log Manager-Erfassungsserver, erfasst und verfeinert Daten und fügt sie in die heiße Datenbank ein. Wenn die heiße Datenbank die konfigurierte Anzahl an Datensätzen erreicht hat, wird sie zu einer warmen Datenbank komprimiert. Da sich die automatische Archivierung dem Plan entsprechend stündlich wiederholt, kopiert das System einmal pro Stunde die warmen Datenbanken und verschiebt sie zum NY-Berichts-ELM, dem CA Enterprise Log Manager-Berichtsserver. Die warmen Datenbanken werden von NY-Erfassungs-ELM gelöscht, wenn sie verschoben werden.
2. Der NY-Berichts-ELM bewahrt die Datenbanken auf, so dass sie abgefragt werden können, bis sie das durch "Maximale Anzahl an Archivtagen" konfigurierte Alter erreicht haben und gelöscht werden. Da sich die automatische Archivierung dem Plan entsprechend täglich wiederholt, kopiert das System einmal pro Stunde die warmen Datenbanken und verschiebt sie als kalte Datenbanken zum NY-Speicherserver. Die kalten Datenbanken können für einen längeren Zeitraum auf dem Speicherserver verbleiben.

3. Sie verschieben die auf dem NY-Netzwerk-Speicherserver gespeicherten kalten Datenbanken dann zu einem externen langfristigen Speicherort, wo sie für die geforderte Anzahl Jahre aufbewahrt werden können.

   Der Grund für die Archivierung besteht darin, die Ereignisprotokolle für die Wiederherstellung verfügbar zu halten. Kalte Datenbanken können wiederhergestellt werden, wenn sich die Notwendigkeit ergibt, alte protokollierte Ereignisse zu untersuchen. Das manuelle Verschieben archivierter Datenbanken vom internen Speicherserver zu einem externen langfristigen Speicherort ist in der folgenden Grafik dargestellt.

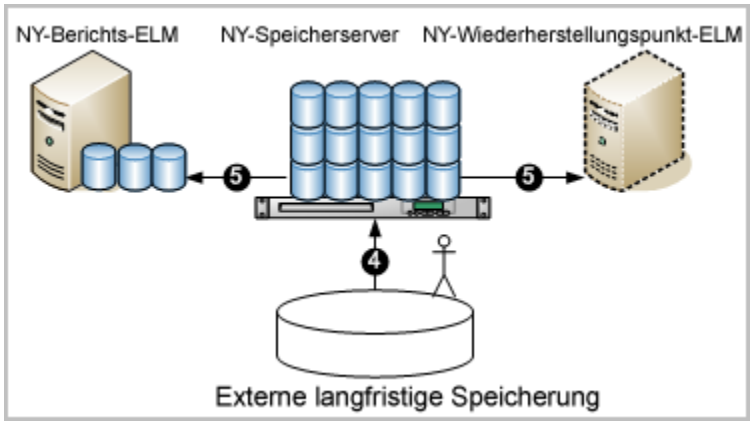


4. Stellen Sie sich eine Situation vor, die es nötig macht, gesicherte und nach extern verschobene Protokolle zu untersuchen. Um den Namen der wiederherzustellenden archivierten Datenbank zu ermitteln, suchen Sie im lokalen Archivkatalog über den NY-Berichts-ELM. (Klicken Sie auf die Registerkarte "Verwaltung", wählen Sie "Archivkatalogabfrage" im "Protokollerfassungs-Explorer", und klicken Sie auf "Abfrage".)

5. Rufen Sie die identifizierte archivierte Datenbank vom externen Speicherort ab. Kopieren Sie sie zurück zum Verzeichnis "/opt/CA/LogManager/data/archive" auf dem NY-Speicherserver. Ändern Sie dann die Eigentumsrechte an dem Archivverzeichnis nach "caelmservice-Benutzer".

6. Stellen Sie die Datenbank entweder auf dem ursprünglichen Berichtsserver wieder her oder an einem Wiederherstellungspunkt, der speziell für die Untersuchung von Protokollen aus wiederhergestellten Datenbanken vorgesehen ist. Gehen Sie dabei folgendermaßen vor:

   - Wenn die Wiederherstellung auf dem NY-Berichts-ELM erfolgen soll, führen Sie das Skript "restore-ca-elm.sh" vom NY-Berichts-ELM aus durch, und geben Sie den NY-Speicherserver als Remote-Host an.
   - Wenn die Wiederherstellung auf dem NY-Berichts-ELM erfolgen soll, führen Sie das Skript "restore-ca-elm.sh" vom NY-Berichts-ELM aus durch, und geben Sie den NY-Speicherserver als Remote-Host an.



Hinweis: Sie können nun die wiederhergestellten Daten abfragen und darüber berichten.

Weitere Informationen:

Wissenswertes über die automatische Archivierung (siehe Seite 151)
Wissenswertes über Archivdateien (siehe Seite 150)
Einstellungen für den Ereignisprotokollspeicher in einer einfachen Umgebung (siehe Seite 170)
Beispiel: Föderationsübersicht für ein großes Unternehmen (siehe Seite 35)

Einstellungen für den Ereignisprotokollspeicher in einer einfachen Umgebung

In einer Umgebung mit getrennten CA Enterprise Log Manager-Servern für die Rolle des (agentenlosen) Quellservers für Protokolldateien und des Berichtsservers sollten Sie die Ereignisprotokollspeicher einzeln als lokale Konfigurationen einrichten. Falls der Berichtsserver auch den Failover-Datenverkehr übernehmen soll, können Sie für "Maximale Zeilenanzahl" einen höheren Wert als den in der Tabelle angegebenen verwenden. Falls Sie den Verwaltungsserver als Berichtsserver verwenden, sollten Sie bedenken, dass der Verwaltungsserver eigene Ereignisinformationen in Form von selbstüberwachenden Ereignissen erzeugt.

Hinweis: Sie müssen jedes Serverpaar, das an der automatischen Archivierung beteiligt ist, für die nicht interaktive Authentifizierung einrichten, damit die Konfiguration für die automatische Archivierung ordnungsgemäß funktioniert.

Die folgende Tabelle ist ein Beispiel. Der CA Enterprise Log Manager-Quellserver für Protokolldateien heißt "CollSrvr-1". Der CA Enterprise Log Manager-Berichtsserver heißt "RptSrvr-1". Das Beispiel beinhaltet zudem den Remote-Speicherserver "RemoteStore-1" für die Speicherung von Offline-Datenbankdateien, die sich im Verzeichnis "/CA-ELM_cold_storage" befinden.

Ereignisprotokollspeicher-Feld	**Quellserver-Werte**	**Berichtsserver-Werte**
Maximale Zeilenzahl	2.000.000 (Standard)	Gilt nicht für die automatische Archivierung
Maximale Anzahl an Archivtagen	1 (gilt nicht für die autom. Archivierung)	30 (gilt für die autom. Archivierung und wenn die autom. Archivierung nicht konfiguriert ist)
Festplattenspeicher für Archiv	10	10
Exportrichtlinie	24	72
Sicherer Service-Port	17001	17001
Optionen für die automatische Archivierung		
Aktiviert	Ja	Ja
Sicherungstyp	Inkrementell	Inkrementell
Häufigkeit	Stündlich	Täglich
Startzeit	0	23
EEM-Benutzer	<CA Enterprise Log Manager_Administrator>	<CA Enterprise Log Manager_Administrator>
EEM-Kennwort	*<Kennwort>*	*<Kennwort>*
Remote-Server	RptSrvr-1	RemoteStore-1
Remote-Benutzer	caelmservice	user_X
Remote-Standort	/opt/CA/LogManager	/CA-ELM_cold_storage
Remote-ELM-Server	Ja	Nein

Mit den Optionen für die automatische Archivierung in diesem Beispiel werden stündlich Archivdateien (Standby-Datenbankdateien) vom Quellserver auf den Berichtsserver verschoben. So wird Speicherplatz auf dem Datenträger für eintreffende Ereignisse verfügbar gemacht. Beide Server verwenden eine inkrementelle Sicherung, damit keine großen Datenmengen auf einmal verschoben werden müssen. Nachdem eine Standby-Datenbank auf den Berichtsserver verschoben wurde, wird sie automatisch vom Quellserver für Protokolldateien gelöscht.

Hinweis: Der Wert "0" als Startzeit hat keine Auswirkung, wenn eine stündliche Sicherungshäufigkeit gewählt wurde.

Für "EEM-Benutzer" und "EEM-Kennwort" geben Sie die Anmeldeinformationen eines CA Enterprise Log Manager-Benutzers an, dem entweder die vordefinierte Administratorrolle zugewiesen ist oder eine benutzerdefinierte Rolle mit individueller Richtlinie, die dem Benutzer die Berechtigung zum Bearbeiten der Datenbankressourcen gibt.

Beim Berichtsserver legen Sie "/opt/CA/LogManager" als Remote-Standort und "caelmservice" als Remote-Benutzer fest, falls die automatische Archivierung vom Berichtsserver auf den Remote-Speicherserver stattfindet. Sie erstellen diesen Pfad und Benutzer, wenn Sie die nicht interaktive Authentifizierung zwischen diesen Servern einrichten.

Mit den Optionen für die automatische Archivierung in diesem Beispiel werden Archivdateien täglich ab 23.00 Uhr vom Berichtsserver auf den Remote-Speicherserver verschoben. Nachdem die Datenbank in den Offline-Speicher auf dem Remote-Server verschoben wurde, verbleibt sie für die "Maximale Anzahl an Archivtagen" auf dem Berichtsserver.

Falls die automatische Archivierung nicht aktiviert ist, werden Standby-Datenbanken basierend auf den für "Maximale Anzahl an Archivtagen" und "Festplattenspeicher für Archiv" konfigurierten Grenzwerten (je nachdem, welcher Wert zuerst auftritt) beibehalten. Archivierte Datenbanken werden im Beispiel 30 Tage lang auf dem Berichtsserver beibehalten, bevor sie gelöscht werden, außer der freie Speicherplatz fällt unter 10 Prozent. In diesem Fall erzeugt der Berichtsserver ein selbstüberwachendes Ereignis und löscht die ältesten Datenbanken, bis der freie Speicherplatz wieder über 10 Prozent liegt. Sie können einen Alarm erstellen, der Sie per E-Mail oder RSS-Feed auf diesen Umstand aufmerksam macht.

Wenn eine Datenbank von einem Remote-Speicherserver wieder auf dem ursprünglichen Berichtsserver hergestellt wird, wird sie drei Tage (72 Stunden) lang beibehalten.

Weitere Informationen zu diesen Feldern und ihren Werten finden Sie in der Online-Hilfe.

Festlegen von Optionen für den Ereignisprotokollspeicher

Im Konfigurationsdialogfeld für den Ereignisprotokollspeicher können Sie globale Optionen für alle CA Enterprise Log Manager-Server festlegen. Sie können auch auf den Pfeil neben dem Eintrag klicken, um den Knoten für den Ereignisprotokollspeicher zu erweitern. Hierdurch werden die einzelnen CA Enterprise Log Manager-Server im Netzwerk angezeigt. Klicken Sie ggf. auf diese Servernamen, um lokale Konfigurationsoptionen festzulegen, die nur für den jeweiligen Server gelten.

Benutzer mit Administratorrolle können jeden CA Enterprise Log Manager-Server von jedem anderen CA Enterprise Log Manager-Server aus konfigurieren.

So legen Sie Optionen für den Ereignisprotokollspeicher fest:

1. Melden Sie sich beim CA Enterprise Log Manager-Server an, und wählen Sie die Registerkarte "Verwaltung" aus.

   Die untergeordnete Registerkarte "Protokollerfassung" wird standardmäßig angezeigt.

2. Klicken Sie auf die untergeordnete Registerkarte "Services".

3. Wählen Sie den Eintrag für den Ereignisprotokollspeicher aus.

   Die Standardoptionen sind eine gute Anfangskonfiguration für ein mittelgroßes Netzwerk mit moderatem Datenverkehr.

   Weitere Informationen zu den einzelnen Feldern finden Sie in der Online-Hilfe.

   Hinweis: Die Tabelle "Untergeordnete Föderation" und die Tabelle für die automatische Archivierung werden nur angezeigt, wenn Sie die lokalen Optionen für einen bestimmten CA Enterprise Log Manager-Server aufrufen.

Hinweise zum ODBC-Server

Sie können einen ODBC-Client oder einen JDBC-Client installieren, um über eine externe Anwendung wie SAP BusinessObjects Crystal Reports auf den CA Enterprise Log Manager-Ereignisprotokollspeicher zuzugreifen.

Über diesen Konfigurationsbereich können Sie die folgenden Aufgaben durchführen:

- Aktivieren oder deaktivieren Sie den ODBC- und JDBC-Zugriff zum Ereignisprotokollspeicher.

- Legen Sie den für die Kommunikation zwischen dem ODBC- oder JDBC-Client und dem CA Enterprise Log Manager-Server verwendeten Dienstport fest.
- Geben Sie an, ob die Kommunikation zwischen dem ODBC- oder JDBC-Client und dem CA Enterprise Log Manager-Server verschlüsselt wird.

Die Feldbeschreibungen lauten wie folgt:

Dienste aktivieren

Gibt an, ob die ODBC- und JDBC-Clients auf Daten im Ereignisprotokollspeicher zugreifen können. Aktivieren Sie dieses Kontrollkästchen, um den externen Zugriff auf Ereignisse zu ermöglichen. Heben Sie die Auswahl des Kontrollkästchens auf, um den externen Zugriff zu deaktivieren.

Der ODBC-Dienst ist derzeit nicht FIPS-kompatibel. Heben Sie die Auswahl dieses Kontrollkästchens auf, wenn Sie eine Ausführung im FIPS-Modus beabsichtigen, um den Zugriff durch ODBC und JDBC zu verhindern. Somit wird nicht konformer Zugriff auf Ereignisdaten verhindert. Wenn Sie beabsichtigen, für im FIPS-Modus ausgeführte Vorgänge den ODBC- und JDBC-Dienst zu deaktivieren, vergewissern Sie sich, dass Sie diesen Wert für *jeden* Server eines Verbunds festlegen.

Listener-Port des Servers

Legt die von ODBC- oder JDBC-Diensten verwendete Portnummer fest. Der Standardwert ist "17002". Der CA Enterprise Log Manager-Server verweigert Verbindungsversuche, wenn in der Windows Data Source- oder JDBC-URL-Zeichenfolge ein anderer Wert angegeben wird.

Verschlüsselt (SSL)

Gibt an, ob die Kommunikation zwischen dem ODBC-Client und dem CA Enterprise Log Manager-Server verschlüsselt werden soll. Der CA Enterprise Log Manager-Server verweigert Verbindungsversuche, wenn der entsprechende Wert in der Windows Data Source oder der JDBC-URL nicht mit dieser Einstellung übereinstimmt.

Sitzungszeitlimit (Minuten)

Gibt die Anzahl der Minuten an, die eine im Leerlauf befindliche Sitzung geöffnet bleibt, bevor sie automatisch geschlossen wird.

Protokollebene

Bestimmt Typ und Ebene der Informationen, die in der Protokolldatei aufgezeichnet werden. Die Optionen in der Dropdown-Liste sind nach Detailgenauigkeit angeordnet, wobei die erste Option den niedrigsten Detailgrad bietet.

Auf alle Protokollierungen anwenden

Bestimmt, ob mit der Einstellung "Protokollebene" alle Protokolleinstellungen aus der Eigenschaftendatei des Protokolls überschrieben werden. Diese Einstellung gilt nur dann, wenn die Einstellung "Protokollebene" niedriger ist (d. h. einen höheren Detailgrad hat) als die Standardeinstellung.

Hinweise zum Berichtsserver

Der Berichtsserver regelt die Verwaltung automatisch verteilter Berichte und ihre Darstellung im PDF-Format. Außerdem verwaltet er die Erfassung von Aktionsalarmen und Berichten. Folgende Aufgaben können im Bereich für die Konfiguration des Berichtsservers erledigt werden:

- Erstellen benutzerdefinierter Listen:

  Benutzerdefinierte Listen (Schlüsselwerte)

  Dient der Erstellung von Relevanzgruppen bei der Berichterstellung sowie der Regelung der Zeiträume, die für diese gelten.

- Festlegen des Mail-Servers für Berichte, der Admin-E-Mail-Adresse und von SMTP-Port und Authentifizierungsinformationen im Bereich "E-Mail-Einstellungen".
- Festlegen von Firmenname und Logo, der Schriftarten und anderer PDF-Berichtseinstellungen im Bereich "Berichtskonfigurationen".
- Bestimmen der Höchstzahl der aufzubewahrenden Aktionsalarme sowie der Aufbewahrungsdauer im Bereich "Alarmaufbewahrung":

  Maximale Aktionsalarme

  Gibt an, wie viele Aktionsalarme zu Prüfzwecken auf dem Berichtsserver gespeichert werden sollen.

  Minimum: 50

  Maximum: 1000

  Aufbewahrungszeitraum für Aktionsalarme

  Gibt den maximalen Zeitraum in Tagen an, über den Aktionsalarme aufbewahrt werden.

  Minimum: 1

  Maximum: 30

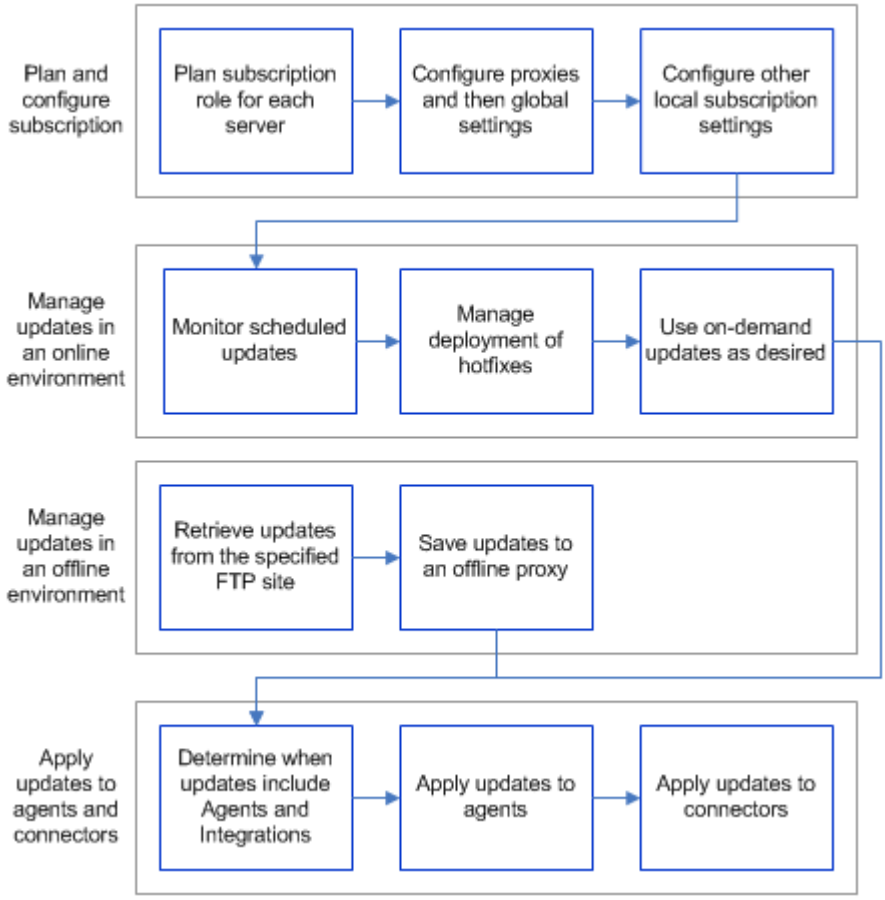
- Festlegen der Aufbewahrungsrichtlinie für den Wiederholungstyp der einzelnen geplanten Berichte im Bereich "Berichtsaufbewahrung".

- Bestimmen, ob oder wie oft das Hilfsprogramm für die Aufbewahrung entsprechend diesen Richtlinien automatisch nach Berichten sucht, die gelöscht werden können. Wenn das Hilfsprogramm für die Berichtsaufbewahrung beispielsweise einmal täglich ausgeführt wird, werden die Berichte, deren Alter den ausgewählten Zeitraum überschreitet, gelöscht.
- Festlegen von CA IT PAM-Prozesseinstellungen
- Festlegen von SNMP-Trap-Einstellungen

Flussdiagramm zur Bereitstellung automatischer Software-Updates

Sie verwalten Aktualisierungen für die CA Enterprise Log Manager-Anwendung, Agenten und Connectors sowie Aktualisierungen über die Funktion der automatischen Software-Updates. Im folgenden Flussdiagramm werden die Planung, Konfiguration und Verwaltung von Aktualisierungen in einer Online- und Offline-Umgebung sowie die Aktualisierung von Agenten und Connectors beschrieben. Die Planung und Konfiguration werden außerdem in diesem Handbuch beschrieben.

Hinweis: Weitere Informationen zu On-Demand-Aktualisierungen, Verwaltung von Aktualisierungen in einer Offline-Umgebung und Aktualisierungen von Agenten und Connectors finden Sie im *Administrationshandbuch*.



Konfigurieren von automatischen Software-Updates

Das Modul für automatische Software-Updates weist ähnlich wie andere Services globale und lokale Einstellungen auf.

Es unterscheidet sich von anderen Services in folgenden Punkten:

- Globale Einstellungen, bei denen die Auswahl von Proxy-Servern erforderlich ist, sind abhängig von den Einstellungen auf lokaler Ebene. Sie legen die Proxy-Server für automatische Inhaltsaktualisierungen auf globaler Ebene fest, die Liste der Proxy-Server wird aber erst gefüllt, nachdem Proxies konfiguriert wurden. Server, die als Proxies fungieren sollen, werden auf lokaler Ebene als Proxy- oder als Offline-Proxy-Server eingerichtet.
- Lokale CA Enterprise Log Manager-Server weisen unterschiedliche Konfigurationsanforderungen auf. Verschiedene Server haben unterschiedliche Rollen. Die Rolle eines Servers bestimmt, welche Einstellungen festgelegt werden müssen.

Die globalen Einstellungen für automatische Software-Updates finden folgende unterschiedliche Anwendung:

- Folgende Einstellungen können nicht auf lokaler Ebene außer Kraft gesetzt werden (d. h. sie sind ausschließlich global):
  - Standard-Proxy für automatische Software-Updates (CA-Software-Update-Proxy)
  - RSS-Feed-URL (von allen Online-Proxy-Servern verwendet)
  - Öffentlicher Schlüssel (von allen Online-Proxy-Servern verwendet)

    Wichtig! Diese Einstellung darf nicht von Hand geändert werden.
  - Aktualisierungen bereinigen, die älter sind als n Tage (gilt für alle Online- und Offline-Proxy-Server)
  - Automatischer Neustart nach Aktualisierung des Betriebssystems (gilt für alle Clients)

    Hinweis: Alle CA Enterprise Log Manager-Systeme sind Clients, auch die, die als Proxies bzw. Offline-Proxies fungieren.
  - Proxy-Server für automatische Inhaltsaktualisierungen
- Folgende Einstellungen werden nur auf lokaler Ebene konfiguriert:
  - Proxy für automatische Software-Updates
  - Offline-Update-Proxy

Bei den Einstellungen auf globaler Ebene, die auf lokaler Ebene außer Kraft gesetzt werden können, ist die Möglichkeit des Außerkraftsetzens davon abhängig, ob der Server als Online-Proxy oder als Client definiert wurde. Es gilt Folgendes:

- Einstellungen für Online-Proxies, die außer Kraft gesetzt werden können:
  - Fünf Einstellungen für den HTTP-Proxy-Server
  - Herunterzuladende Module
- Einstellung für Software-Update-Clients, die außer Kraft gesetzt werden kann:
  - Software-Update-Proxies für den Client

Konfigurieren der globalen Einstellungen für automatische Software-Updates

Sie können die globalen Einstellungen für automatische Software-Updates konfigurieren, sobald Sie alle CA Enterprise Log Manager-Server installiert haben.

Es wird empfohlen, die Proxy-Einstellung für die Server, die als Online- oder Offline-Update-Proxies fungieren sollen, festzulegen, bevor Sie die globalen Einstellungen für automatische Software-Updates konfigurieren. Über diese Einstellung werden die verfügbaren globalen Listen mit den Proxy-Servern für Clients und für Inhaltsaktualisierungen gefüllt.

So konfigurieren Sie die globalen Einstellungen für automatische Software-Updates:

1. Klicken Sie auf die Registerkarte "Verwaltung", klicken Sie auf "Services", klicken Sie auf das Modul "Automatisches Software-Update", und überprüfen Sie die Einstellungen für die globale Service-Konfiguration des Moduls für automatische Software-Updates im rechten Teilfenster.
2. Übernehmen oder ändern Sie die Einstellung für den Standard-Proxy für automatische Software-Updates (CA-Software-Update-Proxy). Beim *Standard-Proxy für automatische Software-Updates* handelt es sich in der Regel um den CA Enterprise Log Manager-Server, der zuerst installiert wurde und eventuell auch als CA Enterprise Log Manager-Verwaltungsserver fungiert. Dies ist der Server, der von den Online-Update-Clients kontaktiert wird, für die keine Software-Update-Proxy-Liste konfiguriert wurde. Falls eine solche Software-Update-Proxy-Liste vorhanden ist, die Suche jedoch keine Ergebnisse erbringt, ruft der Client Updates von diesem Standardserver ab.

   Hinweis: Diese Einstellung kann nicht auf lokaler Ebene überschrieben werden. Die hier festgelegte Einstellung gilt für alle CA Enterprise Log Manager-Server, die denselben CA Enterprise Log Manager-Verwaltungsserver verwenden.

3. Legen Sie den Zeitplan für den Standard-Proxy und die Online-Proxies fest, anhand dessen der CA-Software-Update-Server nach Updates durchsucht werden soll. Clients nehmen zum Abrufen von Aktualisierungen Kontakt zu Proxy-Servern auf, nachdem diese die betreffenden Aktualisierungen vom CA-Server für automatische Software-Updates heruntergeladen haben.

   a. Legen Sie im Feld "Aktualisierungshäufigkeit" in Stunden fest, wie oft der Standard-Proxy den CA-Software-Update-Server auf Updates durchsuchen soll.

   b. Halten Sie sich an folgende Richtlinien, wenn Sie die Einstellung "Startzeit der Aktualisierung" festlegen:

      - Falls Sie für die Aktualisierungshäufigkeit einen Wert unter 24 festlegen, treffen Sie für "Startzeit der Aktualisierung" keine Auswahl. Software-Updates beginnen, wenn iGateway gestartet wird.
      - Wenn Sie für die Aktualisierungshäufigkeit einen Wert gleich oder größer als 24 festlegen, legen Sie im 24-Stunden-Format fest, zu welcher Stunde die Aktualisierung beginnen soll.

4. Übernehmen Sie die vorkonfigurierte RSS-Feed-URL, die auf den CA-Software-Update-Server verweist. Diese URL ermöglicht die Auflistung der verfügbaren herunterzuladenden Module.

5. Übernehmen Sie den angezeigten öffentlichen Schlüssel, oder wählen Sie die richtige Version aus. Da dieser Schlüssel von allen Software-Update-Proxies verwendet wird, kann er nicht auf lokaler Serverebene geändert werden.

   Wichtig! Ändern Sie diesen Wert nur unter Anleitung des technischen Supports. Falls für ein bestimmtes Download eine Änderung des Schlüssels erforderlich ist, wird dieses Feld vor dem Download automatisch aktualisiert.

6. Legen Sie einen Wert in Tagen für die Aufbewahrungszeit der heruntergeladenen Updates auf dem System fest, oder übernehmen Sie den Standardwert "30". Lassen Sie ausreichend Zeit, damit das Download-Verzeichnis von einem Quell-Update-Proxy auf alle Offline-Update-Proxies kopiert und alle Updates auf alle Clients heruntergeladen und dort installiert werden können.

   Hinweis: Die Einstellung für die Bereinigung der Aktualisierungen gilt für alle Software-Update-Proxies und Offline-Update-Proxies. Sie kann nicht auf lokaler Ebene geändert werden.

7. Beachten Sie die folgenden Punkte beim Festlegen der Einstellung "Automatischer Neustart nach Aktualisierung des Betriebssystems", die für alle CA Enterprise Log Manager-Server gilt, wenn ein neues Betriebssystem-Update heruntergeladen und installiert wird:

   - Übernehmen Sie die Standardeinstellung ("Nein"), um festzulegen, dass der CA Enterprise Log Manager-Server nicht automatisch neu gestartet wird, falls die Binär-Updates die Installation von Betriebssystem-Patches beinhalten, bei denen der Server zur Vervollständigung des Updates neu gestartet werden muss. Bei der Einstellung "Nein" werden die Benutzer durch ein selbstüberwachendes Ereignis darauf hingewiesen, dass das System manuell neu gestartet werden muss.
   - Legen Sie "Ja" fest, um sicherzustellen, dass der CA Enterprise Log Manager-Server nach jeder Installation eines Betriebssystem-Patches, bei dem zur Vervollständigung ein Neustart erforderlich ist, automatisch heruntergefahren und neu gestartet wird.

8. Wählen Sie unter den verfügbaren herunterzuladenden Modulen die für Ihre Betriebsumgebung geltenden Module aus. Falls Sie beispielsweise über keine CA Enterprise Log Manager-Server mit einer bestimmten Anwendung oder einem bestimmten Betriebssystem verfügen, wählen Sie das entsprechende herunterzuladende Modul nicht aus.

   Hinweis: Die verfügbare Liste wird während der Update-Runde gefüllt, die auf den Eintrag einer gültigen RSS-Feed-URL folgt. Wann dies erfolgt, wird durch die festgelegte Startzeit und die angegebene Aktualisierungshäufigkeit bestimmt. Falls die RSS-Feed-URL festgelegt wurde, die Liste der herunterzuladenden Module aber nicht gefüllt wird, vergewissern Sie sich, dass die URL gültig ist. Falls sich Ihr Netzwerk hinter einer Firewall befindet, vergewissern Sie sich, dass die HTTP-Proxy-Einstellung aktiviert ist und dass die entsprechenden Einstellungen für den Online-Update-Proxy korrekt sind.

9. Wählen Sie in der Liste "Proxy(s) für automatische Software-Updates für Client" einen oder mehrere Proxy-Server aus, die von Clients mittels Round Robin auf CA Enterprise Log Manager-Software- und Betriebssystemaktualisierungen durchsucht werden sollen. In großen Unternehmen sollte diese Einstellung auf lokaler Ebene geändert werden. Stellen Sie entweder eine Liste bereit, die von den meisten Clients verwendet wird, oder eine "Superliste", die die Proxies enthält, die bei der lokalen Konfiguration ausgewählt werden können.

   Hinweis: Mit dieser Einstellung kann auch eine abgestufte Proxy-Architektur erstellt werden, bei der ein Software-Update-Proxy die ausgewählten Software-Update-Proxies kontaktiert und von dort die Updates abruft und auf die Clients lädt, anstatt den CA-Software-Update-Server direkt zu kontaktieren.

10. Wählen Sie in der Liste der verfügbaren "Proxy(s) für automatische Software-Updates für Inhaltsaktualisierungen" den Proxy-Server aus, der Nicht-Binär-Aktualisierungen an den CA Enterprise Log Manager-Benutzerspeicher übertragen soll. Es empfiehlt sich, einen zweiten Proxy-Server als Sicherungsserver auszuwählen, um sicherzustellen, dass die Aktualisierungen auch dann "ausgeliefert" werden, wenn der Server, der diese Aufgabe normalerweise ausführt, nicht verfügbar ist. Nicht-Binär-Updates beinhalten XMP-Dateien, Datenzuordnungsdateien, Integrationen, Konfigurationsaktualisierungen für CA Enterprise Log Manager-Module sowie Aktualisierungen für öffentlichen Schlüssel. In einer Offline-Umgebung können Sie den Offline-Proxy-Server auswählen, über den Aktualisierungen an den CA Enterprise Log Manager-Benutzerspeicher übertragen werden.
11. Falls sich Ihr Netzwerk hinter einer Firewall befindet und Sie mit einem HTTP-Proxy-Server arbeiten, setzen Sie die Einstellung auf "Ja" und füllen die vier zugehörigen Felder aus. Klicken Sie auf "Proxy testen", um die Konnektivität zu überprüfen. Diese Einstellungen können von Servern, die als Online-Update-Proxy konfiguriert wurden, außer Kraft gesetzt werden.
12. Klicken Sie auf "Speichern".

Weitere Informationen:

Hinweise zu automatischen Software-Updates (siehe Seite 182)
Prüfen der Notwendigkeit eines HTTP-Proxys (siehe Seite 50)
Überprüfen des Zugriffs auf den RSS-Feed für automatische Software-Updates (siehe Seite 51)
Komponenten und Ports für automatische Software-Updates (siehe Seite 48)

Hinweise zu automatischen Software-Updates

Die Updates werden von einem Proxy-/Client-Server bereitgestellt. Der Server, den Sie zuerst installieren, ist der Standard-Proxy für automatische Software-Updates. Er überprüft den CA-Software-Update-Server regelmäßig auf Updates. Spätere Installationen werden als Clients dieses Proxy-Servers konfiguriert, den sie auf Aktualisierungen prüfen.

Das Standardsystem sorgt für eine Verringerung des Netzwerkdatenverkehrs, indem die Notwendigkeit, dass jeder Server eine direkte Verbindung mit dem CA-Software-Update-Server unterhält, entfällt. Das System ist jedoch vollständig konfigurierbar. Sie können Proxy-Server nach Bedarf hinzufügen.

Der Internetdatenverkehr kann zudem durch die Erstellung von Offline-Proxy-Servern noch weiter reduziert werden. Auf diesen werden Informationen zu Aktualisierungen lokal gespeichert und auf Anforderung an Clients bereitgestellt. Unterstützen Sie Offline-Proxy-Server, indem Sie den kompletten Inhalt des Download-Pfades des Online-Proxy-Servers manuell in den Download-Pfad des Offline-Proxy-Servers kopieren. Offline-Proxy-Server müssen in Umgebungen konfiguriert werden, die CA Enterprise Log Manager-Server enthalten, die nicht auf das Internet oder einen mit dem Internet verbundenen Server zugreifen können.

Beachten Sie bei der Konfiguration des Abonnement-Service folgende Hinweise bezüglich bestimmter Einstellungen und ihrer Auswirkungen:

Standard-Proxy für automatische Software-Updates (CA-Software-Update-Proxy)

Legt den standardmäßigen Proxy-Server für den Abonnement-Service fest. Der Standard-Proxy für automatische Software-Updates muss über eine Internetverbindung verfügen. Werden keine anderen Proxys festgelegt, erhält der Server die automatischen Software-Updates vom CA-Software-Update-Server, lädt binäre Updates auf alle Clients und verteilt Inhaltsaktualisierungen. Sind andere Proxys konfiguriert, kontaktieren Clients diesen Server im Zusammenhang mit Aktualisierungen, wenn keine Update-Proxy-Liste konfiguriert wurde, oder wenn die vorhandene Liste abgearbeitet ist. Der Standardwert ist der erste in der Umgebung installierte Server. Dieser Wert ist nur als globale Einstellung verfügbar.

Proxy für automatische Software-Updates

Bestimmt, ob der lokale Server ein Proxy für automatische Software-Updates ist. Online-Proxys für automatische Software-Updates rufen über die Internetverbindung Updates vom CA-Software-Update-Server ab. Sie können so konfiguriert werden, dass sie binäre Aktualisierungen auf Clients herunterladen und Inhaltsaktualisierungen an den Verwaltungsserver verteilen. Online-Proxys eignen sich auch als Quellort beim Kopieren von Aktualisierungen auf Offline-Proxys. Wenn das Kontrollkästchen "Offline-Proxy für automatische Software-Updates" aktiviert ist, muss es deaktiviert werden. Dieser Wert ist nur als lokale Einstellung verfügbar.

Hinweis: Wenn beide Kontrollkästchen für den Proxy für automatische Software-Updates deaktiviert sind, ist der Server ein Abonnement-Client.

Offline-Update-Proxy

Bestimmt, ob der lokale Server ein Offline-Proxy für automatische Software-Updates ist. Ein Offline-Proxy für automatische Software-Updates ist ein Server, der Abonnementaktualisierungen über die Kopie eines manuellen Verzeichnisses (mittels "scp") von einem Online-Proxy für automatische Software-Updates erhält. Offline-Proxys für automatische Software-Updates können so konfiguriert werden, dass sie binäre Aktualisierungen auf Clients herunterladen. Offline-Proxys für automatische Software-Updates benötigen keinen Internetzugang. Wenn das Kontrollkästchen "Proxy für automatische Software-Updates" aktiviert ist, muss es deaktiviert werden. Dieser Wert ist nur als lokale Einstellung verfügbar.

Hinweis: Wenn beide Kontrollkästchen für den Proxy für automatische Software-Updates deaktiviert sind, ist der Server ein Software-Update-Client.

Startzeit der Aktualisierung

Gilt nur, wenn die Aktualisierungshäufigkeit mindestens 24 beträgt.

Legt die Uhrzeit in Stunden fest, zu der die erste Prüfung auf Updates beginnt. Es gilt die Ortszeit des Servers. Die Uhrzeit wird im 24-Stunden-Format angegeben. Der Wert gilt für die erste Prüfung auf Updates. Die Aktualisierungshäufigkeit bestimmt die Zeitplanung für alle nachfolgenden Prüfungen auf Updates. Diese Einstellung gilt nur für den Proxy-Service für automatische Software-Updates.

Obergrenzen: 0-23, wobei 0 für Mitternacht und 23 für 23 Uhr steht.

Aktualisierungshäufigkeit

Bestimmt die Häufigkeit in Stunden, mit welcher der Online-Proxy den CA-Software-Update-Server und der Abonnement-Client den Proxy kontaktiert. Diese Einstellung gilt nur für den Proxy-Service für automatische Software-Updates.

Beispiels: 0,5 bedeutet alle 30 Minuten, 48 jeden zweiten Tag.

Jetzt aktualisieren

Klicken Sie auf diese Schaltfläche, um sofort einen bedarfsgesteuerten Update-Zyklus für den ausgewählten Server zu starten. Sie können immer nur jeweils für einen Server ein Update bei Bedarf durchführen. Aktualisieren Sie den Proxy-Server für automatische Software-Updates, bevor Sie einen Software-Update-Client aktualisieren.

RSS-Feed-URL

Bestimmt die URL des CA-Software-Update-Servers. Über diese URL greifen Online-Proxys für automatische Software-Updates auf den CA-Software-Update-Server zu und laden Updates herunter. Dieser Wert ist nur als globale Einstellung verfügbar.

HTTP-Proxy-Server

Bestimmt, ob dieser Server den CA-Software-Update-Server bezüglich Updates über einen HTTP-Proxy und nicht direkt kontaktiert.

Zu verwendende Proxy-Adresse

Gibt die vollständige IP-Adresse des HTTP-Proxys an.

Port

Gibt die Portnummer an, über welche die Verbindung zum HTTP-Proxy erfolgt.

HTTP-Proxy-Benutzer-ID

Gibt die Benutzer-ID an, über welche die Verbindung zum HTTP-Proxy erfolgt.

HTTP-Proxy-Kennwort

Gibt das Kennwort an, über das die Verbindung zum HTTP-Proxy erfolgt.

Öffentlicher Schlüssel

Legt den Schlüssel fest, mit dem die Signatur für Updates getestet und überprüft wird. Aktualisieren Sie diesen Wert nie manuell. Wenn ein Paar aus einem öffentlichen und einem privaten Schlüssel aktualisiert wird, lädt der Proxy die Aktualisierung für den Wert des öffentlichen Schlüssels herunter und aktualisiert den öffentlichen Schlüssel. Dieser Wert ist nur als globale Einstellung verfügbar.

Aktualisierungen bereinigen, die älter sind als

Bestimmt, wie viele Tage Aktualisierungspakete vom Proxy-Server aufbewahrt werden. Dieser Wert ist nur als globale Einstellung verfügbar.

Automatischer Neustart nach Aktualisierung des Betriebssystems

Legt fest, ob CA Enterprise Log Manager nach einer Aktualisierung des Betriebssystems automatisch neu gestartet wird. Dieser Wert ist nur als globale Einstellung verfügbar.

Herunterzuladende Module

Hiermit können Sie auswählen, welche Module für die Betriebsumgebung gelten. Anhand der für die Proxys ausgewählten Module werden die Module bestimmt, die der CA-Software-Update-Server im Rahmen der Updates herunterlädt. Die für die Clients ausgewählten Module dienen der Aktualisierung der auf dem Client installierten jeweiligen Module. Es ist möglich, ein Modul für einen Client herunterzuladen, das nicht für den zugehörigen Proxy ausgewählt ist. Das Modul wird dann vom Proxy für den Client abgerufen, nicht aber auf dem Proxy installiert.

Hinweis: Wenn das Feld nicht ausgefüllt ist, legen Sie "RSS-Feed-URL" fest. Mit dieser Einstellung kann das System den RSS-Feed lesen und bei der nächsten Aktualisierung die Liste der Module anzeigen, die heruntergeladen werden können.

Software-Update-Proxies für den Client

Hiermit können Sie bestimmen, welche Proxys hinsichtlich Produkt- und Betriebssystemaktualisierungen von allen Clients oder dem ausgewählten Client kontaktiert werden. Die Reihenfolge, in der der Client eine Verbindung zu den Proxys herstellt, kann mit den Pfeilschaltflächen geändert werden. Sobald ein Proxy erreicht wird, werden die Updates heruntergeladen. Steht keiner der konfigurierten Proxys zur Verfügung, kontaktiert der Client den standardmäßigen Proxy für automatische Software-Updates.

Proxy-Server für automatische Inhaltsaktualisierungen

Hiermit können Sie bestimmen, mit welchen Proxys Inhaltsaktualisierungen an den Benutzerspeicher verteilt werden. Zur Auswahl stehen Offline- und Online-Proxys. Dieser Wert ist nur als globale Einstellung verfügbar.

Hinweis: Zwecks Redundanz empfiehlt es sich, mehr als einen Proxy auszuwählen.

Konfigurieren von CA Enterprise Log Manager-Servern für automatische Software-Updates

Unter dem Modul für automatische Software-Updates sind ein oder mehrere CA Enterprise Log Manager-Server aufgeführt. Jeder Server erbt die globalen Einstellungen für automatische Software-Updates. Zunächst sind alle Einstellungen deaktiviert. Um eine Einstellung außer Kraft zu setzen, klicken Sie auf die Umschaltschaltfläche für die globale/lokale Konfiguration und bearbeiten das entsprechende Feld.

Jeder aufgeführte Server muss auf eine der folgenden Weisen konfiguriert werden:

- Software-Update-Proxy (online)
- Offline-Update-Proxy
- Software-Update-Client

Online- und Offline-Update-Proxies installieren Updates selbständig und fungieren als ihr eigener Client. Alle CA Enterprise Log Manager-Server, die nicht als Proxy für automatische Software-Updates (Software-Update-Proxy) fungieren, müssen als Client konfiguriert werden.

Der CA-Software-Update-Proxy ist eine besondere Form von Update-Proxy. Der zuerst installierte CA Enterprise Log Manager-Server registriert sich selbst beim CA Enterprise Log Manager-Benutzerspeicher als CA-Software-Update-Proxy. Diese Einstellung kann allerdings auf globaler Ebene geändert werden. In einer Online-Umgebung laden alle Clients Software-Updates vom CA-Software-Update-Proxy herunter, falls keine weiteren Proxies konfiguriert bzw. verfügbar sind.

Weitere Informationen

Beispiel: Konfiguration für automatische Software-Updates mit sechs Servern (siehe Seite 59)
Konfigurieren eines Online-Proxy-Servers für automatische Software-Updates (Online-Update-Proxys) (siehe Seite 187)
Konfigurieren eines Offline-Proxy-Servers für automatische Software-Updates (Offline-Update-Proxys) (siehe Seite 189)

Konfigurieren eines Online-Proxy-Servers für automatische Software-Updates (Online-Update-Proxys)

Sie können den Standardserver als einzigen Online-Update-Server verwenden. In diesem Fall laden alle anderen CA Enterprise Log Manager-Server in Konkurrenz zueinander Software-Updates von diesem einen Server herunter. Diese Konfiguration eignet sich für kleine Installationen, bei denen keine weiteren Online-Update-Proxies notwendig sind.

Bei großen Installationen sollten Sie mehrere Server konfigurieren. Wenn Sie mehrere Server als Online-Update-Proxies in einer Online-Umgebung einrichten, können Sie festlegen, welche Proxy-Server von welchen Clients abgefragt werden. Wenn ein Client mehrere Server mit der Round-Robin-Methode kontaktieren kann, steigt die Wahrscheinlichkeit, dass Software-Updates ohne große Verzögerung heruntergeladen werden.

Es wird der folgende vorkonfigurierte Download-Pfad verwendet:
.../opt/CA/LogManager/data/subscription

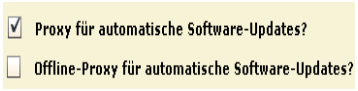
Proxy-Server für automatische Software-Updates können nur von Administratoren konfiguriert werden.

So konfigurieren Sie einen Online-Update-Proxy:

1. Klicken Sie auf die Registerkarte "Verwaltung", klicken Sie auf "Services", erweitern Sie das Modul "Automatisches Software-Update", und wählen Sie den zu konfigurierenden Server aus.

   Die Service-Konfiguration für das Software-Update-Modul wird für den ausgewählten CA Enterprise Log Manager-Server angezeigt.

2. Aktivieren Sie die Option "Proxy für automatische Software-Updates?", und lassen Sie die Offline-Option deaktiviert.

3. Falls Sie eine globale Einstellung außer Kraft setzen möchten, klicken Sie auf die Schaltfläche zum Umschalten zwischen globaler/lokaler Konfiguration, um zur lokalen Servicekonfiguration für das ausgewählte Feld zu gelangen, und nehmen dann die gewünschten Änderungen vor.

   Hinweis: Falls Sie erneut auf die Umschaltschaltfläche klicken, um das Feld zu sperren und die globale Einstellung zu verwenden, wird der Wert beim nächsten Aktualisierungsintervall (wie in der globalen Konfiguration definiert) auf den globalen Wert gesetzt.

4. Es empfiehlt sich, die globalen Einstellungen für die "Startzeit der Aktualisierung" und die "Aktualisierungshäufigkeit" zu übernehmen.

5. Falls dieser Server Software-Updates über einen HTTP-Proxy-Server herunterladen soll, der nicht dem vererbten Server entspricht, wechseln Sie zur lokalen Konfiguration und bearbeiten die fünf Felder für die Einrichtung des HTTP-Proxy-Servers.

6. Falls die Module, die für die CA Enterprise Log Manager-Produkt- bzw. -Betriebssystemaktualisierungen heruntergeladen werden müssen, nicht den vererbten Einstellungen entsprechen, wechseln Sie zur lokalen Konfiguration und nehmen die erforderlichen Änderungen vor.

7. Klicken Sie auf "Speichern".

Weitere Informationen

Hinweise zu automatischen Software-Updates (siehe Seite 182)

Konfigurieren eines Offline-Proxy-Servers für automatische Software-Updates (Offline-Update-Proxys)

Falls bestimmte CA Enterprise Log Manager-Server keine Verbindung zum Internet haben, müssen Sie mindestens einen CA Enterprise Log Manager-Server als Offline-Update-Proxy einrichten, von dem andere Offline-Client-Server Software-Updates herunterladen können.

Hierfür muss ein Administrator die Software-Updates von einem Online-Proxy auf die Offline-Proxies kopieren. Es wird der folgende vorkonfigurierte Download-Pfad verwendet: .../opt/CA/LogManager/data/subscription

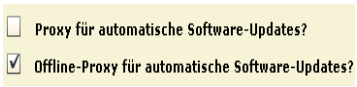
Proxy-Server für automatische Software-Updates können nur von Administratoren konfiguriert werden.

So konfigurieren Sie einen Offline-Update-Proxy:

1. Klicken Sie auf die Registerkarte "Verwaltung", klicken Sie auf "Services", erweitern Sie das Modul "Automatisches Software-Update", und wählen Sie den zu konfigurierenden Server aus.

   Die Service-Konfiguration für das Software-Update-Modul wird für den ausgewählten CA Enterprise Log Manager-Server angezeigt.

2. Aktivieren Sie die Option "Offline-Proxy für automatische Software-Updates?".

3. Klicken Sie auf "Speichern".

   Sie können diesen Offline-Update-Proxy jetzt wie folgt konfigurieren:

   - Fügen Sie ihn zur globalen Einstellung für "Proxy(s) für automatische Software-Updates für Inhaltsaktualisierungen" hinzu.
   - Fügen Sie ihn zur globalen Einstellung und/oder einer lokalen Clienteinstellung für "Proxy(s) für automatische Software-Updates für Client" hinzu.

Weitere Informationen

Prüfen der Notwendigkeit eines Offline-Proxys für automatische Software-Updates (Offline-Update-Proxys) (siehe Seite 52)

Konfigurieren eines Software-Update-Clients

Standardmäßig werden alle CA Enterprise Log Manager-Server, die nicht als Proxy für automatische Software-Updates (Software-Update-Proxy) fungieren, als Client konfiguriert. Sie müssen nur dann Software-Update-Clients konfigurieren, wenn Sie die ausgewählte, global festgelegte Proxy-Liste außer Kraft setzen möchten.

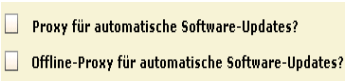
Ein Client für automatische Software-Updates ist ein CA Enterprise Log Manager-Server, der Inhaltsaktualisierungen von einem anderen CA Enterprise Log Manager-Server erhält, der als Proxy-Server für automatische Software-Updates bezeichnet wird. Clients für automatische Software-Updates fragen den konfigurierten Proxy-Server in regelmäßigen Abständen ab und rufen neue Aktualisierungen bei Verfügbarkeit ab. Nach dem Abrufen der Aktualisierungen installiert der Client die heruntergeladenen Komponenten.

So konfigurieren Sie einen Software-Update-Client:

1. Klicken Sie auf die Registerkarte "Verwaltung", klicken Sie auf "Services", erweitern Sie das Modul "Automatisches Software-Update", und wählen Sie den zu konfigurierenden Server aus.

   Die Service-Konfiguration für das Software-Update-Modul wird für den ausgewählten CA Enterprise Log Manager-Server angezeigt.

2. Machen Sie den ausgewählten Server zum Client, indem Sie die beiden Kontrollkästchen für Software-Update-Proxies deaktivieren.

3. Klicken Sie auf die Umschaltschaltfläche für die globale/lokale Konfiguration, um zur lokalen Servicekonfiguration der Option "Proxy(s) für automatische Software-Updates für Client" zu gelangen, und wählen Sie die Software-Update-Proxies aus, die von diesem Client mittels Round-Robin kontaktiert werden sollen, um Produkt- und Betriebssystemaktualisierungen abzurufen.

4. Falls die Module, die für die Produkt- bzw. Betriebssystemaktualisierungen heruntergeladen werden müssen, nicht den vererbten Einstellungen entsprechen, wechseln Sie zur lokalen Konfiguration und nehmen die erforderlichen Änderungen vor. Als Client können die Module heruntergeladen werden, die nicht vom Proxy ausgewählt wurden.

5. Klicken Sie auf "Speichern".

Weitere Informationen:

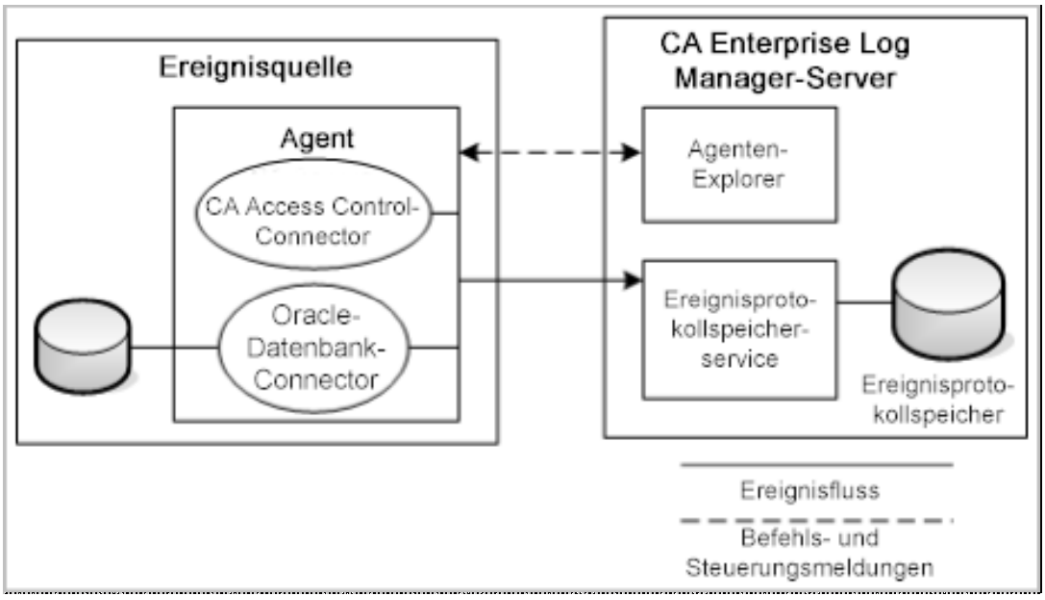
Prüfen der Notwendigkeit einer Proxy-Liste (siehe Seite 58)
Hinweise zu automatischen Software-Updates (siehe Seite 182)

Kapitel 6: Konfigurieren der Ereigniserfassung

Dieses Kapitel enthält folgende Themen:

Installieren von Agenten

CA Enterprise Log Manager-Agenten, bei denen es gesonderte Installationen für bestimmte Plattformen gibt, stellen die Transportschicht dar, über die Ereignisse von Ereignisquellen in den Ereignisprotokollspeicher des CA Enterprise Log Manager-Servers geleitet werden. Agenten verwenden Connectors, um Ereignisprotokolle aus verschiedenen Ereignisquellen zu erfassen. In der folgenden Abbildung ist die Interaktion zwischen Agenten und dem CA Enterprise Log Manager-Server dargestellt:



Nachdem Sie einen Agenten auf einer Ereignisquelle installiert haben, können Sie einen oder mehrere Connectors konfigurieren, die Ereignisse aus Ereignisquellen wie etwa Geräten, Anwendungen, Betriebssystemen und Datenbanken erfassen. Zu den Beispielen im Diagramm gehören Connectors für CA Access Control und eine Oracle-Datenbank. In der Regel wird nur ein Agent pro Hostserver oder Ereignisquelle installiert, Sie können allerdings mehrere Connector-Arten auf diesem Agenten konfigurieren. Mit dem zum CA Enterprise Log Manager-Server gehörigen Agenten-Explorer können Sie Agenten steuern und Connectors auf einem Agenten konfigurieren und kontrollieren. Der Agenten-Explorer bietet Ihnen zudem die Möglichkeit, Agentengruppen zu erstellen, mit denen sich Agenten einfacher verwalten und steuern lassen.

Die Konfiguration eines Connectors basiert entweder auf einer Integration oder einem Listener. Hierbei handelt es sich um Vorlagen, die Dateien für den Datenzugriff, die Nachrichtenanalyse und die Datenzuordnung enthalten können. CA Enterprise Log Manager stellt verschiedene vorgefertigte Integrationen für gängige Ereignisquellen bereit.

Weitere Informationen und Vorgehensweisen zum Installieren von Agenten finden Sie im *CA Enterprise Log Manager-Agent-Installationshandbuch*.

Weitere Informationen

Anzeigen und Steuern des Agenten- bzw. Connector-Status (siehe Seite 209)

Verwenden des Agenten-Explorers

Nachdem Sie einen CA Enterprise Log Manager-Server installiert haben, wird sofort ein Standardagent im Agenten-Explorer aufgelistet. Dieser Agent wird mit dem CA Enterprise Log Manager-Server installiert und für die direkte Syslog-Ereigniserfassung verwendet.

Der Agenten-Explorer erfasst und verzeichnet die im Netzwerk installierten Agenten und stellt einen zentralen Ort für die Konfiguration, Verwendung und Steuerung von Agenten und Connectors bereit. Agenten werden bei dem CA Enterprise Log Manager-Server registriert, den Sie beim ersten Start der Agenten angeben. Nach der Registrierung wird der Agentenname im Agenten-Explorer angezeigt, und Sie können einen Connector einrichten, um mit der Ereignisprotokollerfassung zu beginnen. Connectors sammeln Ereignisprotokolle und senden sie an den CA Enterprise Log Manager-Server. Ein Agent kann mehrere Connectors kontrollieren.

Die Installation, Konfiguration und Steuerung von Agenten und Connectors mit dem Agenten-Explorer umfasst folgende Schritte:

1. Herunterladen der Binärdateien des Agenten
2. Erstellen einer oder mehrerer Agentengruppen (optional)
3. Erstellen und Konfigurieren eines Connectors, und Erstellen und Anwenden von Unterdrückungs- und Zusammenfassungsregeln
4. Anzeigen des Agenten- bzw. Connector-Status

Weitere Informationen zum Erstellen von und Arbeiten mit Agentengruppen und Connectors sowie zum Anwenden von Unterdrückungsregeln für Agenten finden Sie im *CA Enterprise Log Manager-Administrationshandbuch*.

Weitere Informationen

Wissenswertes über Agenten (siehe Seite 63)
Wissenswertes über Agentengruppen (siehe Seite 64)
Wissenswertes über Connectors (siehe Seite 66)
Wissenswertes über Protokollsensoren (siehe Seite 66)
Auswirkungen von Unterdrückungsregeln (siehe Seite 68)

Konfigurieren des Standardagenten

Die CA Enterprise Log Manager-Installation erstellt auf dem CA Enterprise Log Manager-Server einen Standardagenten mit zwei betriebsbereiten Connectors, einem syslog_Connector und einem Linux_local Connector. Der Syslog-Connector erfasst die an den CA Enterprise Log Manager-Server gesendeten Syslog-Ereignisse. Mit dem Linux_local-Connector werden "root"-Ereignisse vom physischen CA Enterprise Log Manager-Server oder von einer Syslog-Datei erfasst.

Konfigurieren Sie in einer einfachen Umgebung mit zwei Servern einen oder mehrere Syslog-Connectors auf dem (agentenlosen) Quellserver für Protokolldateien für den Empfang von Ereignissen.

Die Verwendung des Standardagenten umfasst folgende Schritte:

1. (Optional) Überprüfen Sie die Syslog-Integrationen und -Listener.
2. Erstellen Sie einen Syslog-Connector.
3. Überprüfen Sie, ob der CA Enterprise Log Manager-Server Syslog-Ereignisse empfängt.

Überprüfen von Syslog-Integrationen und -Listenern

Sie können die standardmäßigen Syslog-Integrationen und -Listener überprüfen, bevor Sie einen Connector erstellen. Listener sind im Wesentlichen Vorlagen für Syslog-Connectors, die spezifische, vorgefertigte und mit dem CA Enterprise Log Manager-Server bereitgestellte Syslog-Integrationen verwenden.

So überprüfen Sie Syslog-Integrationen:

1. Melden Sie sich bei CA Enterprise Log Manager an, und rufen Sie die Registerkarte "Verwaltung" auf.
2. Erweitern Sie im Navigationsfenster auf der linken Seite den Knoten "Ereignisverfeinerungs-Bibliothek".
3. Erweitern Sie den Knoten "Integrationen" und den Knoten "Automatisches Software-Update".
4. Wählen Sie eine Integration aus, deren Name mit "..._Syslog" endet.

   Die Details zur Integration werden im Fenster auf der rechten Seite angezeigt. Sie können die von der Integration verwendete Nachrichtenanalyse- und Datenzuordnungsdatei sowie andere Informationen wie etwa die Version und die Liste der Unterdrückungsregeln überprüfen.

So überprüfen Sie einen Syslog-Listener:

1. Erweitern Sie den Knoten "Listener" und den Knoten "Automatisches Software-Update".
2. Wählen Sie den Syslog-Listener aus.

   Die Details zum Standardlistener werden im Fenster auf der rechten Seite angezeigt. Sie können Informationen wie etwa die Versionen, eine Liste der Unterdrückungsregeln, die abgehörten Standardports, eine Liste der vertrauenswürdigen Hosts und die Zeitzone des Listeners überprüfen.

Erstellen eines Syslog-Connectors für den Standardagenten

Erstellen Sie einen Syslog-Connector für den Empfang von Syslog-Ereignissen über den Standardagenten auf dem CA Enterprise Log Manager-Server.

So erstellen Sie einen Syslog-Connector für den Standardagenten:

1. Melden Sie sich bei CA Enterprise Log Manager an, und rufen Sie die Registerkarte "Verwaltung" auf.
2. Erweitern Sie den Agenten-Explorer und eine Agentengruppe.

   Der Standardagent wird automatisch in der Standardagentengruppe installiert. Sie können diesen Agenten in eine andere Gruppe verschieben.

3. Wählen Sie den Agentennamen aus.

   Der Standardagent trägt den Namen, den Sie dem CA Enterprise Log Manager-Server während der Installation zugewiesen haben.

4. Klicken Sie auf "Neuen Connector erstellen", um den Connector-Assistenten zu öffnen.

5. Klicken Sie auf das Optionsfeld "Listener", und geben Sie einen Namen für diesen Connector an.

6. Auf der zweiten Seite des Assistenten können Sie bei Bedarf Unterdrückungsregeln übernehmen oder erstellen.

7. Wählen Sie in der Liste "Verfügbar" eine oder mehrere Ziel-Syslog-Integrationen für diesen Connector aus, und verschieben Sie sie in die Liste "Ausgewählt".

8. Legen Sie Werte für den UDP- und TCP-Port fest, falls Sie nicht die Standardports verwenden, und stellen Sie eine Liste der vertrauenswürdigen Hosts bereit, sofern diese in Ihrer Implementierung verwendet werden.

   Hinweis: Wenn ein CA Enterprise Log Manager-Agent nicht als Root ausgeführt wird, kann der Agent keinen Port unter 1024 öffnen. Der Standard-Syslog-Connector verwendet deshalb UDP-Port 40514. Die Installation wendet eine Firewall-Regel zum CA Enterprise Log Manager-Server an, um den Datenverkehr von Port 514 über 40514 umzuleiten.

9. Wählen Sie eine Zeitzone aus.

10. Klicken Sie auf "Speichern und schließen", um den Connector fertig zu stellen.

    Der Connector erfasst nun auf den angegebenen Ports die Syslog-Ereignisse, die den gewählten Integrationen entsprechen.

Überprüfen des Empfangs von Syslog-Ereignissen durch CA Enterprise Log Manager

Sie können mit den folgenden Schritten überprüfen, ob der Connector auf dem Standardagenten Syslog-Ereignisse erfasst.

So überprüfen Sie den Eingang von Syslog-Ereignissen:

1. Melden Sie sich bei CA Enterprise Log Manager an, und rufen Sie die Registerkarte "Abfragen und Berichte" auf.

2. Wählen Sie die System-Abfragekennung aus, und öffnen Sie die Abfrage "Alle Ereignisse des Systems - Details".

   Sofern der Connector richtig konfiguriert wurde und von der Ereignisquelle aktiv Ereignisse gesendet werden, werden die Ereignisse für den Standardagenten aufgelistet.

Beispiel: Aktivieren der direkten Erfassung mit "ODBCLogSensor"

Sie können die direkte Erfassung von Ereignissen aktivieren, die von spezifischen Datenbanken und CA-Produkten mit dem Sensor "ODBCLogSensor" generiert werden. Hierzu erstellen Sie einen Connector auf dem Standardagenten, der auf einer Integration basiert, in der "ODBCLogSensor" verwendet wird. Dieser Sensor wird in vielen Integrationen verwendet, beispielsweise in "CA_Federation_Manager", "CAIdentityManager", "Oracle10g", "Oracle9i" und "MS_SQL_Server_2005".

Im Folgenden finden Sie eine Liste mit einem Auszug von Produkten, die Ereignisse generieren, die direkt vom Standardagenten auf einem CA Enterprise Log Manager-Server erfasst werden können. Für jedes Produkt wird ein eindeutiger Connector verwendet. Alle Connectors wiederum verwenden den Sensor "ODBCLogSensor".

- CA Federation Manager
- CA SiteMinder
- CA Identity Manager
- Oracle 9i und Oracle 10g
- Microsoft SQL Server 2005 Express

Eine vollständige Liste finden Sie unter "Support Online" in der Produktintegrationsmatrix.

In diesem Beispiel wird gezeigt, wie Sie die direkte Erfassung von Ereignissen aus einer Microsoft SQL Server-Datenbank aktivieren. Der auf dem Standardagenten bereitgestellte Connector basiert auf der Integration "MS_SQL_Server_2005". In diesem Beispiel befindet sich die SQL Server-Datenbank auf einem ODBC-Server. Der für den CA Enterprise Log Manager-Agenten bereitgestellte Connector erfasst Ereignisse aus der Tabelle "MSSQL_TRACE". Im Rahmen der Aktivierung der Erfassung von Ereignissen aus einer Microsoft SQL Server-Datenbank legen Sie fest, dass ausgewählte Ereignisse an diese Ablaufverfolgungstabelle weitergeleitet werden. Die expliziten Anweisungen hierzu finden Sie im *CA Connector-Handbuch für Microsoft SQL Server*.

So konfigurieren Sie die Microsoft SQL Server-Ereignisquelle:

1. Klicken Sie auf die Registerkarte "Verwaltung".
2. Blenden Sie nacheinander "Ereignisverfeinerungs-Bibliothek", "Integrationen" und "Automatisches Software-Update" ein, und wählen Sie "MS_SQL_Server_2005" aus.

   Im Fensterbereich "Integrationsdetails anzeigen" wird der Name des Sensors angezeigt, "ODBCLogSensor". Die unterstützten Plattformen sind Windows und Linux.
3. Klicken Sie im Fensterbereich "Integrationsdetails anzeigen" auf den Link "Hilfe".

   Das Connector-Handbuch für Microsoft SQL Server wird angezeigt.
4. Sehen Sie sich die Abschnitte zu den Voraussetzungen und zur Konfiguration von Microsoft SQL Server und die darin enthaltenen Richtlinien an.

So konfigurieren Sie die Ereignisquelle und überprüfen die Protokollierung:

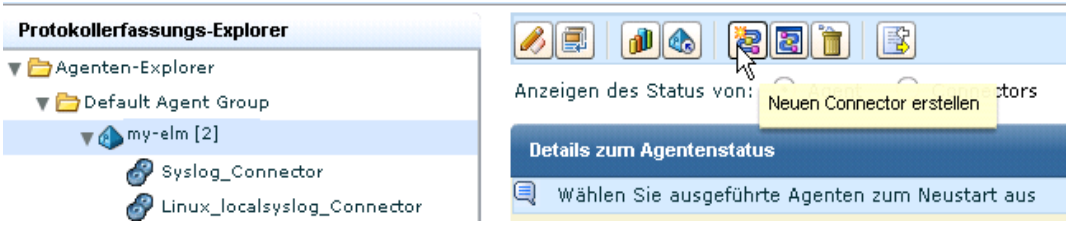
1. Erfassen Sie folgende Details: IP-Adresse des ODBC-Servers, Datenbankname, Administratorbenutzername und -kennwort, die für die Anmeldung beim Server erforderlich sind, sowie für die SQL Server-Authentifizierung verwendete Anmeldeinformationen des Benutzers mit eingeschränkten Berechtigungen. (Dies ist der Benutzer, für den nur schreibgeschützter Zugriff auf die Ablaufverfolgungstabelle definiert wurde.)
2. Melden Sie sich mit dem Administratorbenutzernamen und -kennwort beim ODBC-Server an.
3. Stellen Sie anhand der Angaben im *Connector-Handbuch für Microsoft SQL Server* Konnektivität über TCP/IP sicher.
4. Konfigurieren Sie den SQL-Server, und vergewissern Sie sich, dass Ereignisse wie im *Connector-Handbuch für Microsoft SQL Server* angegeben an die Ablaufverfolgungstabelle weitergeleitet werden.

   Hinweis: Notieren Sie sich den Namen der Datenbank, in der Sie die Ablaufverfolgungstabelle erstellen. Sie müssen den Datenbanknamen in der Verbindungszeichenfolge angeben. Beispiel: "master".

So erstellen Sie einen Connector auf dem Standardagenten, um Ereignisse abzurufen, die von einer SQL Server-Datenbank auf einem ODBC-Server generiert werden:

1. Klicken Sie auf die Registerkarte "Verwaltung" und auf die Unter-Registerkarte "Protokollerfassung".
2. Blenden Sie den Agenten-Explorer und anschließend die Agentengruppe ein, die den CA Enterprise Log Manager-Standardagenten enthält.
3. Wählen Sie einen Standardagenten aus, das heißt, einen Agenten mit dem Namen eines CA Enterprise Log Manager-Servers.

   Der Standardagent kann über weitere Connectors verfügen, die für ihn bereitgestellt wurden.
4. Klicken Sie auf "Neuen Connector erstellen".



Der Assistent "Erstellung eines neuen Connectors" wird angezeigt. Der Schritt "Connector-Details" ist ausgewählt.

5. Wählen Sie aus der Dropdown-Liste "Version" die Integration "MS_SQL_Server_2005" aus.

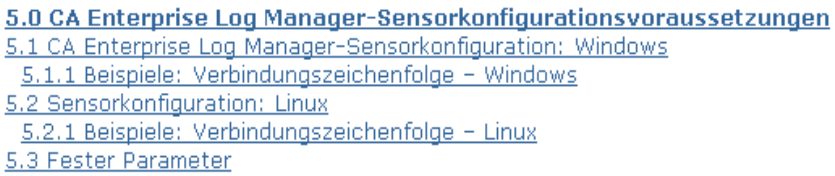
   Hierdurch wird das Feld "Connector-Name" mit der Zeichenfolge "MS_SQL_Server_2005" gefüllt.
6. (Optional) Ersetzen Sie den Standardnamen durch einen Namen, anhand dessen Sie den Connector gut identifizieren können. Falls Sie mehrere SQL Server-Datenbanken mit demselben Agenten überwachen, sollten Sie einen eindeutigen Namen angeben.

7. (Optional) Klicken Sie auf den Schritt "Unterdrückungsregeln anwenden", und wählen Sie Regeln aus, die den unterstützten Ereignissen zugeordnet sind.

   Wählen Sie beispielsweise "MSSQL_2005_Authorization 12.0.44.12" aus.

8. Klicken Sie auf den Schritt "Connector-Konfiguration" und dann auf den Link "Hilfe".

   In den Anweisungen sind die Anforderungen für die CA Enterprise Log Manager-Sensorkonfiguration für Windows und Linux angegeben.

9. Lesen Sie sich die Schritte für Linux, die Plattform des Standardagenten, durch, und konfigurieren Sie das Feld "Verbindungszeichenfolge" und die anderen Felder wie angegeben.

   a. Geben Sie die Verbindungszeichenfolge wie unter "Sensorkonfiguration" für Linux angegeben an, wobei es sich bei der Adresse um den Hostnamen oder die IP-Adresse der Ereignisquelle und bei der Datenbank um die SQL Server-Datenbank handelt, in der sich MSSQLSERVER_TRACE befindet.

      `DSN=SQLServer Wire Protocol;Address=`*`IPaddress`*`,`*`port`*`;Database=`*`databasename`*

   b. Geben Sie den Namen des Benutzers mit Zugriffsrechten zum schreibgeschützten Erfassen von Ereignissen an. Damit dieser Benutzer schreibgeschützten Zugriff erhält, müssen ihm die Rollen "db_datareader" und "public" zugewiesen werden.

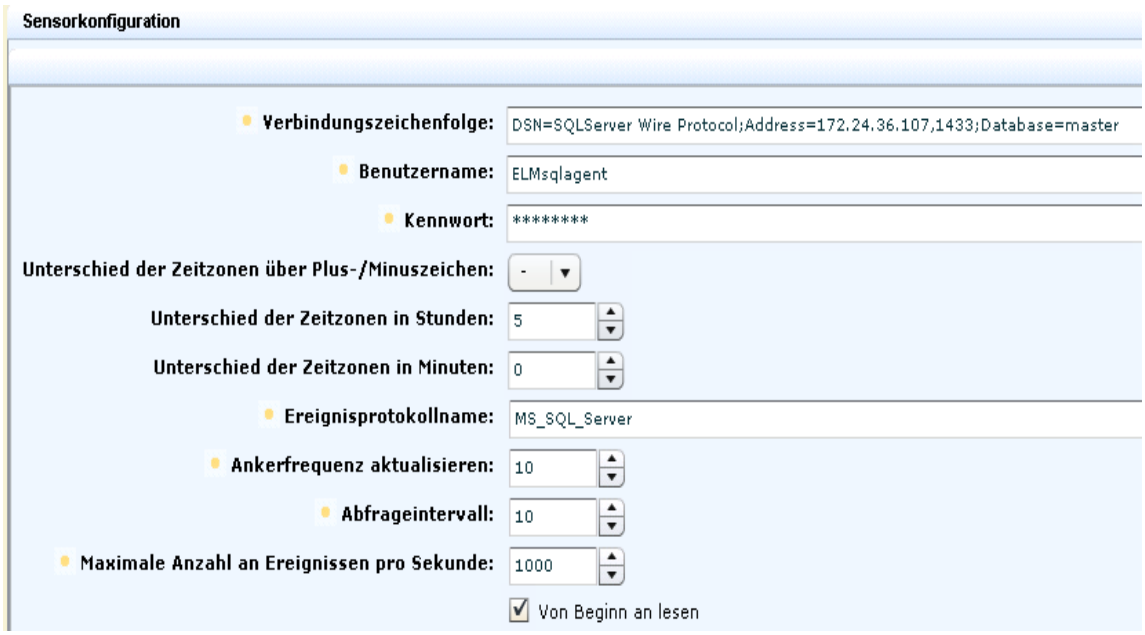
   c. Geben Sie das Kennwort für den angegebenen Benutzernamen ein.

   d. Geben Sie die Zeitzone der Datenbank in Form der GMT-Abweichung an.

      Hinweis: Auf Windows-Servern werden diese Informationen im Fenster "Eigenschaften von Datum und Uhrzeit" auf der Registerkarte "Zeitzone" angezeigt. Öffnen Sie die Uhr in der Taskleiste.

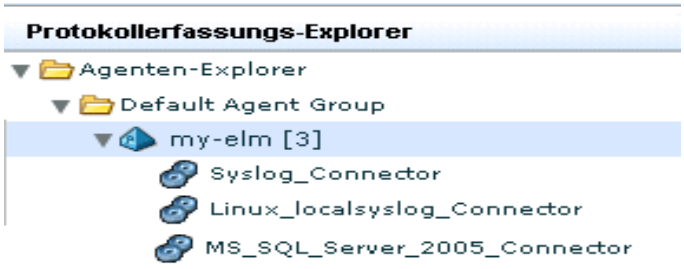
e. Aktivieren oder deaktivieren Sie das Kontrollkästchen "Von Beginn an lesen", je nachdem, ob der Protokollsensor Ereignisse vom Beginn der Datenbank an lesen soll.

Als Beispiel folgt ein Auszug des Fensters:



10. Klicken Sie auf "Speichern und schließen".

    Der neue Connector-Name wird unter dem Agenten im Agenten-Explorer angezeigt.



11. Klicken Sie auf "MS_SQL_Server_2005_Connector", um Statusdetails anzuzeigen.

    Als Anfangsstatus wird "Konfiguration ausstehend" angezeigt. Warten Sie, bis der Status "Wird ausgeführt" angezeigt wird.

Connector	Agent	Agentengruppe	Plattform	Integration	Status
MS_SQL_Server_2005_Connector	my-elm	Default Agent Group	Linux_X86_32	MS_SQL_Server_2005	Wird ausgeführt

12. Wählen Sie den Connector aus, und klicken Sie auf "Wird ausgeführt", um Details zur Ereigniserfassung anzuzeigen.

    Hinweis: Sie können auch einen Bericht ausführen, um Daten aus dieser Datenbank anzuzeigen.

So überprüfen Sie, ob der Standardagent Ereignisse aus der Zielereignisquelle erfasst:

1. Wählen Sie die Registerkarte "Abfragen und Berichte". Die Unterregisterkarte "Abfragen" wird angezeigt.
2. Erweitern Sie in der Abfrageliste den Eintrag "Eingabeaufforderungen", und wählen Sie "Connector" aus.
3. Geben Sie den Connector-Namen ein, und klicken Sie auf "Los".

   Die erfassten Ereignisse werden angezeigt. Die beiden ersten Ereignisse sind interne Ereignisse. Bei den darauf folgenden Ereignissen handelt es sich um Ereignisse, die aus der von Ihnen konfigurierten MS SQL-Ablaufverfolgungstabelle erfasst wurden.

   Hinweis: Wenn die erwarteten Ereignisse nicht angezeigt werden, klicken Sie in der Hauptsymbolleiste auf "Globale Filter und Einstellungen", und speichern Sie die Einstellung.
4. (Optional) Wählen Sie "Rohereignisse anzeigen" aus, und untersuchen Sie die Ergebniszeichenfolge für die ersten beiden Ereignisse. Die Ergebniszeichenfolge wird im Rohereignis an letzter Stelle angezeigt. Die folgenden Werte geben an, dass der Start erfolgreich verlaufen ist.
   - result_string=ODBCSource initiated successfully - MSSQL_TRACE
   - result_string=<connector name> Connector Started Successfully

Beispiel: Aktivieren der direkten Erfassung mit "WinRMLinuxLogSensor"

Sie können die direkte Erfassung der von Windows-Anwendungen oder dem Betriebssystem Windows Server 2008 generierten Ereignisse mit dem Sensor "WinRMLinuxLogSensor" aktivieren. Hierzu erstellen Sie einen Connector auf dem Standardagenten, der auf einer Integration basiert, in der "WinRMLinuxLogSensor" verwendet wird. Dieser Sensor wird in vielen Integrationen verwendet, beispielsweise in "Active_Directory_Certificate_Services", "Forefront_Security_for_Exchange_Server", "Hyper-V", "MS_OCS" und "WinRM". Unter den Microsoft Windows-Anwendungen und -Betriebsystemen, die Ereignisse generieren, kann "WinRMLinuxLogSensor" Ereignisse von denjenigen abrufen, für die die Windows-Remoteverwaltung aktiviert ist.

Im Folgenden finden Sie eine Liste mit einem Auszug von Produkten, die Ereignisse generieren, die direkt vom Standardagenten auf einem CA Enterprise Log Manager-Server erfasst werden können. Für jedes Produkt wird ein eindeutiger Connector verwendet. Alle Connectors wiederum verwenden den Sensor "WinRMLinuxLogSensor".

- Microsoft Active Directory Certificate Services
- Microsoft Forefront Security for Exchange Server
- Microsoft Forefront Security for SharePoint Server
- Microsoft Hyper-V Server 2008
- Microsoft Office Communication Server
- Microsoft Windows Server 2008

Eine vollständige Liste finden Sie unter "Support Online" in der Produktintegrationsmatrix.

In diesem Beispiel wird gezeigt, wie Sie die direkte Erfassung von Ereignissen mit einem Connector basierend auf der WinRM-Integration aktivieren. Wenn ein solcher Connector bereitgestellt wird, erfasst er Ereignisse aus einer Ereignisquelle des Betriebssystems Windows Server 2008. Die Erfassung beginnt, nachdem Sie die Ereignisquellen entsprechend den Angaben in dem dieser Integration zugeordneten Connector-Handbuch so konfiguriert haben, dass Ereignisse in der Windows-Ereignisanzeige erfasst werden und die Windows-Remoteverwaltung auf dem Server aktiviert wird.

So konfigurieren Sie die Windows Server 2008-Ereignisquelle:

1. Klicken Sie auf die Registerkarte "Verwaltung".
2. Blenden Sie nacheinander "Ereignisverfeinerungs-Bibliothek", "Integrationen" und "Automatisches Software-Update" ein, und wählen Sie "WinRM" aus.

   Im Fensterbereich "Integrationsdetails anzeigen" wird der Name des Sensors angezeigt, "WinRMLinuxLogSensor". Die unterstützten Plattformen sind Windows und Linux.
3. Klicken Sie im Fensterbereich "Integrationsdetails anzeigen" für WinRM auf den Link "Hilfe".

   Das Connector-Handbuch für Microsoft Windows Server 2008 zu WinRM wird angezeigt.

So konfigurieren Sie die Ereignisquelle und überprüfen die Protokollierung:

1. Melden Sie sich auf dem Zielhost, auf dem eine Edition von Windows Server 2008 installiert ist.
2. Befolgen Sie die Anweisungen im *CA Connector-Handbuch für Microsoft Windows Server 2008*, um sicherzustellen, dass Ereignisse in der Windows-Ereignisanzeige angezeigt werden und die Windows-Remoteverwaltung auf dem Zielserver aktiviert ist.

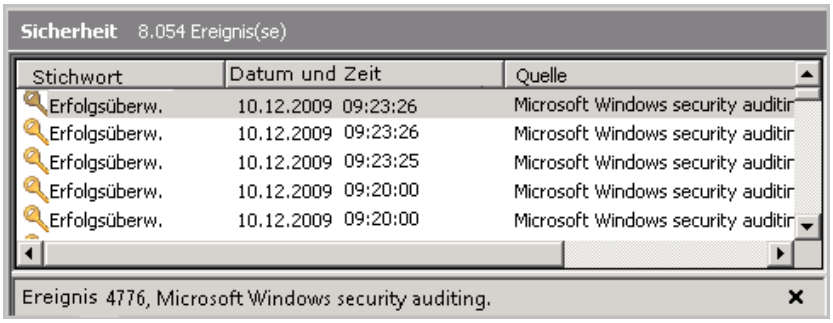
   Hinweis: Im Rahmen dieses Prozesses erstellen Sie den Benutzernamen und das Kennwort, die Sie bei der Konfiguration des Connectors eingeben müssen. Durch diese Anmeldeinformationen wird die Authentifizierung ermöglicht, die zum Herstellen von Konnektivität zwischen der Ereignisquelle und CA Enterprise Log Manager erforderlich ist.
3. Überprüfen Sie die Protokollierung.

   a. Führen Sie im Dialogfeld "Ausführen" den Befehl "eventvwr" aus.

      Die Ereignisanzeige wird geöffnet.

   b. Blenden Sie "Windows-Protokolle" ein, und klicken Sie auf "Sicherheit".

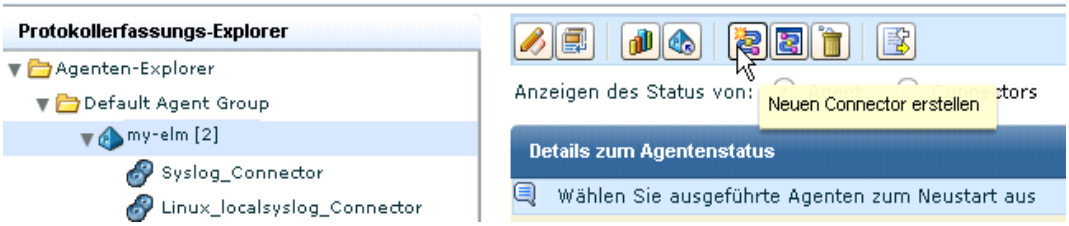
      Der daraufhin eingeblendeten Anzeige können Sie entnehmen, dass die Protokollierung durchgeführt wird. Sie sieht in etwa wie folgt aus:



So aktivieren Sie die direkte Erfassung von Ereignissen aus Windows-Ereignisquellen:

1. Klicken Sie auf die Registerkarte "Verwaltung" und auf die Unter-Registerkarte "Protokollerfassung".
2. Blenden Sie im Protokollerfassungs-Explorer den Agenten-Explorer und anschließend die Agentengruppe ein, die den CA Enterprise Log Manager-Standardagenten enthält.
3. Wählen Sie einen Standardagenten aus, das heißt, einen Agenten mit dem Namen eines CA Enterprise Log Manager-Servers.

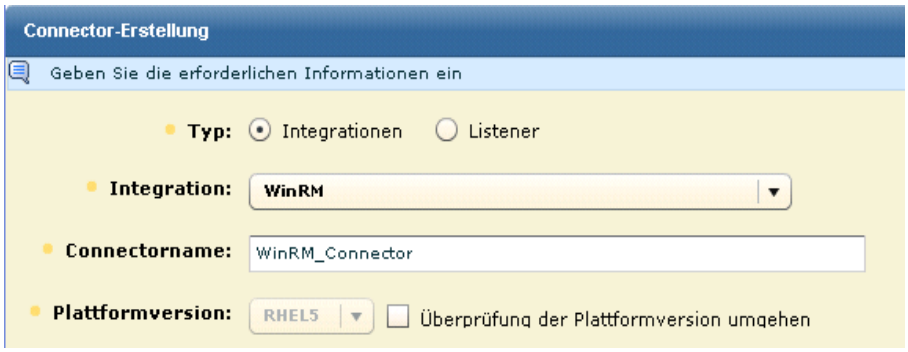
   Der Standardagent verfügt möglicherweise über weitere Connectors, die für ihn bereitgestellt wurden.
4. Klicken Sie auf "Neuen Connector erstellen".



Der Assistent "Erstellung eines neuen Connectors" wird angezeigt. Der Schritt "Connector-Details" ist ausgewählt.

5. Wählen Sie in der Dropdown-Liste "Integration" eine Integration aus, in der der Protokollsensor "WinRM" verwendet wird.

   Wählen Sie beispielsweise "WinRM" aus.



Hierdurch wird das Feld "Connector-Name" mit der Zeichenfolge "WinRM_Connector" gefüllt.

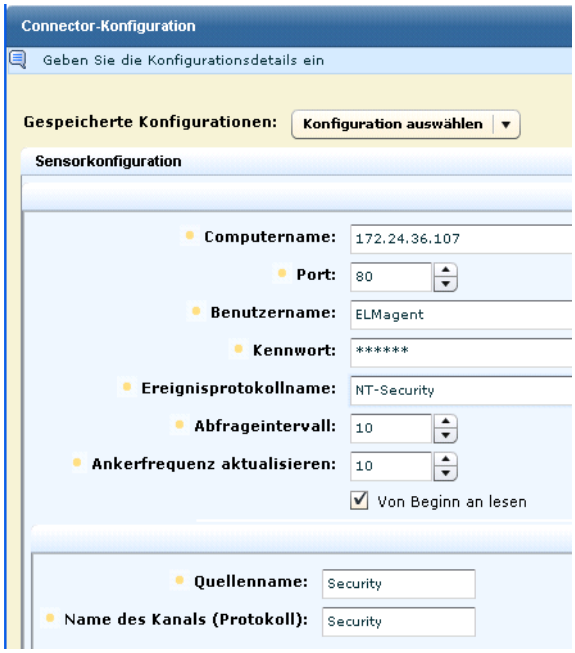
6. (Optional) Klicken Sie auf "Unterdrückungsregeln anwenden", und wählen Sie Regeln aus, die den unterstützten Ereignissen zugeordnet sind.
7. Klicken Sie auf den Schritt "Connector-Konfiguration" und dann auf den Link "Hilfe".

   In den Anweisungen finden Sie auch Angaben zur CA Enterprise Log Manager-Sensorkonfiguration für WinRM.

   5.0 Konfigurieren des CA Enterprise Log Manager-Sensors: WinRM
   5.1 Fester Parameter

8. Befolgen Sie die Anweisungen in diesem Connector-Handbuch, um den Sensor zu konfigurieren. Geben Sie statt des Hostnamens die IP-Adresse des Hosts ein, auf dem Sie die Windows-Remoteverwaltung konfiguriert haben. Die Felder "Benutzername" und "Kennwort" enthalten die Anmeldeinformationen, die Sie während der Konfiguration der Windows-Remoteverwaltung eingegeben haben.

   Beispiel:

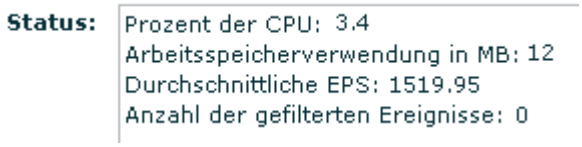


9. Klicken Sie auf "Speichern und schließen".
10. Der neue Connector-Name wird unter dem Agenten im Agenten-Explorer angezeigt.

11. Klicken Sie auf "WinRM_Connector", um die Statusdetails anzuzeigen.

    Als Anfangsstatus wird "Konfiguration ausstehend" angezeigt. Warten Sie, bis der Status "Wird ausgeführt" angezeigt wird.

12. Klicken Sie auf "Wird ausgeführt", um Übersichtsdaten anzuzeigen, beispielsweise zu den EPS-Werten (Ereignisse pro Sekunde).



So überprüfen Sie, ob der Standardagent Ereignisse aus der Zielereignisquelle erfasst:

1. Wählen Sie die Registerkarte "Abfragen und Berichte". Die Unterregisterkarte "Abfragen" wird angezeigt.
2. Erweitern Sie in der Abfrageliste den Eintrag "Eingabeaufforderungen", und wählen Sie "Connector" aus.
3. Geben Sie den Connector-Namen ein, und klicken Sie auf "Los".
4. Zeigen Sie die erfassten Ereignisse an.

Anzeigen und Steuern des Agenten- bzw. Connector-Status

Sie können den Status der Agenten bzw. Connectors in Ihrer Umgebung überwachen, Agenten neu starten und Connectors nach Bedarf starten, stoppen und neu starten.

Die Agenten bzw. Connectors können auf verschiedenen Ebenen der Ordnerstruktur im Agenten-Explorer angezeigt werden. Mit jeder Ebene wird die Anzeige entsprechend eingegrenzt:

- Auf der Ebene des Ordners "Agenten-Explorer" können Sie alle dem aktuellen CA Enterprise Log Manager-Server zugeordneten Agenten bzw. Connectors sehen.
- Auf der Ebene eines bestimmten Agentengruppenordners können Sie die dieser Agentengruppe zugewiesenen Agenten und Connectors sehen.
- Auf der Ebene eines einzelnen Agenten sehen Sie nur diesen Agenten und die ihm zugeordneten Connectors.

Sie können auf allen drei Ebenen den FIPS-Modus (FIPS oder Nicht-FIPS) für einen Agenten bestimmen.

So zeigen Sie den Agenten- bzw. Connector-Status an:

1. Klicken Sie auf die Registerkarte "Verwaltung" und anschließend auf die Unterregisterkarte "Protokollerfassung".

   Die Ordnerliste "Protokollerfassung" wird angezeigt.

2. Wählen Sie den Ordner "Agenten-Explorer" aus.

   Im Detailfenster werden Schaltflächen für die Agentenverwaltung angezeigt.

3. Klicken Sie auf "Status und Befehl": 

   Das Statusfenster wird angezeigt.

4. Wählen Sie "Agenten" oder "Connectors" aus.

   Das Fenster für die Agenten- bzw. Connector-Suche wird eingeblendet.

5. (Optional) Wählen Sie Suchkriterien für die Agenten- oder Connector-Aktualisierung aus. Falls Sie keine Suchbegriffe eingeben, werden alle verfügbaren Updates angezeigt. Sie können unter den folgenden Kriterien wählen, um die Suche einzugrenzen:
   - Agentengruppe: Gibt nur die der ausgewählten Gruppe zugewiesenen Agenten und Connectors zurück.
   - Plattform: Gibt nur die auf dem ausgewählten Betriebssystem ausgeführten Agenten und Connectors zurück.
   - Suchmuster für den Agentennamen: Gibt nur die Agenten und Connectors zurück, die das angegebene Muster enthalten
   - (Nur Connectors) Integration: Gibt nur Connectors zurück, die die gewählte Integration verwenden
6. Klicken Sie auf "Status anzeigen".

   Es wird eine Detailübersicht mit dem Status der Agenten bzw. Connectors angezeigt, die den Suchkriterien entsprechen. Beispiel:

   ```
   Summe: 10 Wird ausgeführt: 8 Ausstehend: 1 Beendet: 1 Antwortet nicht: 0
   ```
7. (Optional) Klicken Sie auf die Statusanzeige, um Detailinformationen im Statusfenster unten in der Übersicht einzublenden.

   Hinweis: Wenn Sie auf die Schaltfläche für den Bedarfsstatus eines Agenten oder Connectors klicken, wird die Statusanzeige aktualisiert.
8. (Optional) Falls Connectors angezeigt werden, wählen Sie einen Connector aus und klicken Sie auf "Neu starten", "Start" oder "Beenden". Falls Agenten angezeigt werden, wählen Sie einen Agenten aus und klicken Sie auf "Neu starten".

Kapitel 7: Erstellen von Föderationen

Dieses Kapitel enthält folgende Themen:

Abfragen und Berichte in einer föderierten Umgebung

Ein einzelner CA Enterprise Log Manager-Server gibt als Antwort auf Abfragen und zum Erstellen von Berichten Daten aus seiner internen Ereignisdatenbank zurück. Falls Sie über eine Föderation (Verbund) von CA Enterprise Log Manager-Servern verfügen, können Sie steuern, wie Ereignisinformationen in Abfragen und Berichten zurückgegeben werden, indem Sie die Beziehungen in der Föderation entsprechend konfigurieren. Ferner können Sie Abfrageergebnisse von einzelnen Servern abrufen, indem Sie die globale Einstellung "Föderierte Abfragen ausführen" deaktivieren.

Standardmäßig ist die globale Einstellung "Föderierte Abfragen ausführen" aktiviert. Hierdurch werden Abfragen von einem übergeordneten CA Enterprise Log Manager-Server an alle untergeordneten CA Enterprise Log Manager-Server gesendet. Jeder untergeordnete CA Enterprise Log Manager-Server sendet eine Abfrage an den aktiven Ereignisprotokollspeicher, den Archivkatalog und an alle ihm untergeordneten CA Enterprise Log Manager-Server. Auf jedem untergeordneten CA Enterprise Log Manager-Server wird dann ein einzelner Ergebnissatz erstellt, der an den abfragenden übergeordneten CA Enterprise Log Manager-Server gesendet wird. CA Enterprise Log Manager enthält einen integrierten Schutz gegen im Kreis verlaufende Abfragen und ermöglicht so Netzkonfigurationen.

Eine typische CA Enterprise Log Manager-Implementierung in Unternehmen weist zwischen einem und fünf Servern auf. Große Implementierungen können aus zehn und mehr Servern bestehen. Durch die Art und Weise, in der die Föderation konfiguriert ist, bestimmen Sie, wie viele Informationen für den abfragenden CA Enterprise Log Manager-Server sichtbar sind. Die einfachste Art von Abfrage geht vom primären CA Enterprise Log Manager-Server aus und gibt Informationen von allen diesem Server untergeordneten Servern zurück.

Wenn Sie von einem untergeordneten Server aus eine Abfrage an die Föderation senden, sind die Ergebnisse davon abhängig, wie die Föderation konfiguriert wurde. In einer *hierarchischen* Föderation geben alle Server, die als untergeordnete Server zu einem Server konfiguriert wurden, Ergebnisse an diesen Server zurück. In einem *Netz*verbund geben alle untereinander verbundenen Server Daten an den abfragenden Server zurück.

Hierarchischer Verbund

Hierarchische Verbunde (Verbunde werden auch als Föderationen bezeichnet) verwenden eine von oben nach unten verlaufende Pyramidenstruktur, um die Arbeitslast der Ereigniserfassung über ein weites Gebiet zu verteilen. Die Struktur ähnelt einem Organisationsdiagramm. Die Anzahl der erstellten Ebenen ist nicht vorgegeben und wird von Ihnen entsprechend Ihrer Geschäftsanforderungen gewählt.

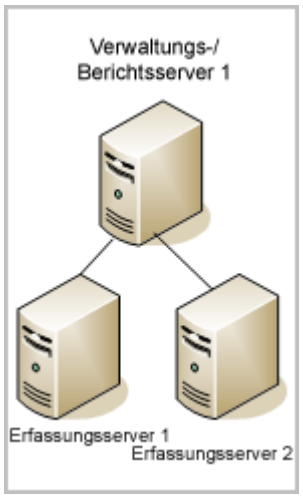
In einem hierarchischen Verbund können Sie mit jedem CA Enterprise Log Manager-Server eine Verbindung herstellen, um Berichte zu den Ereignisdaten dieses Servers und den Daten der untergeordneten Server anzuzeigen. Der Umfang der Daten, auf die Sie zugreifen können, wird durch Ihren Ausgangspunkt in der Hierarchie bestimmt. Falls Sie auf einen Server in der Mitte der Hierarchie zugreifen, können Sie nur die Daten dieses Servers und der ihm untergeordneten Server anzeigen. Je höher Sie sich im hierarchischen Verbund befinden, desto mehr Netzwerkdaten können Sie einsehen. Auf der obersten Ebene haben Sie Zugang zu allen Daten in der gesamten Serverstruktur.

Hierarchische Verbunde sind beispielsweise bei regionalen Bereitstellungen sinnvoll. So möchten Sie zum Beispiel erreichen, dass lokale Ressourcen Zugang zu Ereignisdaten in einer bestimmten Hierarchie bzw. einem Zweig des Netzwerks haben, nicht jedoch auf die Ereignisdaten anderer, paralleler Zweige zugreifen können. In diesem Fall erstellen Sie einen hierarchischen Verbund mit zwei oder mehr parallelen Zweigen, die die Daten für die jeweilige Region enthalten. Jeder Zweig kann dann Daten an den CA Enterprise Log Manager-Verwaltungsserver im Hauptquartier senden, um dort eine Gesamtübersicht über alle Ereignisprotokollberichte zu ermöglichen.

Beispiel für einen hierarchischen Verbund

In der unten zu sehenden Föderationsübersicht verwendet das Netzwerk den CA Enterprise Log Manager-Verwaltungsserver als Berichtsserver und mehrere (agentenlose) Quellserver für Protokolldateien. Diese Konfiguration ähnelt einem Organisationsdiagramm. Der Verwaltungs-/Berichtsserver fungiert als übergeordneter CA Enterprise Log Manager-Server und stellt Funktionen für Authentifizierung und Autorisierung, wesentliche Verwaltungsfunktionen sowie die Berichtsfunktionen zur Verarbeitung von Abfragen, Berichten und Alarmen bereit. Die (agentenlosen) Quellserver für Protokolldateien in diesem Beispiel sind untergeordnete Server des -Verwaltungs-/Berichtsservers 1. Sie können weitere Ebenen in die Hierarchie einfügen. Es kann allerdings nur einen Verwaltungsserver geben. Die zusätzlichen Ebenen enthalten dann Berichtsserver als übergeordnete Server für die Quellserver.

Bei dieser Art von Föderation könnte der Verwaltungs-/Berichtsserver 1 beispielsweise in der Hauptniederlassung stehen und die Quellserver könnten sich in regionalen bzw. Zweigstellen (repräsentiert durch Quellserver 1 und 2) befinden. Jede Zweigstelle kann dann Berichtsinformationen für die eigenen Daten abrufen, nicht jedoch für die Daten der anderen Zweigstelle. Daten für Quellserver 1 können nur vom Quellserver 1 abgerufen und in Berichte gefasst werden. Über den Verwaltungs-/Berichtsserver 1 können allerdings Daten für den Verwaltungs-/Berichtserver 1 sowie für die Quellserver 1 und 2 abgerufen und als Berichte ausgegeben werden.



In einem hierarchischen Verbund kann jeder CA Enterprise Log Manager-Server über mehrere untergeordnete Server, aber nur über einen übergeordneten Server verfügen. Diese Art der Föderation wird in einer von oben nach unten verlaufenden Struktur, beginnend mit dem Verwaltungsserver, konfiguriert. Anschließend werden auf den darunter liegenden Ebenen die untergeordneten Berichts- und Quellserver eingerichtet. Ein wesentlicher Schritt bei der Konfiguration einer Föderation ist, dass Sie zunächst eine Übersicht über die Server und ihre gewünschten Beziehungen erstellen. Dann können Sie einen CA Enterprise Log Manager-Server als untergeordneten Server konfigurieren und die Beziehungen zwischen den Servern implementieren.

Netzverbund

Ein *Netzverbund* (Verbund wird auch als Föderation bezeichnet) kann wie ein hierarchischer Verbund Ebenen aufweisen. Der Hauptunterschied zwischen den beiden Verbundarten liegt in der Konfiguration der Verbindungen zwischen den Servern. Bei einem Netzverbund können theoretisch über jeden CA Enterprise Log Manager-Server im Netzwerk die Daten auf allen anderen CA Enterprise Log Manager-Servern abgefragt und entsprechende Berichte dazu erstellt werden. Die Möglichkeiten der Berichterstellung sind abhängig von den Beziehungen zwischen den Servern.

So können die Server in einem Netzverbund beispielsweise nur innerhalb eines vertikalen Zweigs miteinander verbunden sein. In diesem Fall haben alle CA Enterprise Log Manager-Server in diesem Zweig Zugang zu allen anderen CA Enterprise Log Manager-Servern in demselben Zweig. Dies steht in direktem Gegensatz zu einem CA Enterprise Log Manager-Server in einem hierarchischen Verbund, der nur Berichte über die Daten auf den ihm untergeordneten Servern ermöglicht.

In einer ring- oder sternförmigen Anordnung ist jeder CA Enterprise Log Manager-Server ein untergeordneter Server zu allen anderen Servern. Wenn Sie Berichtsdaten von einem der CA Enterprise Log Manager-Server anfordern, werden die Daten für alle CA Enterprise Log Manager-Server im Netzwerk angezeigt.

In einem Netzverbund werden zwei oder mehr CA Enterprise Log Manager-Server als Primärserver ausgewiesen und die Server im Verbund werden unabhängig von ihrer Platzierung im Netzwerk verwendet. Die *als* untergeordnete Server eingerichteten Server sind so konfiguriert, dass auch die untergeordneten Server in demselben oder anderen Zweigen angezeigt werden, je nachdem, wie der Verbund aufgebaut it. Falls Sie beispielsweise über die beiden CA Enterprise Log Manager-Server A und B verfügen, können Sie einen Netzverbund erstellen, indem Sie Server B zu einem untergeordneten Server von Server A machen *und* A zu einem untergeordneten Server von B. Diese Konfiguration wird erwartet, wenn Sie zwei oder mehr Verwaltungsserver verwenden.

Beispiel für einen Netzverbund

Betrachten Sie die folgende Abbildung eines vollständigen Netzverbunds:

Im abgebildeten Netzverbund sind vier (agentenlose) Quellserver für Protokolldateien miteinander und mit den beiden Berichtsservern föderiert. Jeder Server ist gleichzeitig jedem anderen Server im Verbund unter- und übergeordnet.

Ein potenzieller Vorzug dieser Art der Bereitstellung gegenüber einer streng hierarchischen Föderation ist, dass Sie von jedem Punkt im Netz aus auf Daten zugreifen und Ergebnisse unabhängig von einer Hierarchie von allen CA Enterprise Log Manager-Servern im Netz abrufen können.

Sie können Netzverbunde und hierarchische Verbunde miteinander kombinieren und so jede Konfiguration erstellen, die Ihren Anforderungen entspricht. Beispielsweise kann ein Netzverbund innerhalb eines einzelnen Zweigs im Netzwerk bei globalen Bereitstellungen sehr sinnvoll sein. Dann können Sie eine globale Übersicht der Daten auf den übergeordneten Berichtsservern abrufen und gleichzeitig regionale Cluster (Zweige) unterhalten, die nur auf ihre eigenen Daten zugreifen können.

Konfigurieren einer CA Enterprise Log Manager-Föderation

Jeder CA Enterprise Log Manager-Server, der einer Föderation (auch Verbund genannt) hinzugefügt wird, muss auf denselben Anwendungsinstanznamen auf dem Verwaltungsserver verweisen. Auf diese Weise können auf dem Verwaltungsserver alle Konfigurationen zusammen als globale Konfigurationen gespeichert und verwaltet werden.

Sie können die Föderation jederzeit konfigurieren. Es empfiehlt sich jedoch, sie einzurichten, bevor Sie Berichte planen, falls konsolidierte Berichte gewünscht werden.

Die Konfiguration einer Föderation umfasst folgende Aufgaben:

1. Erstellen einer Föderationsübersicht
2. Installieren des ersten CA Enterprise Log Manager-Servers, d. h. des Verwaltungsservers
3. Installieren von mindestens einem weiteren Server
4. Konfigurieren der Beziehungen zwischen übergeordneten und untergeordneten Servern Wählen Sie beispielsweise zuerst die untergeordneten Föderationsserver des Verwaltungsservers in den Ereignisprotokollspeicher-Einstellungen dieses Servers aus.

   Diese erste Gruppe mit untergeordneten Servern bildet die zweite Ebene der Föderation, falls Sie einen hierarchischen Verbund einrichten.

5. Rufen Sie das Föderationsdiagramm auf, um zu überprüfen, ob die Struktur zwischen den Servern auf der über- und der untergeordneten Ebene so konfiguriert ist wie von Ihnen beabsichtigt.

Konfigurieren eines CA Enterprise Log Manager-Servers als untergeordneter Server

Die Konfiguration eines CA Enterprise Log Manager-Servers als untergeordneter Server eines anderen Servers ist der wesentliche Schritt beim Anlegen einer Föderation (Verbunds). Gehen Sie wie unten beschrieben vor, um Ihrem Serververbund Server hinzuzufügen. Bevor Sie diesen Teil der Konfiguration durchführen, müssen Sie alle CA Enterprise Log Manager-Server, die in den Verbund aufgenommen werden sollen, unter demselben registrierten Anwendungsinstanznamen installieren. Die Namen aller neu installierten Server werden in der Liste der für die Föderation verfügbaren Server angezeigt. Sie können die folgenden Schritte so oft wie nötig durchführen, um die von Ihnen gewünschte Föderationsstruktur (Verbundstruktur) zu erstellen.

So konfigurieren Sie einen CA Enterprise Log Manager-Server als untergeordneten Server:

1. Melden Sie sich bei einem CA Enterprise Log Manager-Server an, der unter demselben Anwendungsinstanznamen registriert ist wie die anderen Server in Ihrer gewünschten Föderation.
2. Klicken Sie auf die Registerkarte "Verwaltung", und wählen Sie die untergeordnete Registerkarte "Services" aus.
3. Erweitern Sie den Ordner für den Ereignisprotokollspeicher-Service, und wählen Sie den Servernamen für den übergeordneten CA Enterprise Log Manager-Server aus.
4. Blättern Sie nach unten zur Liste "Untergeordnete Föderation".
5. Wählen Sie in der Liste "Verfügbar" einen oder mehrere Namen von Servern aus, die als untergeordnete Server des übergeordneten Servers konfiguriert werden sollen.
6. Verschieben Sie die ausgewählten Server mit den Pfeiltasten in die Liste "Ausgewählt".

   Die ausgewählten und in die Liste verschobenen CA Enterprise Log Manager-Server sind jetzt untergeordnete Server im Verbund mit dem übergeordneten Server.

Weitere Informationen

Verwenden föderierter Abfragen (siehe Seite 147)

Föderationsdiagramm und Server-Statusmonitor anzeigen

Sie können ein Diagramm mit den CA Enterprise Log Manager-Servern in Ihrer Umgebung und deren Beziehungen innerhalb der Föderation sowie Statusinformationen einzelner Server anzeigen. Im Föderationsdiagramm werden die aktuelle Föderationsstruktur und Statusdetails zu jedem Server angezeigt. Darüber hinaus können Sie den lokalen Server, der in dieser Sitzung abgefragt wird, als übergeordneten Server auswählen.

Zum Anzeigen des Föderationsdiagramms klicken Sie am oberen Bildschirmrand auf die Schaltfläche zum Anzeigen des Föderationsdiagramms und des Statusmonitors: 

Es wird ein Fenster mit einer grafischen Übersicht aller Ereignisspeicherhosts, die beim derzeitigen Verwaltungsserver registriert sind, eingeblendet:

- Ereignisspeicher mit untergeordneten Föderationsservern werden hellblau und mit schwarzen Verbindungslinien, die die Beziehung innerhalb der Föderation angeben, dargestellt.
- Ereignisspeicher ohne untergeordnete Föderationsserver werden hellgrün dargestellt.

Sie können einen aktuellen lokalen Server für Abfragezwecke auswählen.

Des Weiteren können Sie Statusdetails aller angezeigten Server anzeigen. Klicken Sie auf einen Server im Föderationsdiagramm, um die Statusdetailanzeigen anzuzeigen, dazu zählen:

- Prozentuale CPU-Auslastung
- Prozentuale Auslastung des verfügbaren Speichers
- Prozentuale Auslastung des verfügbaren Festplattenspeichers
- Empfangene Ereignisse pro Sekunde
- Hauptdiagramm des Status des Ereignisprotokollspeichers

Weitere Informationen

Beispiel: Föderationsübersicht für ein mittelgroßes Unternehmen (siehe Seite 37)
Beispiel: Föderationsübersicht für ein großes Unternehmen (siehe Seite 35)

Kapitel 8: Arbeiten mit der Ereignisverfeinerungs-Bibliothek

Dieses Kapitel enthält folgende Themen:

Wissenswertes über die Ereignisverfeinerungs-Bibliothek

Die Ereignisverfeinerungs-Bibliothek stellt Werkzeuge bereit, mit denen Sie neue Analyse- und Zuordnungsdateien erstellen bzw. bestehende Dateien so ändern können, dass neue Geräte, Anwendungen usw. unterstützt werden. Die Bibliothek bietet folgende Optionen:

- Integrationen
- Listener
- Zuordnungs- und Analysedateien
- Unterdrückungs- und Zusammenfassungsregeln

Mit Unterdrückungsregeln wird verhindert, dass Daten erfasst bzw. in den Ereignisprotokollspeicher eingefügt werden. Mittels Zusammenfassungsregeln können Sie Ereignisse aggregieren und so die Anzahl von Einfügungen für ähnliche Ereignistypen oder Aktionen reduzieren. Unterdrückungs- und Zusammenfassungsregeln sind der am häufigsten verwendete Teil der Bibliothek, da hiermit die Netzwerk- und Datenbankleistung optimiert werden kann.

Im Abschnitt für Integrationen können Sie vordefinierte Integrationen anzeigen und neue Integrationen für Ihre eigenen Geräte, Anwendungen, Dateien oder Datenbanken erstellen. Weitere Informationen finden Sie im *CA Enterprise Log Manager-Administrationshandbuch* und in der Online-Hilfe.

Unterstützen neuer Ereignisquellen mit der Ereignisverfeinerungs-Bibliothek

Falls Geräte, Anwendungen, Datenbanken oder Ereignisquellen unterstützt werden sollen, die derzeit noch nicht unterstützt werden, müssen Sie die erforderlichen Komponenten mit Hilfe des Assistenten für Analysedateien, des Assistenten für Zuordnungsdateien und des Assistenten für Integrationen erstellen.

Der Vorgang umfasst die folgenden allgemeinen Schritte:

1. Erstellen von Analysedateien zum Erfassen von Ereignisdaten als Namen-Wert-Paare
2. Erstellen von Zuordnungsdateien zum Zuordnen der Namen-Wert-Paare in der ELM-Schemadefinition
3. Erstellen neuer Integrationen und Listener zum Erfassen von Daten aus der Ereignisquelle

Integrationen, Analyse- und Zuordnungsdateien sowie Unterdrückungs- und Zusammenfassungsregeln werden ausführlich im *CA Enterprise Log Manager-Administrationshandbuch* und in der Online-Hilfe besprochen.

Zuordnungs- und Analysedateien

Während des Betriebs liest CA Enterprise Log Manager die eintreffenden Ereignisse und unterteilt sie in einem *Analyse* genannten Vorgang in Abschnitte. Es gibt eigene Nachrichtenanalysedateien für unterschiedliche Geräte, Betriebssysteme, Anwendungen und Datenbanken. Nachdem die eintreffenden Ereignisse in Namen-Wert-Paaren analysiert wurden, durchlaufen diese Daten ein *Zuordnungs*modul, mit dem die Ereignisdaten in den Feldern der Datenbank abgelegt werden.

Das Zuordnungsmodul verwendet Datenzuordnungsdateien, die ähnlich den Nachrichtenanalysedateien für spezifische Ereignisquellen erstellt wurden. Beim Datenbankschema handelt es sich um die ELM-Schemadefinition, eine der zentralen Funktionen von CA Enterprise Log Manager.

Mittels Analyse und Zuordnung werden Daten normalisiert und unabhängig vom Ereignistyp oder Meldungsformat in einer allgemeinen Datenbank gespeichert.

Der Integrationsassistent und einige CA-Adaptermodule erfordern die Konfiguration der Zuordnungs- und Analysedateien, die die Art von Ereignisdaten, die von einem Connector oder Adapter überwacht werden, am besten beschreiben. In den Konfigurationsfenstern mit diesen Steuerelementen sollte die Reihenfolge der Nachrichtenanalysedateien die relative Anzahl der eingehenden Ereignisse dieses Typs widerspiegeln. Die Reihenfolge der Datenzuordnungsdateien sollte die Menge der von einer bestimmten Quelle eingehenden Ereignisse widerspiegeln.

Wenn das Syslog-Listener-Modul eines bestimmten CA Enterprise Log Manager-Servers beispielsweise vor allem Ereignisse der Cisco PIX Firewall empfängt, sollten die Dateien "CiscoPIXFW.XMPS" und "CiscoPIXFW.DMS" in der jeweiligen Liste ganz oben stehen.

Anhang A: Aspekte für CA Audit-Benutzer

Dieses Kapitel enthält folgende Themen:

Unterschiede in der Architektur

Bei der Planung der gemeinsamen Verwendung von CA Audit und CA Enterprise Log Manager müssen Sie zunächst die Unterschiede in der Architektur und deren Auswirkungen auf die Netzwerkstruktur kennen.

CA Enterprise Log Manager verwendet einen eingebetteten Ereignisprotokollspeicher und stellt einen Agenten-Explorer für die Konfiguration und Verwaltung von Agenten bereit. Dank neuer Technologie gekoppelt mit einer ELM-Schemadefinition können Ereignisse schneller an den Speicher geleitet und eine größere Anzahl von Ereignisquellen unterstützt werden. Mit der ELM-Schemadefinition kann CA Enterprise Log Manager Ereignisse aus vielen verschiedenen Ereignisquellen in einem einzelnen Datenbankschema normalisieren.

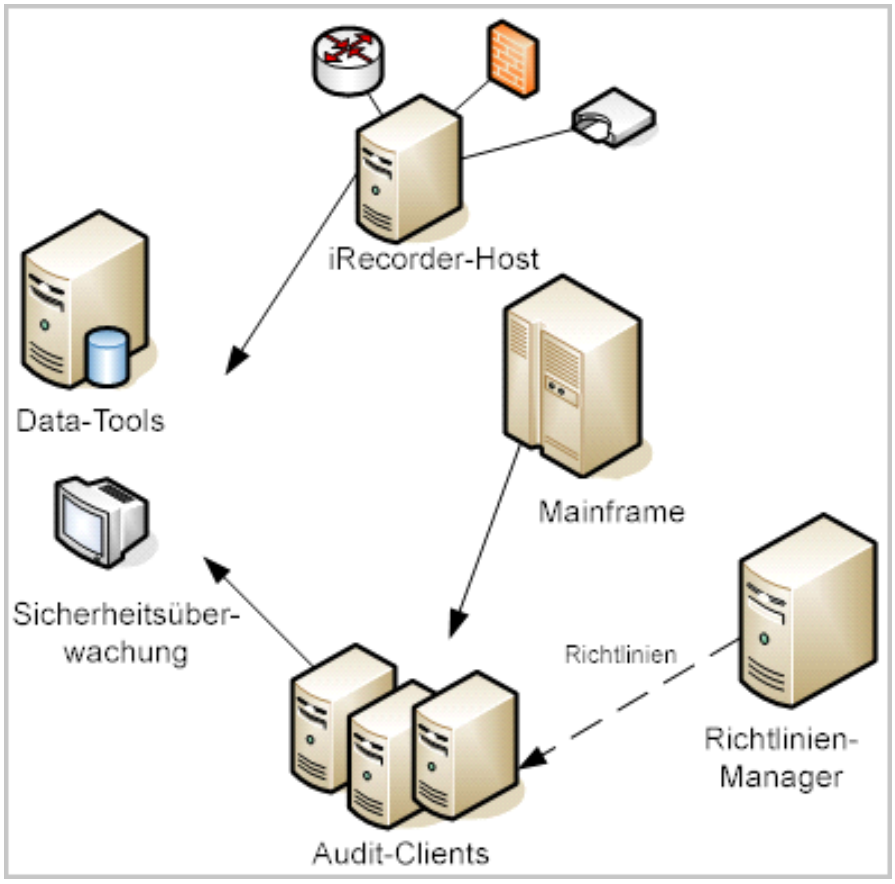
CA Enterprise Log Manager kann auf einem bestimmten Niveau mit CA Audit interagieren, ist jedoch nicht auf vollständige Interoperabilität ausgelegt. CA Enterprise Log Manager ist eine neue und eigenständige Serverinfrastruktur, die parallel zu CA Audit ausgeführt werden kann. Dabei gilt es allerdings, folgende Punkte zur Ereignisverarbeitung zu bedenken:

CA Enterprise Log Manager bietet folgende Funktionen:	**CA Enterprise Log Manager bietet folgende Funktionen *nicht*:**
Empfang von Ereignisprotokollen, die von CA Audit-Clients und iRecordern über konfigurierbare Listener gesendet werden	Direkter Zugriff auf Ereignisprotokolle, die in der CA Audit-Collector-Datenbank gespeichert sind
Hilfsprogramm für den Import von Ereignisprotokolldaten, die in der CA Audit-Collector-Datenbank (SEOSDATA-Tabelle) gespeichert sind	

CA Enterprise Log Manager bietet folgende Funktionen:	**CA Enterprise Log Manager bietet folgende Funktionen *nicht*:**
Verwendung von Agenten zum ausschließlichen Senden von Ereignisprotokollen an die CA Enterprise Log Manager-Serverinfrastruktur	
Ausführen von CA Enterprise Log Manager-Agenten und CA Audit-Clients mit iRecordern auf demselben physischen Host	Gleichzeitiger Zugriff auf dieselben Protokollquellen durch CA Enterprise Log Manager-Agenten und CA Audit-Clients mit iRecordern
Verwenden des integrierten Agenten-Explorers zum ausschließlichen Verwalten von CA Enterprise Log Manager-Agenten. Während des parallelen Betriebs der beiden Systeme verwendet CA Audit seinen Richtlinien-Manager nur zum Verwalten von CA Audit-Clients.	
	Migrieren von CA Audit-Daten in Tabellen-Collectors, Berichtsvorlagen oder benutzerdefinierten Berichten, Alarmrichtlinien, Erfassungs-/Filterrichtlinien oder rollenbasierten Zugriffssteuerungsrichtlinien

Architektur von CA Audit

Die folgende Abbildung zeigt eine einfache CA Audit-Implementierung:



Bei einigen Unternehmensbereitstellungen von CA Audit werden Ereignisdaten vom Collector-Service in einer auf dem Data-Tools-Server ausgeführten relationalen Datenbank gespeichert. Diese Datenbank wird von einem Datenbankadministrator überwacht und gewartet. Der Datenbankadministrator arbeitet mit einem Systemadministrator zusammen, um sicherzustellen, dass mit Hilfe der richtigen Richtlinien die gewünschten Ereignisse erfasst und nicht benötigte Ereignisse von der Erfassung ausgeschlossen werden.

Die durchgezogenen Linien in diesem Diagramm zeigen Ereignisse, die von CA Audit-Clients sowie von Recorder- und iRecorder-Hosts an den Data-Tools-Server und in einigen Fällen an eine optionale Konsole zur Sicherheitsüberwachung gesendet werden. Die gestrichelte Linie zeigt den Verlauf der auf Richtlinien basierenden Steuerung zwischen dem Richtlinien-Manager-Server und den Clients.

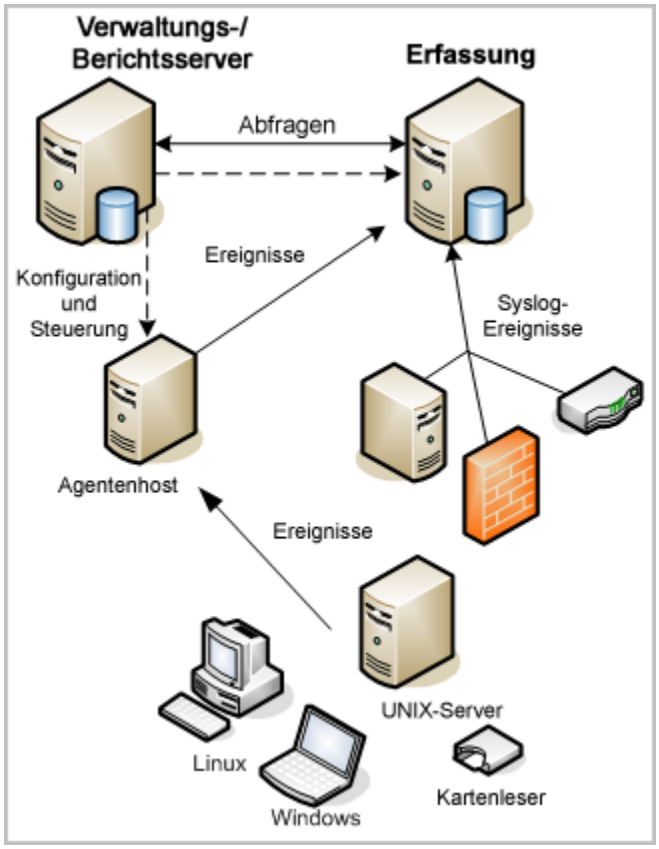
Der Data-Tools-Server stellt einfache Berichts- und Visualisierungsprogramme sowie eine Ereignisspeicherung bereit. Benutzerdefinierte Abfragen und Berichte, deren Erstellung und Verwaltung sehr zeitaufwändig ist, sind die Regel in Unternehmensimplementierungen.

Diese Netzwerktopologie ermöglicht die Erfassung verschiedener Ereignistypen aus unterschiedlichen Geräten, Anwendungen und Datenbanken. Der zentrale Speicher für die erfassten Ereignisse ist normalerweise Teil des Data-Tools-Servers, der diesen Speicher auch verwaltet und bestimmte Berichte bereitstellt.

Sie benötigen allerdings zusätzliche Ressourcen, um Ihre Lösung so anzupassen, dass schnell ansteigende Ereignismengen verarbeitet werden können. Sie müssen Berichte erstellen, die zeigen, dass lokale und internationale Bestimmungen eingehalten werden. Und Sie müssen in der Lage sein, diese Berichte schnell und problemlos aufzufinden.

Architektur von CA Enterprise Log Manager

Die folgende Abbildung zeigt eine einfache CA Enterprise Log Manager-Implementierung mit zwei Servern:



Ein CA Enterprise Log Manager-System kann über einen oder mehrere Server verfügen, wobei der zuerst installierte Server als Verwaltungsserver fungiert. Jedes System kann nur einen Verwaltungsserver haben, Sie können jedoch über mehrere Systeme verfügen. Auf dem Verwaltungsserver werden der Inhalt und die Konfiguration aller CA Enterprise Log Manager-Server verwaltet und die Benutzerautorisierung und -authentifizierung durchgeführt.

In einer einfachen Implementierung mit zwei Servern übernimmt der Verwaltungsserver auch die Funktion eines Berichtsservers. Ein Berichtsserver empfängt aufbereitete Ereignisse von einem oder mehreren (agentenlosen) Quellservern für Protokolldateien. Der Berichtsserver verarbeitet Bedarfsabfragen und -berichte sowie geplante Alarme und Berichte. Auf dem (agentenlosen) Quellserver für Protokolldateien werden die erfassten Ereignisse aufbereitet.

Jeder CA Enterprise Log Manager-Server verfügt über seine eigene interne Ereignisprotokollspeicherdatenbank. Beim Ereignisprotokollspeicher handelt es sich um eine proprietäre Datenbank, die mittels Komprimierung die Speicherkapazität verbessert und Abfragen in aktiven Datenbankdateien, für die Archivierung ausgewiesenen Dateien und verfügbar gemachten Dateien ermöglicht. Für die Ereignisspeicherung ist kein relationales DBMS-Paket erforderlich.

Der (agentenlose) CA Enterprise Log Manager-Quellserver für Protokolldateien kann Ereignisse direkt über den Standardagenten bzw. über Agenten auf anderen Ereignisquellen empfangen. Agenten können sich auch auf einem Host befinden, der als Collector für andere Ereignisquellen im Netzwerk oder für einen VPN-Concentrator oder Router-Host fungiert.

Die durchgezogenen Linien in diesem Diagramm zeigen den Ereignisfluss von den Ereignisquellen über die Agenten hin zum Quellserver für Protokolldateien und weiter zur Berichtsfunktion des Verwaltungs-/Berichtsservers. Die gestrichelten Linien zeigen den Konfigurations- und Steuerungsverlauf zwischen den CA Enterprise Log Manager-Servern sowie den Verlauf von der Verwaltungsrolle des Verwaltungs-/Berichtsservers hin zu den Agenten. Sie können über jeden CA Enterprise Log Manager-Server im Netzwerk jeden Agenten im Netzwerk steuern, sofern die CA Enterprise Log Manager-Server während der Installation mit demselben Anwendungsinstanznamen beim Verwaltungsserver registriert wurden.

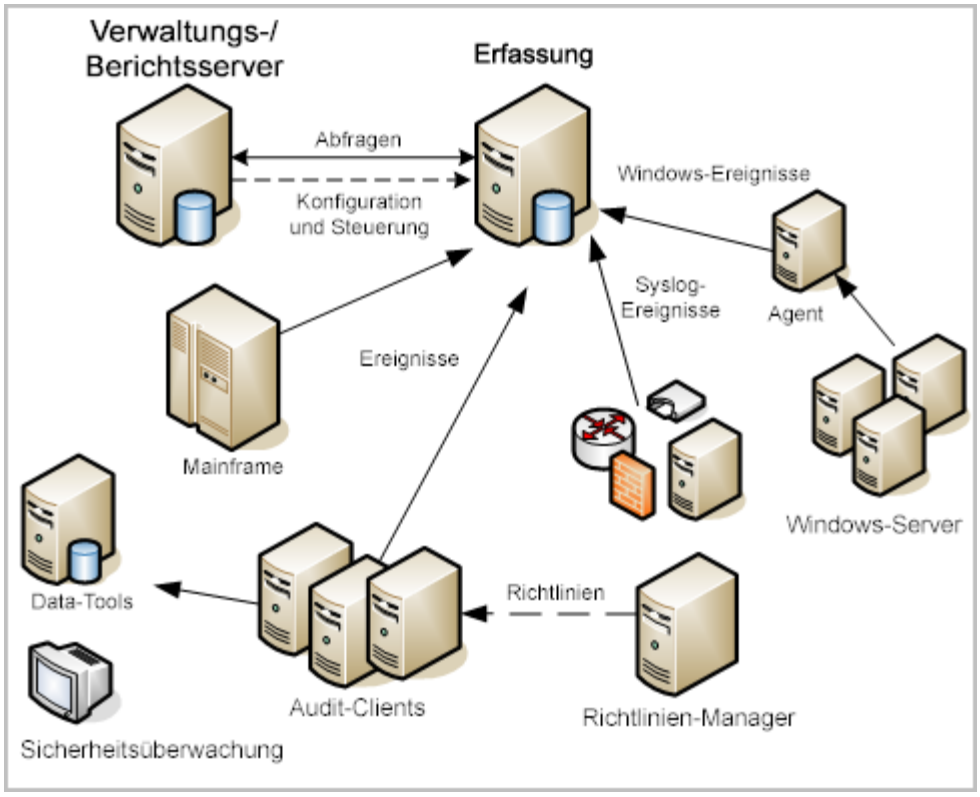
Agenten erfassen Ereignisse mit Hilfe von Connectors (nicht abgebildet). Ein einzelner Agent kann mehrere Connectors verwalten, so dass verschiedene Arten von Ereignissen gleichzeitig erfasst werden können. Dies bedeutet, dass ein einzelner, auf einer bestimmten Ereignisquelle bereitgestellter Agent verschiedene Arten von Daten erfassen kann. Der CA Enterprise Log Manager-Server stellt ferner Listener bereit, über die mit Hilfe der vorhandenen iRecorder and SAPI-Recorder Ereignisse aus anderen CA-Anwendungen im CA Audit-Netzwerk erfasst werden können.

Sie können CA Enterprise Log Manager-Server in einen Verbund (Föderation) einbinden, um Ihre Lösung zu skalieren und Berichtsdaten zwischen den Servern auszutauschen, ohne dass Daten zwischen den Servern übertragen werden müssen. So können Sie die Compliance im gesamten Netzwerk überprüfen und gleichzeitig die Vorgaben zur Wahrung des physischen Speicherorts der Daten einhalten.

Dank automatischer Software-Updates für vordefinierte Abfragen und Berichte müssen Sie Abfragen und Berichte nicht mehr manuell verwalten. Mit den integrierten Assistenten können Sie Ihre eigenen Integrationen für noch nicht unterstützte Drittanbietergeräte und -anwendungen erstellen.

Integrierte Architektur

Das folgende Diagramm zeigt ein typisches CA Audit-Netzwerk, dem CA Enterprise Log Manager hinzugefügt wurde, so dass die Ressourcen zur Verarbeitung großer Ereignisvolumen und zur Erstellung Compliance-basierter Berichte optimal genutzt werden können:



CA Enterprise Log Manager verwendet einen integrierten Agenten-Explorer, einen eingebetteten Ereignisprotokollspeicher und eine einzelne Benutzeroberfläche für eine zentrale und einfache Protokollerfassung. Dank der CA Enterprise Log Manager-Agententechnologie gekoppelt mit der ELM-Schemadefinition können Ereignisse schneller an den Speicher geleitet und eine größere Anzahl von Ereignisquellen verarbeitet werden. Über einen einzelnen Agenten lassen sich mehrere Connectors für Ereignisquellen steuern, wodurch die Agentenverwaltung erleichtert wird und die Vorteile der vordefinierten Integrationen für gängige bzw. beliebte Ereignisprotokollquellen genutzt werden können.

Bei dieser Implementierung empfängt der (agentenlose) CA Enterprise Log Manager-Quellserver für Protokolldateien die Syslog-, iTechnology-basierten und SAPI-Recorder-Ereignisse direkt. Der Quellserver für Protokolldateien empfängt Ereignisse aus Windows-Ereignisquellen über einen eigenen Windows-basierten CA Enterprise Log Manager-Agenten. Sie können im Netzwerk mehrere Agenten bereitstellen, die jeweils viele unterschiedliche Ereignisdaten über ihre Connectors erfassen. Hierdurch können der an die SEOSDATA-Datenbank geleitete Ereignisstrom reduziert und die in CA Enterprise Log Manager verfügbaren Abfragen und Berichte genutzt werden. Mit einer einfachen Richtlinienregeländerung wird den CA Audit-Clients ermöglicht, erfasste Ereignisse sowohl an den Data-Tools-Server als auch an den CA Enterprise Log Manager-Server zu senden.

Neben einem höheren Durchsatz bietet CA Enterprise Log Manager vorgefertigte Abfragen und Berichte, mit denen Sie zeigen können, dass Normen wie etwa PCI (DSS) und SOX erfüllt werden. Wenn Sie die vordefinierten Abfragen und Berichte mit Ihrer bestehenden CA Audit- und CA Security Command Center-Implementierung verknüpfen, nutzen Sie Ihre Investitionen in individuelle Lösungen sowie die CA Enterprise Log Manager-Berichte und den höheren Durchsatz zu Ihren Gunsten.

Konfigurieren von CA-Adaptern

Bei den CA-Adaptern handelt es sich um eine Gruppe von Listenern, die Ereignisse von alten Komponenten wie etwa CA Audit-Clients, iRecordern und SAPI-Recordern sowie von Ereignisquellen, die Ereignisse systemeigen über iTechnology senden, empfangen.

Legen Sie die Konfigurationsoptionen für die CA-Adapter fest, bevor Sie die Konfiguration der CA Audit-Richtlinien oder iRecorder ändern. So wird sichergestellt, dass die Listener-Prozesse arbeiten, bevor Ereignisse eintreffen. Dies beugt falsch zugeordneten Ereignisdaten vor.

Falls Sie Ereignisse über einen iRecorder an CA Audit senden oder einen CA Audit-Client mit iRecorder nutzen, verwenden Sie die CA Enterprise Log Manager-SAPI-Adapter zum Empfang von Ereignissen. Um Ereignisse an CA Enterprise Log Manager zu senden, ändern Sie eine bestehende CA Audit-Richtlinie für CA Access Control-Ereignisse. Sie können entweder eine Collector- oder eine Route-Aktion zu einer bestehenden Regel hinzufügen.

- Falls Sie eine Collector-Aktion für eine Regel in einer bestehenden CA Audit-Richtlinie erstellen, konfigurieren Sie den SAPI-Collector-CA-Adapter für den Empfang von Ereignissen.
- Falls Sie eine Route-Aktion für eine Regel in einer bestehenden CA Audit-Richtlinie erstellen, konfigurieren Sie den SAPI-Router-CA-Adapter für den Empfang von Ereignissen.

Anleitungen dazu, wie Sie SAPI so neu konfigurieren können, dass Ereignisse direkt an CA Enterprise Log Manager gesendet werden, finden Sie in der SAPI-Dokumentation.

Falls Sie einen eigenständigen iRecorder installieren oder einen bestehenden iRecorder verwenden möchten, konfigurieren Sie das iTech-Ereignis-Plugin zum Empfang von Ereignissen. Verwenden Sie diese Vorgehensweise zum Beispiel, wenn CA Audit nicht installiert ist, Sie aber mit einem CA-iRecorder Ereignisse aus einer unterstützten Ereignisquelle erfassen möchten. Der Vorgang umfasst folgende Schritte:

- Konfigurieren des iTechnology-Ereignis-Plugins
- Konfigurieren des iRecorder- oder iTechnology-basierten Produkts, so dass Ereignisse direkt an den CA Enterprise Log Manager-Server gesendet werden

Wissenswertes über den SAPI-Router und -Collector

Die SAPI-Services sind im Allgemeinen für den Empfang von Ereignissen von bestehenden CA Audit-Clients und integrierten Produkten zuständig. CA Enterprise Log Manager verwendet zwei Instanzen eines SAPI-Listener-Service, wovon der eine als SAPI-Collector, der andere als SAPI-Router installiert wird.

Die SAPI-Module verwenden den iGateway-Daemon für die Befehlsgebung und Steuerung. Die Module fungieren als SAPI-Router und SAPI-Collector und verwenden entweder statische Ports oder dynamische Ports über den Portmapper.

Verwenden Sie den SAPI-Collector zum Senden von Ereignissen, die von CA Audit-Clients stammen, so dass Sie die integrierte Failover-Unterstützung der Audit-Collector-Aktion nutzen können.

Verwenden Sie den SAPI-Router zum Senden von Ereignissen, die von CA Audit-Clients stammen, mittels Route-Aktion oder zum Senden von Ereignissen, die von SAPI-Recordern oder Integrationen stammen, die das direkte Senden von Ereignissen an einen CA Audit-Client unterstützen. In diesem Fall konfigurieren Sie den Remote-Sender so, als ob es sich beim CA Enterprise Log Manager-Server um den CA Audit-Client handeln würde.

Der SAPI-Listener öffnet seinen eigenen Port und überwacht diesen passiv auf neue Ereignisse. Jede Instanz des SAPI-Moduls verfügt über ihre eigene Konfiguration, mit der folgende Einstellungen angegeben werden:

- Zu überwachender Port
- Zu ladende Datenzuordnungsdateien
- Zu verwendende Verschlüsselungsbibliotheken

Nach Eingang des Ereignisses wird dieses vom Modul an die Zuordnungsbibliothek gesendet und dann von CA Enterprise Log Manager in die Datenbank eingefügt.

Wichtig: Die Datenzuordnungsbibliothek kann Zuordnungsdateien mit demselben Namen, aber einer anderen Versionsnummer enthalten. Die verschiedenen Dateien unterstützen unterschiedliche Versionen derselben Ereignisquelle, wie etwa eines Betriebssystems oder einer Datenbank. Wichtig ist, dass Sie bei der Konfiguration des SAPI-Collectors bzw. -Routers nur eine Zuordnungsdatei mit der richtigen Version auswählen.

Falls die Liste der ausgewählten Zuordnungsdateien zwei Dateien mit demselben Namen enthält, verwendet das Zuordnungsmodul nur die erste Datei in der Liste. Falls dies nicht die richtige Datei für den eintreffenden Ereignisstrom ist, kann das Zuordnungsmodul die Ereignisse nicht richtig zuordnen. Dies kann wiederum dazu führen, dass die falsch zugeordneten Ereignisse nicht in Abfragen und Berichten erscheinen bzw. dass Abfragen und Berichte überhaupt keine Ereignisse enthalten.

Konfigurieren des SAPI-Collector-Service

Gehen Sie wie unten beschrieben vor, um den SAPI-Collector-Service zu konfigurieren.

Sie können CA Audit-Richtlinien ändern, die Ereignisse mit Hilfe von Collector-Aktionen an einen CA Enterprise Log Manager-Server senden, wobei der CA Enterprise Log Manager-Server zusätzlich zur oder anstelle der CA Audit-Collector-Datenbank verwendet werden kann. Konfigurieren Sie diesen Service, bevor Sie die Audit-Richtlinien ändern, damit keine Ereignisse verloren gehen.

So konfigurieren Sie den SAPI-Collector-Service:

1. Melden Sie sich beim CA Enterprise Log Manager-Server an, und wählen Sie die Registerkarte "Verwaltung" aus.

   Die untergeordnete Registerkarte "Protokollerfassung" wird standardmäßig angezeigt.

2. Erweitern Sie den Eintrag "CA-Adapter".
3. Wählen Sie den SAPI-Collector-Service aus.
4. Eine Beschreibung der einzelnen Felder finden Sie in der Online-Hilfe.
5. Klicken Sie abschließend auf "Speichern".

Konfigurieren des SAPI-Router-Service

Gehen Sie wie unten beschrieben vor, um den SAPI-Router-Service zu konfigurieren.

Sie können CA Audit-Richtlinien ändern, die Ereignisse mit Hilfe von Route-Aktionen an einen CA Enterprise Log Manager-Server senden, wobei die Ereignisse zusätzlich zu oder anstelle von anderen Zielen an den CA Enterprise Log Manager-Server geleitet werden. Ferner können Sie SAPI-Recorder-Ereignisse so umleiten, dass diese direkt an den SAPI-Router-Listener gesendet werden, indem Sie die entsprechenden Konfigurationsdateien bearbeiten. Konfigurieren Sie diesen Service, bevor Sie die Audit-Richtlinien oder die Konfigurationen für den SAPI-Recorder ändern, damit keine Ereignisse verloren gehen.

So konfigurieren Sie den SAPI-Router-Service:

1. Melden Sie sich beim CA Enterprise Log Manager-Server an, und wählen Sie die Registerkarte "Verwaltung" aus.

   Die untergeordnete Registerkarte "Protokollerfassung" wird standardmäßig angezeigt.

2. Erweitern Sie den Eintrag "CA-Adapter".

3. Wählen Sie den SAPI-Router-Service aus.
4. Eine Beschreibung der einzelnen Felder finden Sie in der Online-Hilfe.
5. Klicken Sie abschließend auf "Speichern".

Wissenswertes über das iTechnology-Ereignis-Plugin

Das iTechnology-Ereignis-Plugin empfängt Ereignisse, die über den iGateway-Mechanismus für die Ereignisverarbeitung gesendet wurden. Konfigurieren Sie das iTechnology-Ereignis-Plugin, falls mindestens einer der folgenden Punkte auf Ihre Umgebung zutrifft:

- Ihr Netzwerk weist bestehende iRecorder auf, für die es keine CA Audit-Clients auf demselben System gibt.
- Sie verfügen über andere Produkte wie etwa CA EEM, die Ereignisse über iTechnology weiterleiten können.

Nach Eingang eines Ereignisses wird dieses von diesem Service an die Zuordnungsbibliothek übermittelt. Anschließend wird das zugeordnete Ereignis von CA Enterprise Log Manager in den Ereignisprotokollspeicher eingefügt.

Konfigurieren des iTechnology-Ereignis-Plugins

Gehen Sie wie unten beschrieben vor, um das iTechnology-Ereignis-Plugin zu konfigurieren, mit dem Sie Ereignisse von iRecorder- und anderen iTechnology-Ereignisquellen empfangen können.

Verwenden Sie das iTechnology-Plugin, wenn Sie einen eigenständigen iRecorder so konfigurieren, dass dessen Ereignisse an einen CA Enterprise Log Manager-Server gesendet werden. Konfigurieren Sie diesen Service, *bevor* Sie einen iRecorder installieren bzw. konfigurieren, damit keine Ereignisse verloren gehen.

So konfigurieren Sie das iTechnology-Ereignis-Plugin:

1. Melden Sie sich beim CA Enterprise Log Manager-Server an, und wählen Sie die Registerkarte "Verwaltung" aus.

   Die untergeordnete Registerkarte "Protokollerfassung" wird standardmäßig angezeigt.
2. Erweitern Sie den Eintrag "CA-Adapter".

3. Wählen Sie den Service für das iTechnology-Ereignis-Plugin aus.
4. Wählen Sie in der Liste der verfügbaren Datenzuordnungsdateien eine oder mehrere Datenzuordnungsdateien aus, und verschieben Sie sie mit den Pfeilen in die Liste der ausgewählten Datenzuordnungsdateien.

   Der Service für das Ereignis-Plugin ist so vorkonfiguriert, dass er die meisten wichtigen Datenzuordnungsdateien umfasst.
5. Klicken Sie auf "Speichern", um die Änderungen in den Konfigurationsdateien auf dem Verwaltungsserver zu speichern.

Senden von CA Audit-Ereignissen an CA Enterprise Log Manager

Sie können CA Enterprise Log Manager auf folgende Weise in Ihre bestehende CA Audit-Implementierung integrieren:

- Konfigurieren Sie einen iRecorder, der sich nicht auf demselben Host befindet wie ein CA Audit-Client, so, dass Ereignisse an CA Enterprise Log Manager gesendet werden.
- Ändern Sie eine bestehende CA Audit-Richtlinie so, dass Ereignisse an CA Audit und CA Enterprise Log Manager gesendet werden.

Konfigurieren eines iRecorders zum Senden von Ereignissen an CA Enterprise Log Manager

CA Enterprise Log Manager empfängt Ereignisse von iRecordern über den Listener für das iTech-Ereignis-Plugin. Sie müssen den Listener konfigurieren, bevor Sie die Konfiguration des iRecorders ändern. Andernfalls können Ereignisdaten verloren gehen. Nachdem Sie den Listener konfiguriert haben, gehen Sie wie unten beschrieben vor, um den iRecorder für das Senden von Ereignissen an den CA Enterprise Log Manager-Server einzurichten.

iRecorder, die auf demselben Computer installiert sind wie ein CA Audit-Client, senden Ereignisse direkt an den Client. Verwenden Sie bei diesen Rechnern vorzugsweise den SAPI-Collector oder Router-Adapter.

Wichtig! Ein eigenständiger iRecorder kann Ereignisse nur an ein Ziel senden. Falls Sie einen iRecorder wie unten beschrieben neu konfigurieren, werden die Ereignisse *nur* im CA Enterprise Log Manager-Ereignisprotokollspeicher gespeichert. Falls die Ereignisse sowohl im Ereignisprotokollspeicher als auch in der Datenbank des CA Audit-Collectors aufbewahrt werden müssen, fügen Sie eine entsprechende Regelaktion zu einer bestehenden Richtlinie hinzu oder erstellen eine neue Richtlinie für einen CA Audit-Client.

So konfigurieren Sie den iRecorder zum Senden von Ereignissen an CA Enterprise Log Manager:

1. Melden Sie sich beim Hostserver des iRecorders als Benutzer mit Administratorrechten an.
2. Navigieren Sie zu folgendem Verzeichnis auf Ihrem Betriebssystem:
   - UNIX oder Linux: /opt/CA/SharedComponents/iTechnology
   - Windows: \Programme\CA\SharedComponents\iTechnology
3. Stoppen Sie den iGateway-Daemon bzw. -Service mit folgendem Befehl:
   - UNIX oder Linux: ./S99igateway stop
   - Windows: net stop igateway
4. Bearbeiten Sie die Datei "iControl.conf".
5. Geben Sie den folgenden Wert für "RouteEvent" an:

   ```
   <RouteEvent>true</RouteEvent>
   ```

   Mit diesem Eintrag wird iGateway angewiesen, alle Ereignisse, einschließlich aller iRecorder-Ereignisse, an den im Tag-Paar "RouteHost" angegebenen Host zu senden.
6. Geben Sie den folgenden Wert für "RouteHost" an:

   ```
   <RouteHost>CA_ELM_Hostname</RouteHost>
   ```

   Mit diesem Eintrag wird iGateway angewiesen, Ereignisse an den CA Enterprise Log Manager-Server zu senden, der seinen DNS-Namen verwendet.
7. Starten Sie den iGateway-Daemon bzw. -Service mit folgendem Befehl:
   - UNIX oder Linux: ./S99igateway start
   - Windows: net start igateway

   Mit dieser Aktion werden die neuen Einstellungen im iRecorder aktiviert. Ereignisse fließen jetzt vom iRecorder zum CA Enterprise Log Manager-Server.

Weitere Informationen

Wissenswertes über den SAPI-Router und -Collector (siehe Seite 230)
Konfigurieren des SAPI-Collector-Service (siehe Seite 232)
Konfigurieren des SAPI-Router-Service (siehe Seite 232)

Ändern einer bestehenden CA Audit-Richtlinie zum Senden von Ereignissen an CA Enterprise Log Manager

Gehen Sie wie unten beschrieben vor, um einen CA Audit-Client so einzurichten, dass Ereignisse an CA Enterprise Log Manager *und* an die CA Audit-Collector-Datenbank gesendet werden. Indem Sie der Route- bzw. Collector-Aktion einer bestehenden Regel ein neues Ziel hinzufügen, können Sie erfasste Ereignisse an beide Systeme senden. Alternativ können Sie bestimmte Richtlinien bzw. Regeln auch so ändern, dass Ereignisse *nur* an den CA Enterprise Log Manager-Server gesendet werden.

CA Enterprise Log Manager erfasst Ereignisse von CA Audit-Clients mit Hilfe des CA Audit-SAPI-Router- und des CA Audit-SAPI-Collector-Listeners. Erfasste Ereignisse werden im CA Enterprise Log Manager-Ereignisprotokollspeicher erst gespeichert, *nachdem* die Richtlinie auf die Clients übertragen und aktiviert wurde.

Wichtig: Sie müssen die CA Enterprise Log Manager-Listener für den Empfang von Ereignissen einrichten, bevor Sie die Richtlinie ändern und aktivieren. Falls Sie diese Konfiguration nicht zuerst vornehmen, können falsch zugeordnete Ereignisse auftreten, wenn Ereignisse vor dem Zeitpunkt, zu dem die Richtlinie in Kraft tritt und die Listener die Ereignisse richtig zuordnen können, eintreffen.

So ändern Sie die Aktion einer bestehenden Richtlinienregel zum Senden von Ereignissen an CA Enterprise Log Manager:

1. Melden Sie sich beim Richtlinien-Manager-Server an, und greifen Sie links im Fenster auf die Registerkarte "Meine Richtlinien" zu.
2. Erweitern Sie den Richtlinienordner, bis die gewünschte Richtlinie angezeigt wird.
3. Klicken Sie auf die Richtlinie, damit die grundlegenden Informationen im Detailabschnitt rechts im Fenster angezeigt werden.
4. Klicken Sie im Detailabschnitt auf "Bearbeiten", um die Richtlinienregeln hinzuzufügen. Der Regelassistent wird gestartet.
5. Klicken Sie auf "Aktionen bearbeiten" neben dem Pfeil für Schritt 3 im Assistenten. Die Assistentenseite mit den Regelaktionen wird angezeigt.
6. Klicken Sie im Fenster "Aktionen durchsuchen" auf der linken Seite auf die Aktion "Collector". Hierdurch wird auf der rechten Seite die Liste der Aktionen eingeblendet.

   Sie können auch mit der Route-Aktion eine Regel erstellen, über die Ereignisse an einen CA Enterprise Log Manager-Server gesendet werden.
7. Klicken Sie auf "Neu", um eine neue Regel hinzuzufügen.

8. Geben Sie die IP-Adresse bzw. den Hostnamen des CA Enterprise Log Manager-Quellservers für Protokolldateien ein.

   Bei CA Enterprise Log Manager-Implementierungen mit zwei oder mehr Servern können Sie im Feld für den alternativen Hostnamen einen anderen CA Enterprise Log Manager-Hostnamen bzw. eine andere IP-Adresse eingeben, um die CA Audit-Funktion des automatischen Failovers zu nutzen. Falls der erste CA Enterprise Log Manager-Server nicht verfügbar ist, sendet CA Audit automatisch Ereignisse an den im Feld "Alternativer Hostname" benannten Server.

9. Geben Sie im Feld "Alternativer Hostname" den Namen des CA Enterprise Log Manager-Verwaltungsservers ein, und erstellen Sie eine Beschreibung für die neue Regelaktion.

10. Deaktivieren Sie das Kontrollkästchen "Diese Aktion auf Remote-Server durchführen", falls es aktiviert ist.

11. Klicken Sie auf "Hinzufügen", um die neue Regelaktion zu speichern, und klicken Sie dann im Assistentenfenster auf "Fertig stellen".

12. Wählen Sie unten rechts die Registerkarte "Regeln" aus, und wählen Sie dann die zu überprüfende Regel aus.

13. Klicken Sie auf "Richtlinien überprüfen", um die geänderte Regel mit den neuen Aktionen zu überprüfen und sicherzustellen, dass sie richtig kompiliert wird.

    Nehmen Sie ggf. alle notwendigen Änderungen an der Regel vor, und vergewissern Sie sich, dass sie richtig kompiliert wird, bevor Sie sie aktivieren.

14. Klicken Sie auf "Aktivieren", um die überprüfte Richtlinie mit den neuen, hinzugefügten Regelaktionen zu verteilen.

15. Wiederholen Sie diesen Vorgang für alle Regeln und Richtlinien mit erfassten Ereignissen, die an CA Enterprise Log Manager gesendet werden sollen.

Weitere Informationen

Wissenswertes über den SAPI-Router und -Collector (siehe Seite 230)
Konfigurieren des SAPI-Collector-Service (siehe Seite 232)
Konfigurieren des SAPI-Router-Service (siehe Seite 232)

Ändern einer bestehenden r8 SP2-Richtlinie zum Senden von Ereignissen an CA Enterprise Log Manager

Gehen Sie wie unten beschrieben vor, um einen r8 SP2-CA Audit-Client so einzurichten, dass Ereignisse an CA Enterprise Log Manager *und* an die CA Audit-Collector-Datenbank gesendet werden. Indem Sie der Route- bzw. Collector-Aktion einer bestehenden Regel ein neues Ziel hinzufügen, können Sie erfasste Ereignisse an beide Systeme senden. Alternativ können Sie bestimmte Richtlinien bzw. Regeln auch so ändern, dass Ereignisse *nur* an den CA Enterprise Log Manager-Server gesendet werden.

Weitere Informationen zum Arbeiten mit Richtlinien finden Sie im *Implementierungshandbuch für CA Audit r8 SP2*. Dort finden Sie eine genaue Beschreibung der unten aufgeführten Schritte.

CA Enterprise Log Manager erfasst Ereignisse von CA Audit-Clients mit Hilfe des CA Audit-SAPI-Router- und des CA Audit-SAPI-Collector-Listeners. Erfasste Ereignisse werden im CA Enterprise Log Manager-Ereignisprotokollspeicher erst gespeichert, *nachdem* die Richtlinie auf die Clients übertragen und aktiviert wurde.

Wichtig: Sie müssen die CA Enterprise Log Manager-Listener für den Empfang von Ereignissen einrichten, bevor Sie die Richtlinie ändern und aktivieren. Falls Sie diese Konfiguration nicht zuerst vornehmen, können falsch zugeordnete Ereignisse auftreten, wenn Ereignisse vor dem Zeitpunkt, zu dem die Richtlinie in Kraft tritt und die Listener die Ereignisse richtig zuordnen können, eintreffen.

So ändern Sie die Aktion einer bestehenden r8 SP2-Richtlinienregel zum Senden von Ereignissen an CA Enterprise Log Manager:

1. Melden Sie sich beim Richtlinien-Manager-Server als Benutzer mit der Maker-Rolle an.
2. Greifen Sie auf die zu bearbeitende Regel zu, indem Sie den entsprechenden Ordner im Richtlinienfenster erweitern und die gewünschte Richtlinie auswählen.

   Die Richtlinie wird mit den zugehörigen Regeln im Detailfenster angezeigt.
3. Klicken Sie auf die Regel, die bearbeitet werden soll.

   Die Regel wird mit den zugehörigen Aktionen im Detailfenster angezeigt.

4. Klicken Sie auf "Bearbeiten".

   Der Assistent zum Bearbeiten von Regeln wird geöffnet.

5. Ändern Sie die Regel im Assistenten so, dass Ereignisse an den CA Enterprise Log Manager-Server gesendet werden, entweder zusätzlich zu den oder anstelle der derzeitigen Ziele. Klicken Sie abschließend auf "Fertig stellen".

6. Überprüfen Sie die Regel, und übernehmen Sie sie als Maker-Benutzer, so dass sie von einem Benutzer mit Checker-Rolle genehmigt werden kann.

7. Melden Sie sich ab, und melden Sie sich erneut beim Richtlinien-Manager-Server als Benutzer mit Checker-Rolle an, falls in Ihrem Unternehmen die Pflichtentrennung verwendet wird.

8. Überprüfen und genehmigen Sie den Richtlinienordner mit der geänderten Richtlinie und Regel.

   Nachdem die Richtlinie genehmigt wurde, wird durch die Einstellungen des Richtlinien-Manager-Verteilungsservers vorgegeben, wann die neue Richtlinie an die Audit-Knoten verteilt wird. Sie können den Aktivierungsstatus der Richtlinie im Aktivierungsprotokoll einsehen.

9. Wiederholen Sie diesen Vorgang für alle Regeln und Richtlinien mit erfassten Ereignissen, die an CA Enterprise Log Manager gesendet werden sollen.

Grund für den Import von Ereignissen

Falls Sie über einen CA Audit-Data-Tools-Server mit Collector-Datenbank verfügen, gibt es eine SEOSDATA-Tabelle mit Ereignisdaten. Um das CA Audit- und das CA Enterprise Log Manager-System nebeneinander auszuführen und Berichte zu bereits erfassten Daten anzuzeigen, können Sie Daten aus der SEOSDATA-Tabelle importieren.

Sie können mit dem SEOSDATA-Importhilfsprogramm Ereignisdaten aus der Collector-Datenbank in einen CA Enterprise Log Manager-Ereignisprotokollspeicher importieren. Im Allgemeinen werden Ereignisdaten sofort nach der Bereitstellung eines CA Enterprise Log Manager-Servers importiert. Falls Sie die beiden Systeme integrieren, können Sie die Daten je nach Verwendung und Netzwerkkonfiguration auch mehrmals importieren.

Hinweis: Durch den Import von Daten aus der SEOSDATA-Tabelle werden die dort gespeicherten Daten *nicht* gelöscht oder geändert. Beim Import werden die Daten kopiert, analysiert und im CA Enterprise Log Manager-Ereignisprotokollspeicher zugeordnet.

Wissenswertes über das SEOSDATA-Importhilfsprogramm

Das Importhilfsprogramm "LMSeosImport" verwendet eine Befehlszeilenschnittstelle und kann auf den Betriebssystemen Windows und Solaris ausgeführt werden. Das Hilfsprogramm führt folgende Aktionen durch:

- Herstellen einer Verbindung mit der SEOSDATA-Tabelle und Abrufen von Ereignissen in der festgelegten Form
- Analysieren der ausgewählten SEOSDATA-Ereignisse in Namen-Wert-Paaren
- Übermitteln der Ereignisse an den CA Enterprise Log Manager-Server über den SAPI-Ereignissponsor bzw. den iTech-Ereignissponsor und Einfügen der Ereignisse in den Ereignisprotokollspeicher

Die Ereignisse werden der ELM-Schemadefinition zugeordnet, die die Basis für die Datenbanktabellen des Ereignisprotokollspeichers bildet. Sie können dann anhand der vordefinierten Abfragen und Berichte Informationen aus den gespeicherten Ereignissen abrufen.

Importieren aus einer aktiven SEOSDATA-Tabelle

Die Verwendung des Hilfsprogramms "LMSeosImport" bei einer aktiven SEOSDATA-Tabelle ist zwar nicht empfehlenswert, gelegentlich jedoch unumgänglich. Falls Sie das Hilfsprogramm bei einer Online-Datenbank ausführen, wird nur ein bestimmter Teil der Daten importiert. Der Grund hierfür ist, dass Ereignisse, die der Datenbank hinzugefügt werden, *nachdem* das Hilfsprogramm "LMSeosImport" gestartet wurde, während dieser Importsitzung nicht importiert werden.

Falls Sie beispielsweise die Parameter "-minid" und "-maxid" nicht in der Befehlszeile angeben, werden beim Start des Hilfsprogramms in der Datenbank die erste und die letzte Eintrags-ID abgefragt. Das Hilfsprogramm führt die Abfragen und den Import dann anhand dieser Werte aus. Die Eintrags-IDs der Ereignisse, die nach dem Start des Hilfsprogramms in die Datenbank eingefügt werden, liegen außerhalb dieses Bereichs und werden daher nicht importiert.

Nach Abschluss der Importsitzung zeigt das Hilfsprogramm die letzte verarbeitete Eintrags-ID an. Eventuell müssen Sie mehrere Importsitzungen ausführen, um alle Ereignisse zu erfassen, oder Sie führen das Importhilfsprogramm zu einer Zeit mit wenig Netzwerk- und Ereignisaktivitäten aus. Sie können ggf. weitere Importsitzungen durchführen und dabei die letzte Eintrags-ID der vorherigen Sitzung als Wert für den Parameter "-minid" in der neuen Sitzung verwenden.

Importieren von Daten aus einer SEOSDATA-Tabelle

Gehen Sie beim Importieren von Daten aus einer Collector-Datenbank (SEOSDATA-Tabelle) wie unten beschrieben vor, um optimale Ergebnisse zu erzielen:

1. Kopieren Sie das Hilfsprogramm "LMSeosImport" in den iTechnology-Ordner auf einem CA Audit-Data-Tools-Server.

   Hinweis: Für das Hilfsprogramm "LMSeosImport" sind die unterstützenden Bibliotheken *etsapi* und *etbase* erforderlich, die mit dem CA Audit-Client bereitgestellt werden.

2. Machen Sie sich mit der LMSeosImport-Befehlszeile und den -Optionen vertraut.

3. Erstellen Sie einen Ereignisbericht, um Art und Anzahl der Ereignisse sowie die Eintrags-ID-Bereiche in Erfahrung zu bringen.

4. Zeigen Sie eine Vorschau der Importergebnisse für die Parameter an, die Sie zu verwenden gedenken.

   Sie können die Importvorschau auch mehrmals durchführen, um die Befehlszeilenoptionen zu optimieren.

5. Importieren Sie mit den optimierten Befehlszeilenoptionen Ereignisse aus einer Collector-Datenbank.

Kopieren des Hilfsprogramms für den Ereignisimport auf einen Solaris-Data-Tools-Server

Bevor Sie Daten aus der SEOSDATA-Tabelle importieren können, müssen Sie das Hilfsprogramm "LMSeosImport" von der CA Enterprise Log Manager-Anwendungsinstallations-DVD-ROM auf Ihren Solaris-Data-Tools-Server kopieren.

Hinweis: Für das Hilfsprogramm "LMSeosImport" müssen die Bibliotheken *etsapi* und *etbase* vorhanden sein. Diese Dateien gehören zum Umfang der Basisinstallation des Data-Tools-Servers. Vergewissern Sie sich vor der Verwendung des Hilfsprogramms "LMSeosImport", dass die PATH-Systemanweisung das CA Audit-Installationsverzeichnis enthält. Das Standardverzeichnis ist "opt/CA/eTrustAudit/bin".

Legen Sie die folgenden Umgebungsvariablen mit dem Befehl *env* fest, bevor Sie das Hilfsprogramm ausführen:

- ODBC_HOME=<*CA Audit-Data-Tools-Installationsverzeichnis*>/odbc
- ODBCINI=<*CA Audit-Data-Tools-Installationsverzeichnis*>/odbc/odbc.ini

So kopieren Sie das Hilfsprogramm:

1. Rufen Sie auf dem Solaris-Data-Tools-Server eine Eingabeaufforderung auf.
2. Legen Sie die CA Enterprise Log Manager-Anwendungsinstallations-DVD-ROM ein.
3. Navigieren Sie zu dem Verzeichnis "/CA/ELM/Solaris_sparc".
4. Kopieren Sie das Hilfsprogramm "LMSeosImport" in das iTechnology-Verzeichnis des CA Audit-Data-Tools-Servers "/opt/CA/SharedComponents/iTechnology".

   Sie können das Hilfsprogramm verwenden, sobald es in das vorgesehene Verzeichnis kopiert wurde und die erforderlichen Umgebungsvariablen festgelegt wurden. Eine eigene Installation ist nicht erforderlich.

Kopieren des Importhilfsprogramms auf einen Windows-Data-Tools-Server

Bevor Sie Daten aus der SEOSDATA-Tabelle importieren können, müssen Sie das Hilfsprogramm "LMSeosImport" von der CA Enterprise Log Manager-Anwendungsinstallations-DVD-ROM auf Ihren Windows-Data-Tools-Server kopieren.

Hinweis: Für das Hilfsprogramm "LMSeosImport" müssen die Dynamic Link Libraries *etsapi* und *etbase* vorhanden sein. Diese Dateien gehören zum Umfang der Basisinstallation des Data-Tools-Servers. Vergewissern Sie sich vor der Verwendung des Hilfsprogramms "LMSeosImport", dass die PATH-Systemanweisung das Verzeichnis "Programme\CA\eTrust Audit\bin" enthält.

So kopieren Sie das Hilfsprogramm:

1. Rufen Sie auf dem Windows-Data-Tools-Server eine Eingabeaufforderung auf.
2. Legen Sie die CA Enterprise Log Manager-Anwendungsinstallations-DVD-ROM ein.
3. Navigieren Sie zu dem Verzeichnis "\CA\ELM\Windows".
4. Kopieren Sie die Datei "LMSeosImport.exe" in das iTechnology-Verzeichnis des CA Audit-Data-Tools-Servers "<Laufwerk>:\Programme\CA\SharedComponents\iTechnology".

   Sie können das Hilfsprogramm verwenden, sobald es in das vorgesehene Verzeichnis kopiert wurde. Eine eigene Installation ist nicht erforderlich.

Wissenswertes über die LMSeosImport-Befehlszeile

Das Hilfsprogramm "LMSeosImport" verwendet eine Reihe von Befehlszeilenargumenten, mit denen Sie steuern können, welche Ereignisse migriert werden. Jedes Ereignis in der SEOSDATA-Tabelle steht in einer Zeile und weist eine eindeutige *Eintrags-ID* auf, mit der es identifiziert wird. Sie können mit dem Importhilfsprogramm einen Bericht abrufen, der diverse nützliche Informationen enthält. Der Bericht enthält die Anzahl der Ereignisse in der SEOSDATA-Tabelle (als Anzahl von Eintrags-IDs), die Ereignisanzahl pro Protokolltyp sowie die Zeiträume für die Ereignisse. Das Hilfsprogramm bietet zudem die Möglichkeit der Wiederholung, falls beim Import eines Ereignisses ein Fehler auftritt.

Ferner können Sie in einer Vorschau überprüfen, welche Importergebnisse eine bestimmte Befehlsstruktur erbringt. Bei der Vorschau werden keine Daten importiert. Hierdurch können Sie die Befehlszeilenoptionen vor der eigentlichen Migration optimieren.

Darüber hinaus kann das Migrationshilfsprogramm auch mehrmals mit unterschiedlichen Parametern ausgeführt werden, falls Sie verschiedene Arten von Daten importieren möchten. So können Sie Daten beispielsweise in mehreren eigens abgestimmten Sitzungen basierend auf einem Eintrags-ID-Bereich, der Protokollart oder bestimmten Zeiträumen migrieren.

Hinweis: Das Hilfsprogramm speichert *keine* Informationen zu vorangegangenen Importsitzungen. Daher kann es zu doppelten Daten in der CA Enterprise Log Manager-Datenbank kommen, falls Sie den Befehl mehrmals mit denselben Parametern ausführen.

Die besten Ergebnisse und die beste Importleistung erzielen Sie, wenn Sie den Import anhand der Protokollart (mit der Option "-log") oder anhand der Eintrags-ID (mit den Optionen "-minid" und "-maxid") aufteilen. Mit der Option "-retry" können Sie potenziellen Fehlern beim Ereignisimport begegnen. Das Hilfsprogramm verwendet einen Standardwert von 300 Sekunden für die Option "-retry", damit der Import möglichst erfolgreich ablaufen kann.

Hilfsprogramm für den Import – Befehlssyntax und Optionen

Das Hilfsprogramm "LMSeosImport" unterstützt die folgende Befehlszeilensyntax und die folgenden Optionen:

```
LMSeosImport -dsn DSN-Name -user Benutzername -password Kennwort -target Zielname
{-sid nnn -eid nnnn -stm jjjj-mm-tt -etm jjjj-mm-tt -log Protokollname -transport
(sapi|itech) -chunk nnnn -pretend -verbose -delay -report -retry}
```

-dsn

Gibt den Namen des Hostservers an, auf dem sich die SEOSDATA-Tabelle befindet. Dieser Parameter ist erforderlich.

-user

Gibt die gültige ID eines Benutzers an, der zumindest Lesezugriff auf die SEOSDATA-Tabelle hat. Dieser Parameter ist erforderlich.

-password

Gibt das Kennwort für das im Parameter "-user" festgelegte Benutzerkonto an. Dieser Parameter ist erforderlich.

-target

Gibt den Hostnamen oder die IP-Adresse des CA Enterprise Log Manager-Servers an, der die migrierten Ereignisse aus der SEOSDATA-Tabelle empfangen soll. Dieser Parameter ist erforderlich.

-minid nnnn

Gibt die erste ENTRYID für die Auswahl von Ereignissen in der SEOSDATA-Tabelle an. Dieser Parameter ist optional.

-maxid nnnn

Gibt die letzte ENTRYID für die Auswahl von Ereignissen in der SEOSDATA-Tabelle an. Dieser Parameter ist optional.

-mintm JJJJ-MM-TT

Gibt die Anfangszeit (im Format JJJJ-MM-TT) für die Auswahl von Ereignissen in der SEOSDATA-Tabelle an. Dieser Parameter ist optional.

-maxtm JJJJ-MM-TT

Gibt die Endezeit (im Format JJJJ-MM-TT) für die Auswahl von Ereignissen in der SEOSDATA-Tabelle an. Dieser Parameter ist optional.

-log Protokollname

Legt fest, dass das Hilfsprogramm nur Ereignisdatensätze mit dem angegebenen Protokollnamen auswählen soll. Dieser Parameter ist optional. Falls der Protokollname Leerzeichen enthält, muss er in Anführungszeichen eingeschlossen werden.

-transport <sapi | itech>

Legt fest, welche Transportmethode zwischen dem Hilfsprogramm für den Import und CA Enterprise Log Manager verwendet werden soll. Standardmäßig wird die Transportmethode "sapi" verwendet.

-chunk nnnn

Legt fest, wie viele Ereignisdatensätze pro Durchlauf in der SEOSDATA-Tabelle ausgewählt werden sollen. Der Standardwert ist 5000 Ereignisse (Zeilen). Dieser Parameter ist optional.

-preview

Gibt die Ergebnisse der Ereignisdatensatzauswahl in STDOUT aus, ohne dass die Daten tatsächlich importiert werden. Dieser Parameter ist optional.

-port

Gibt die zu verwendende Portnummer an, wenn Sie als Transportoption SAPI festlegen und der CA Enterprise Log Manager-SAPI-Router so eingerichtet wurde, dass ein fester Portwert (unter Umgehung des Portmappers) verwendet wird.

-verbose

Legt fest, dass vom Hilfsprogramm ausführliche Verarbeitungsmeldungen an STDOUT gesendet werden sollen. Dieser Parameter ist optional.

-delay

Legt in Sekunden fest, welche Pause zwischen der Verarbeitung der einzelnen Ereignisse eingelegt werden soll. Dieser Parameter ist optional.

-report

Zeigt einen Bericht zum Zeitraum, dem ENTRYID-Bereich und der Protokollanzahl in der SEOSDATA-Tabelle an. Dieser Parameter ist optional.

-retry

Legt den Gesamtzeitraum in Sekunden fest, in dem Wiederholungsversuche durchgeführt werden, wenn beim Importieren eines Ereignisses ein Fehler auftritt. Die Verarbeitung wird fortgesetzt, sobald dieses Ereignis erfolgreich gesendet wurde. Das Hilfsprogramm verwendet automatisch den Standardwert 300 Sekunden. Der Parameter muss nur eingegeben werden, falls Sie einen anderen Wert festlegen möchten. Meldungen zum Wiederholungsstatus werden an STDOUT gesendet.

Befehlszeilenbeispiele für das Hilfsprogramm "LMSeosImport"

Sie können mit Hilfe der folgenden Befehlszeilenbeispiele Ihren eigenen Befehl erstellen, wenn Sie das SEOSDATA-Importhilfsprogramm verwenden.

So importieren Sie die Datensätze zwischen den ENTRYIDs 1000 und 4000:

Geben Sie die folgende Befehlszeile ein:

```
LMSeosImport –dsn eAudit_DSN –user sa –password sa –target 130,200.137,192 –
minid 1000 –maxid 4000
```

So importieren Sie Datensätze ausschließlich für NT-Application-Ereignisse:

Geben Sie die folgende Befehlszeile ein:

```
LMSeosImport –dsn eAudit_DSN –user sa –password sa –target 130,200.137,192 –log NT-Application
```

Erstellen eines Ereignisberichts

Indem Sie vor dem eigentlichen Import von Daten einen SEOSDATA-Ereignisbericht erstellen, erhalten Sie die notwendigen Informationen über die Ereignisse in der Tabelle. Im Bericht werden der Ereigniszeitraum, die Ereignisanzahl pro Protokolltyp und der Eintrags-ID-Bereich angezeigt. Anhand der Werte im Bericht können Sie die Befehlszeilenoptionen für die Vorschau oder den eigentlichen Import optimieren.

So zeigen Sie einen Bericht mit aktuellen SEOSDATA-Ereignisinformationen auf Windows an:

1. Rufen Sie eine Befehlszeile auf dem CA Audit-Data-Tools-Server auf.
2. Navigieren Sie zu dem Verzeichnis "\Programme\CA\SharedComponents\iTechnology".
3. Geben Sie die folgende Befehlszeile ein:

   ```
   LMSeosImport –dsn eAudit_DSN –user sa –password sa -target <Log_Manager_Hostname> –report
   ```

Der erstellte Bericht sieht in etwa wie folgt aus:

```
SEOSProcessor::InitOdbc: successfully attached to source [eAudit_DSN]

---------- SEOSDATA Event Time Range ----------

Minimum TIME = 2007-08-27
Maximum TIME = 2007-10-06

---------- Event Count Per Log ----------

com.ca.iTechnology.iSponsor : 3052
EiamSdk : 1013
NT-Application : 776
NT-System : 900

---------- SEOSDATA EntryID Range ----------

Minimum ENTRYID : 1
Maximum ENTRYID : 5741

Report Completed.
```

Vorschau der Importergebnisse

Sie können einen Testimport mit Ausgabe an STDOUT durchführen, um eine Vorschau der Importergebnisse anzuzeigen, ohne die Daten tatsächlich zu importieren oder zu migrieren. Auf diese Weise können Sie die für eine einmalige Migration oder einen regelmäßig geplanten Batch-Import eingegebenen Befehlszeilenparameter überprüfen.

So führen Sie einen Testimport zur Vorschau der Importergebnisse durch:

1. Rufen Sie eine Befehlszeile auf dem CA Audit-Data-Tools-Server auf.
2. Navigieren Sie zum entsprechenden Verzeichnis:

   Solaris: /opt/CA/SharedComponents/iTechnology

   Windows: \Programme\CA\SharedComponents\iTechnology
3. Geben Sie die folgende Befehlszeile ein:

   Solaris:

   ```
   ./LMSeosImport.sh –dsn eAudit_DSN –user sa –password sa –target
   <Log_Manager_Hostname_oder_IP-Adresse> –minid 1000 –maxid 4000 -preview
   ```

   Windows:

   ```
   LMSeosImport.exe –dsn eAudit_DSN –user sa –password sa –target
   <Log_Manager_Hostname_oder_IP-Adresse> –minid 1000 –maxid 4000 -preview
   ```

Importieren von Ereignissen aus einer Windows-Collector-Datenbank

Sie können anhand der unten beschriebenen Vorgehensweise Ereignisdaten aus einer Collector-Datenbank, die sich auf einem Windows-Data-Tools-Server befindet, importieren.

So importieren Sie Ereignisse aus einer SEOSDATA-Tabelle auf einem Windows-Server:

1. Suchen Sie den Namen des Servers, auf dem sich die SEOSDATA-Tabelle befindet.
2. Vergewissern Sie sich, dass Sie sich mit den Anmeldedaten eines Benutzers bei diesem Server anmelden, die Ihnen zumindest Lesezugriff auf die SEOSDATA-Tabelle geben.
3. Rufen Sie eine Befehlszeile auf dem CA Audit-Data-Tools-Server auf.
4. Navigieren Sie zu dem Verzeichnis "\Programme\CA\SharedComponents\iTechnology".
5. Starten Sie das Importhilfsprogramm mit der folgenden Befehlssyntax:

   ```
   LMSeosImport.exe -dsn <DSN-Name> -user <Benutzer-ID> -password <Kennwort> -target <Zielhostname> <optionale Flags>
   ```

Importieren von Ereignissen aus einer Solaris-Collector-Datenbank

Sie können anhand der unten beschriebenen Vorgehensweise Ereignisdaten aus einer Collector-Datenbank, die sich auf einem Solaris-Data-Tools-Server befindet, importieren.

So importieren Sie Ereignisse aus einer SEOSDATA-Tabelle auf einem Solaris-Server:

1. Suchen Sie den Namen des Servers, auf dem sich die SEOSDATA-Tabelle befindet.
2. Vergewissern Sie sich, dass Sie sich mit den Anmeldedaten eines Benutzers bei diesem Server anmelden, die Ihnen zumindest Lesezugriff auf die SEOSDATA-Tabelle geben.
3. Rufen Sie eine Befehlszeile auf dem CA Audit-Data-Tools-Server auf.
4. Navigieren Sie zu dem Verzeichnis "/opt/CA/SharedComponents/iTechnology".
5. Starten Sie das Importhilfsprogramm mit der folgenden Befehlssyntax:

   ```
   ./LMSeosImport -dsn <DSN-Name> -user <Benutzer-ID> -password <Kennwort> -target <Zielhostname> <optionale Flags>
   ```

Anhang B: Aspekte für CA Access Control-Benutzer

Dieses Kapitel enthält folgende Themen:

Integration mit CA Access Control

Sie können CA Enterprise Log Manager in verschiedene Release-Versionen von CA Access Control integrieren. Dabei gilt die folgende allgemeine Vorgehensweise:

Bei CA Access Control-Versionen mit einem TIBCO-Nachrichtenserver für das Weiterleiten von Ereignissen gehen Sie wie folgt vor:

- Installieren Sie einen CA Enterprise Log Manager-Agenten.
- Konfigurieren Sie einen Connector, der den Connector AccessControl_R12SP1_TIBCO_Connector verwendet.

Informationen zu CA Access Control r12.5 finden Sie im *CA Access Control r12.5-Implementierungshandbuch* und dem *CA Enterprise Log Manager CA Access Control-Connector-Handbuch*.

Informationen zu CA Access Control r12. SP1 finden Sie im *CA Access Control r12 SP1-Implementierungshandbuch, 3. Edition* und dem *CA Enterprise Log Manager-Connector-Handbuch für CA Access Control*.

Hinweis: Diese Implementierungen verwenden Komponenten, die Teil der CA Access Control Premium Edition sind.

Bei CA Access Control-Versionen mit selogrd für das Weiterleiten von Ereignissen gehen Sie wie folgt vor:

- Installieren Sie einen CA Enterprise Log Manager-Agenten.
- Konfigurieren Sie einen Connector, der die ACSelogrd-Integration verwendet.

Weitere Informationen zum Konfigurieren eines Connectors zum Erfassen von CA Access Control-Ereignissen finden Sie im *CA Access Control r8 SP1-Connector-Handbuch*.

Falls Sie zurzeit CA Access Control-Ereignisse an CA Audit senden, verwenden Sie folgende Methoden, um Ereignisse an CA Enterprise Log Manager zu übertragen:

- Ändern Sie eine bestehende CA Audit-Richtlinie so, dass Ereignisse sowohl an CA Audit als auch an CA Enterprise Log Manager gesendet werden, sofern Sie zum Erfassen von Ereignissen einen CA Audit-iRecorder verwenden. Sie können die Richtlinie bei Bedarf auch so ändern, dass Ereignisse nur an den CA Enterprise Log Manager-Server gesendet werden.
- Konfigurieren Sie die Datei control.conf für einen iRecorder, um die Ereignisse direkt an CA Enterprise Log Manager zu senden.

Hinweis: Falls Sie mit einer Version von eTrust Access Control arbeiten, die keine iRecorder unterstützt, können Sie Ereignisse direkt an den CA Audit-Router senden. Weitere Informationen finden Sie im Abschnitt zur CA Audit-Integration im *Administrationshandbuch für eTrust Access Control r5.3*.

Die nachfolgenden Richtlinien verwenden die r8 SP2-Serie für die Benutzerschnittstelle des Richtlinien-Managers. Die allgemeine Vorgehensweise ist bei früheren CA Audit-Versionen identisch, obwohl die Benutzerschnittstelle unterschiedlich ist.

Ändern von CA Audit-Richtlinien zum Senden von Ereignissen an CA Enterprise Log Manager

Die Änderung einer bestehenden CA Audit-Richtlinie zum Senden von Ereignissen an CA Enterprise Log Manager umfasst die folgenden Schritte:

- Stellen Sie sicher, dass folgende Punkte erfüllt sind:
  - Vergewissern Sie sich, dass Ihre Anmeldedaten für den CA Audit-Richtlinien-Manager Ihnen die Berechtigung zum Erstellen, Überprüfen und Aktivieren von Richtlinien verleihen.
  - Besorgen Sie sich die zum Zugriff auf die Benutzeroberfläche von Audit-Administrator erforderliche IP-Adresse bzw. den erforderlichen Hostnamen. Die URL zum Zugriff auf die Webanwendung des Richtlinien-Manager-Servers der R8 SP2-Serie hat folgendes Format:

    `https://<IP_Adresse_des_CA Audit_RMs>:5250/spin/auditadmin`
- Konfigurieren Sie den CA Enterprise Log Manager-SAPI-Collector-Service bzw. SAPI-Router-Service, je nachdem, wie Sie die Regelaktion erstellen möchten.

  Falls Sie eine Collector-Aktion erstellen möchten, konfigurieren Sie den SAPI-Collector. Falls Sie eine Route-Aktion einrichten möchten, konfigurieren Sie den SAPI-Router.

  Hinweis: Im Beispiel dieses Abschnitts wird die Collector-Aktion verwendet.
- Ändern Sie eine bestehende CA Access Control-Richtlinie so, dass Ereignisse an CA Enterprise Log Manager gesendet werden.
- Überprüfen und aktivieren Sie die geänderte Richtlinie, so dass Sie an die Überwachungsknoten verteilt werden kann.

Wiederholen Sie diese Schritte, um ggf. neue Regelaktionen zu weiteren Richtlinienregeln hinzuzufügen.

Weitere Informationen

Wissenswertes über den SAPI-Router und -Collector (siehe Seite 230)

Konfigurieren des SAPI-Collector-Adapters für den Empfang von CA Access Control-Ereignissen

Gehen Sie wie unten beschrieben vor, um den SAPI-Collector-Adapter für den Empfang von CA Access Control-Ereignissen aus einer CA Audit-Implementierung einzurichten.

Sie können CA Audit-Richtlinien ändern, die Ereignisse mit Hilfe von Collector-Aktionen an einen CA Enterprise Log Manager-Server senden, wobei der CA Enterprise Log Manager-Server zusätzlich zur oder anstelle der CA Audit-Collector-Datenbank verwendet werden kann. Konfigurieren Sie diesen Service, *bevor* Sie die CA Audit-Richtlinien ändern, damit keine Ereignisse verloren gehen.

(Der SAPI-Router-Service wird auf ähnliche Weise konfiguriert. Falls Sie den Router- und den Collector-Service verwenden, vergewissern Sie sich, dass die aufgeführten Ports unterschiedlich sind oder vom Portmapper-Service gesteuert werden.)

So konfigurieren Sie den SAPI-Collector-Service:

1. Melden Sie sich beim CA Enterprise Log Manager-Server als Administrator an, und wählen Sie die Registerkarte "Verwaltung" aus.

   Die untergeordnete Registerkarte "Protokollerfassung" wird standardmäßig angezeigt.

2. Erweitern Sie den Eintrag "CA-Adapter".

3. Wählen Sie den SAPI-Collector-Service aus.

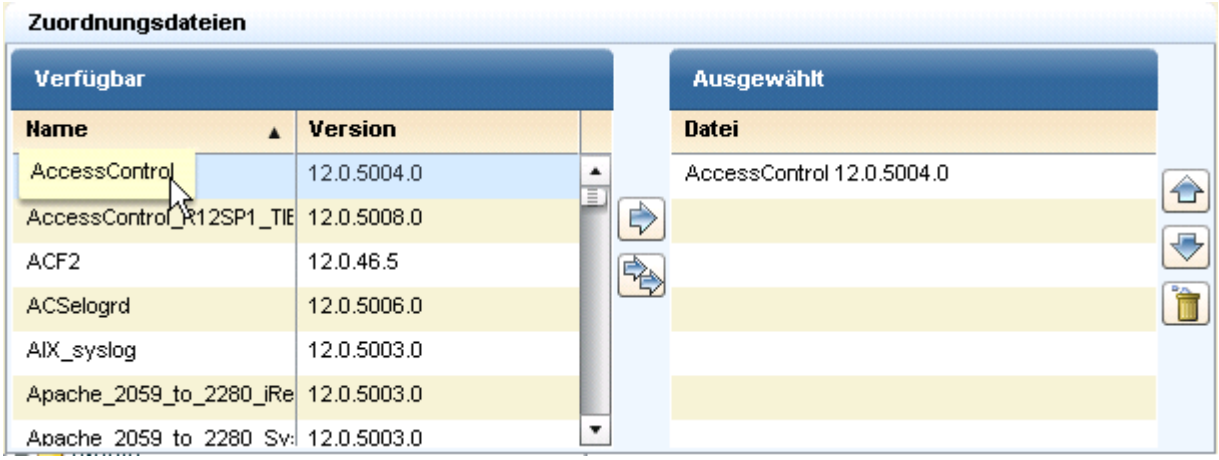
4. Aktivieren Sie das Kontrollkästchen "Listener aktivieren", und legen Sie als Wert für "Sapi-Port" einen Wert fest, der mit dem von CA Audit verwendeten Wert übereinstimmt.

   Der Standard-CA Enterprise Log Manager-Wert 0 ordnet Ports mit dem Portmap-Dienst zu. Falls Sie in CA Audit einen Port definiert haben, verwenden Sie die Einstellung an dieser Stelle.

5. Übernehmen Sie die Standardwerte für die übrigen Felder, und blättern Sie zur Liste der Zuordnungsdateien.

   Wenn Sie das Kontrollkästchen "Registrieren" aktivieren, geben Sie einen Wert für den SAPI-Port an.

6. Fügen Sie die "AccessControl"-Zuordnungsdatei hinzu, sofern noch nicht geschehen, und entfernen Sie alle anderen Zuordnungsdateien aus der Liste der ausgewählten Zuordnungsdateien.



7. Klicken Sie auf "Speichern".

Ändern einer bestehenden CA Audit-Richtlinie zum Senden von Ereignissen an CA Enterprise Log Manager

Gehen Sie wie unten beschrieben vor, um einen CA Audit-Client so einzurichten, dass Ereignisse an CA Enterprise Log Manager *und* an die CA Audit-Collector-Datenbank gesendet werden. Indem Sie der Route- bzw. Collector-Aktion einer bestehenden Regel ein neues Ziel hinzufügen, können Sie erfasste Ereignisse an beide Systeme senden. Alternativ können Sie bestimmte Richtlinien bzw. Regeln auch so ändern, dass Ereignisse *nur* an den CA Enterprise Log Manager-Server gesendet werden.

CA Enterprise Log Manager erfasst Ereignisse von CA Audit-Clients mit Hilfe des CA Audit-SAPI-Router- und des CA Audit-SAPI-Collector-Listeners. (CA Enterprise Log Manager kann Ereignisse auch direkt über das iTech-Plugin erfassen, falls Sie iRecorder für den direkten Versand zum CA Enterprise Log Manager-Server konfiguriert haben.) Erfasste Ereignisse werden nur im CA Enterprise Log Manager-Ereignisprotokollspeicher gespeichert, *nachdem* Sie die Richtlinie an die Clients weitergegeben haben und diese aktiv wird.

Wichtig: Richten Sie die CA Enterprise Log Manager-Listener für den Empfang von Ereignissen ein, bevor Sie die Richtlinie ändern und aktivieren. Falls Sie diese Konfiguration nicht zuerst vornehmen, können falsch zugeordnete Ereignisse auftreten, wenn Ereignisse vor dem Zeitpunkt eintreffen, an dem die Richtlinie in Kraft tritt und die Listener die Ereignisse richtig zuordnen können.

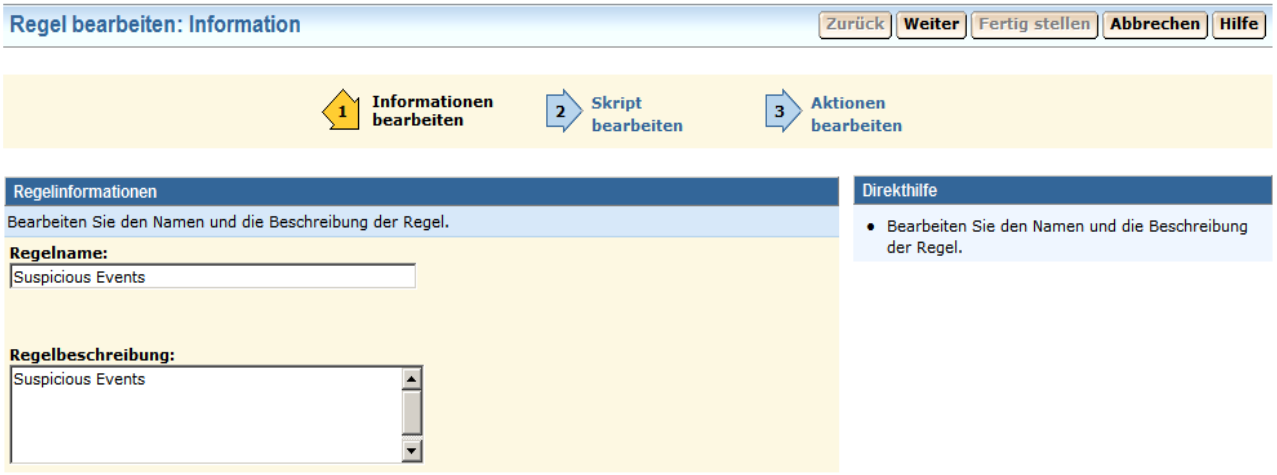
So ändern Sie die Aktion einer bestehenden Richtlinienregel zum Senden von Ereignissen an CA Enterprise Log Manager:

1. Melden Sie sich beim Richtlinien-Manager-Server an, und greifen Sie links im Fenster auf die Registerkarte "Meine Richtlinien" zu.
2. Erweitern Sie den Richtlinienordner, bis die gewünschte Richtlinie angezeigt wird.

3. Klicken Sie auf die Richtlinie, damit die grundlegenden Informationen im Detailabschnitt rechts im Fenster angezeigt werden.

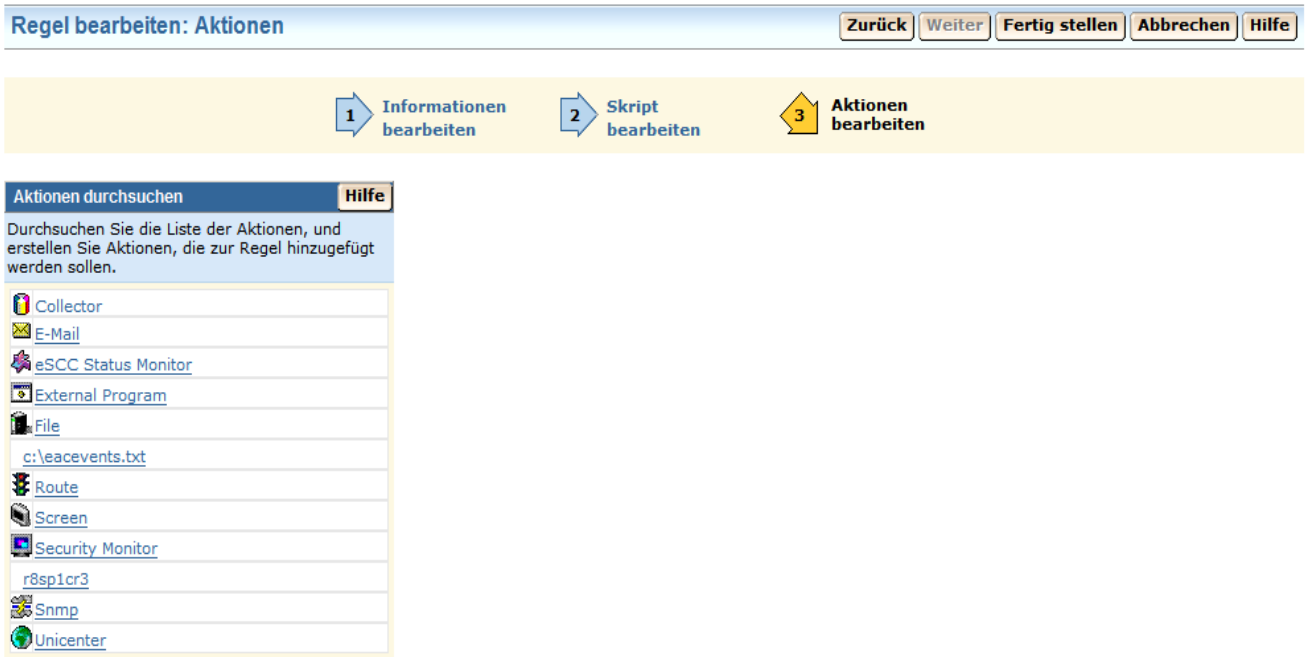
4. Klicken Sie im Bereich "Details" auf "Bearbeiten", um die Richtlinienregeln hinzuzufügen.

   Der Regelassistent wird gestartet:

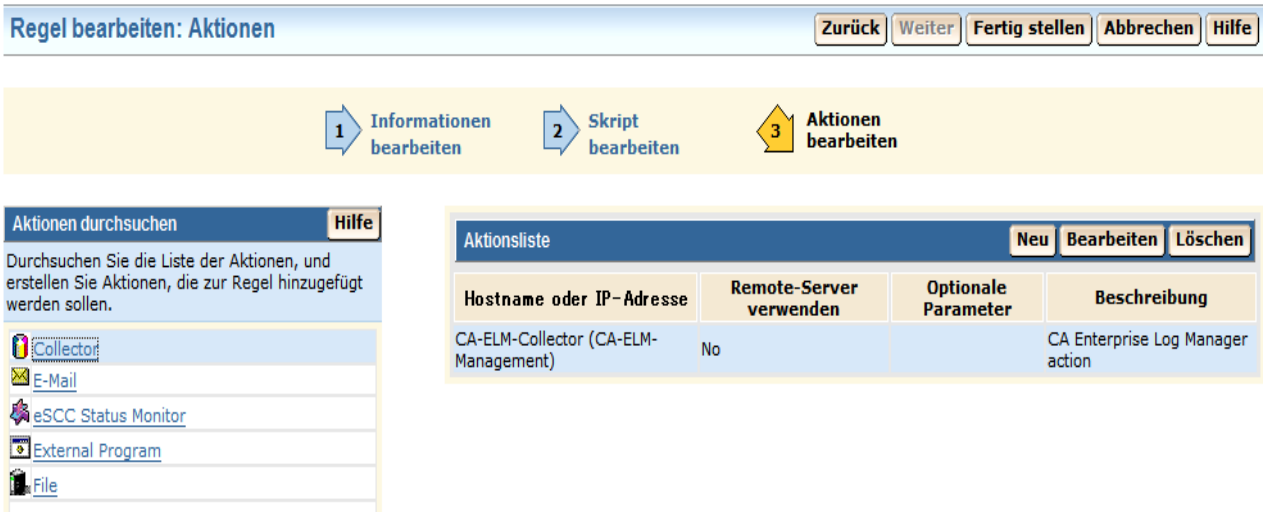


5. Klicken Sie auf "Aktionen bearbeiten" neben dem Pfeil für Schritt 3.

   Die Seite mit den Regelaktionen wird angezeigt:

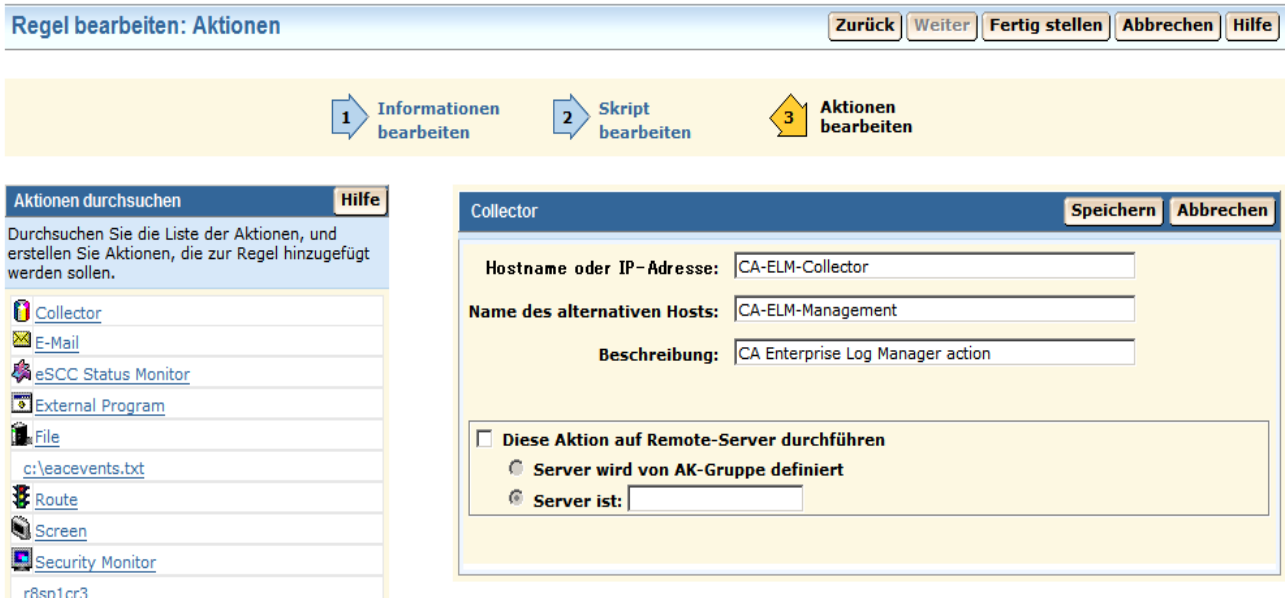


6. Klicken Sie im Fenster "Aktionen durchsuchen" auf die Aktion "Collector", um die Aktionsliste auf der rechten Seite anzuzeigen.



Sie können auch die Route-Aktion verwenden. Die Collector-Aktion bietet jedoch den Vorteil, dass zusätzlich ein alternativer Hostname für eine einfache Failover-Verarbeitung angegeben werden kann.

7. Klicken Sie auf "Neu", um eine neue Regel hinzuzufügen.
8. Geben Sie die IP-Adresse bzw. den Hostnamen des CA Enterprise Log Manager-Quellservers für Protokolldateien ein.



Bei CA Enterprise Log Manager-Implementierungen mit zwei oder mehr Servern können Sie im Feld für den alternativen Hostnamen einen anderen CA Enterprise Log Manager-Hostnamen bzw. eine andere IP-Adresse eingeben. Dadurch wird die CA Audit-Funktion des automatischen Failovers genutzt. Falls der erste CA Enterprise Log Manager-Server nicht verfügbar ist, sendet CA Audit automatisch Ereignisse an den im Feld "Alternativer Hostname" benannten Server.

9. Geben Sie im Feld "Alternativer Hostname" den Namen des CA Enterprise Log Manager-Verwaltungsservers ein, und erstellen Sie eine Beschreibung für die neue Regelaktion.
10. Deaktivieren Sie das Kontrollkästchen "Diese Aktion auf Remote-Server durchführen", falls es aktiviert ist.
11. Klicken Sie auf "Hinzufügen", um die neue Regelaktion zu speichern, und klicken Sie dann im Assistentenfenster auf "Fertig stellen".

    Hinweis: Als Nächstes überprüfen und aktivieren Sie die Richtlinie, melden Sie sich daher *nicht* vom CA Audit-Richtlinien-Manager ab.

Weitere Informationen

Ändern einer bestehenden r8 SP2-Richtlinie zum Senden von Ereignissen an CA Enterprise Log Manager (siehe Seite 238)

Überprüfen und Aktivieren der geänderten Richtlinie

Nachdem Sie eine bestehende Richtlinie geändert und eine Regelaktion hinzugefügt haben, überprüfen (kompilieren) und aktivieren Sie die Richtlinie.

So überprüfen und aktivieren Sie eine CA Access Control-Richtlinie:

1. Wählen Sie unten rechts die Registerkarte "Regeln" aus, und wählen Sie dann die zu überprüfende Regel aus.

2. Klicken Sie auf "Richtlinien überprüfen", um die geänderte Regel mit den neuen Aktionen zu überprüfen und sicherzustellen, dass sie richtig kompiliert wird.

   Nehmen Sie ggf. alle notwendigen Änderungen an der Regel vor, und vergewissern Sie sich, dass sie richtig kompiliert wird, bevor Sie sie aktivieren.

3. Klicken Sie auf "Aktivieren", um die überprüfte Richtlinie mit den neuen, hinzugefügten Regelaktionen zu verteilen.

4. Wiederholen Sie diesen Vorgang für alle Regeln und Richtlinien mit erfassten Ereignissen, die an CA Enterprise Log Manager gesendet werden sollen.

Konfigurieren eines CA Access Control-iRecorders zum Senden von Ereignissen an CA Enterprise Log Manager

Sie können einen eigenständigen CA Access Control-iRecorder so konfigurieren, dass die erfassten Ereignisse direkt zur Speicherung und Berichterstellung an den CA Enterprise Log Manager-Server gesendet werden. Der Vorgang umfasst folgende Schritte:

1. Konfigurieren Sie den Listener für das iTech-Ereignis-Plugin so, dass er Daten von einem CA Access Control-iRecorder empfängt.

2. Laden Sie einen CA Access Control-iRecorder herunter, und installieren Sie ihn.

3. Konfigurieren Sie den iRecorder so, dass die erfassten Ereignisse direkt an CA Enterprise Log Manager gesendet werden.

4. Überprüfen Sie, ob CA Enterprise Log Manager Ereignisse empfängt.

Hinweis: iRecorder können Ereignisse nur an ein Ziel senden. Wenn Sie die Konfiguration wie hier beschrieben vornehmen, ist der benannte CA Enterprise Log Manager-Server das einzige Ziel.

Konfigurieren des iTech-Ereignis-Plugins für CA Access Control-Ereignisse

Bevor Sie einen iRecorder so einrichten, dass Ereignisse direkt an CA Enterprise Log Manager gesendet werden, müssen Sie einen Listener für den Empfang dieser Ereignisse konfigurieren.

So konfigurieren Sie den Listener:

1. Melden Sie sich als Benutzer mit Administratorrolle beim CA Enterprise Log Manager-Server an.
2. Klicken Sie auf die Registerkarte "Verwaltung", und erweitern Sie den Knoten "CA-Adapter".

3. Erweitern Sie den Knoten für das iTechnology-Ereignis-Plugin.
4. Wählen Sie den aktuellen CA Enterprise Log Manager-Server aus, um die lokalen Einstellungen anzuzeigen.
5. Vergewissern Sie sich, dass die "AccessControl"-Zuordnungsdatei ganz oben in der Liste der ausgewählten Zuordnungsdateien steht, damit ein optimaler Betrieb gewährleistet ist.
6. Vergewissern Sie sich, dass der Wert für die Protokollebene auf NOTSET eingestellt ist, damit alle Ereignisebenen erfasst werden.
7. Klicken Sie auf "Speichern".

Herunterladen und Installieren eines CA Access Control-iRecorders

Sie können CA Access Control-Ereignisse erfassen und an einen CA Enterprise Log Manager-Server senden, auch wenn CA Audit nicht installiert ist. Wenn Sie Ereignisse auf diese Weise erfassen, verwenden Sie einen eigenständigen iRecorder. Den iRecorder erhalten Sie auf der CA-Support-Website.

Hinweis: iRecorder werden nur mit CA Access Control ab Release 8 unterstützt.

So können Sie einen iRecorder herunterladen und installieren:

1. Rufen Sie die folgende CA-Website auf:

   `https://support.ca.com/irj/portal/anonymous/phpdocs?filePath=0/154/cacirecr8-certmatrix.html#caacirec`

2. Wählen Sie den geeigneten iRecorder für Ihre CA Access Control-Version aus.
3. Folgen Sie den Installationsanleitungen, die Sie über den Link "Integration Guide" in der Matrix aufrufen können.

Konfigurieren eines eigenständigen CA Access Control-iRecorders

Gehen Sie wie unten beschrieben vor, um den iRecorder so zu konfigurieren, dass CA Access Control-Ereignisse an CA Enterprise Log Manager gesendet werden.

Wichtig! Ein eigenständiger iRecorder kann Ereignisse nur an ein Ziel senden. Wenn Sie einen iRecorder auf die unten beschriebene Weise konfigurieren, senden alle auf diesem System installierten iRecorder ihre Ereignisse *ausschließlich* an den benannten CA Enterprise Log Manager-Ereignisprotokollspeicher.

iRecorder, die auf demselben Computer installiert sind wie ein CA Audit-Client, senden Ereignisse direkt an den Client. Bei diesen Servern sollten Sie eine bestehende CA Audit-Richtlinie ändern und Regelaktionen hinzufügen, nachdem Sie den CA Enterprise Log Manager-SAPI-Collector- bzw. -Router-Adapter konfiguriert haben.

So konfigurieren Sie den iRecorder zum Senden von Ereignissen an CA Enterprise Log Manager:

1. Melden Sie sich beim Hostserver des iRecorders als Benutzer mit Administratorrechten bzw. mit "root"-Berechtigungen an.
2. Navigieren Sie zu folgendem Verzeichnis auf Ihrem Betriebssystem:
   - UNIX oder Linux: /opt/CA/SharedComponents/iTechnology
   - Windows: \Programme\CA\SharedComponents\iTechnology

3. Stoppen Sie den iGateway-Daemon bzw. -Service mit folgendem Befehl:
   - UNIX oder Linux: ./S99igateway stop
   - Windows: net stop igateway
4. Bearbeiten Sie die Datei "iControl.conf".

   Im Folgenden finden Sie ein Beispiel für eine iControl-Datei, wobei die erforderlichen Abschnitte fett gedruckt dargestellt sind:

```
<?xml version='1.0' encoding='UTF-8' standalone='no'?>
<iSponsor>
    <Name>iControl</Name>
    <ImageName>iControl</ImageName>
    <Version>4.5.0.2</Version>
    <DispatchEP>iDispatch</DispatchEP>
    <ISType>DSP</ISType>
    <Gated>false</Gated>
    <PreLoad>true</PreLoad>
    <RouteEvent>false</RouteEvent>
    <RouteEventHost>localhost</RouteEventHost>
    <EventsToCache>100</EventsToCache>
    <EventUseHttps>true</EventUseHttps>
    <EventUsePersistentConnections>true</EventUsePersistentConnections>
    <EventUsePipeline>false</EventUsePipeline>
    <StoreEventHost max="10000">localhost</StoreEventHost>
    <RetrieveEventHost interval="60">localhost</RetrieveEventHost>
    <UID>ef1f44ef-r8sp1cr3596a1052-abcd28-2</UID>
    <PublicKey>Wert_des_öffentlichen_Schlüssels</PublicKey>
    <PrivateKey>Wert_des_privaten_Schlüssels</PrivateKey>
    <EventsToQueue>10</EventsToQueue>
</iSponsor>
```

5. Geben Sie den folgenden Wert für "RouteEvent" an:

   ```
   <RouteEvent>true</RouteEvent>
   ```

   Mit diesem Eintrag wird iGateway angewiesen, alle Ereignisse, einschließlich aller iRecorder-Ereignisse, an den im Tag-Paar "RouteEventHost" angegebenen Host zu senden.

6. Geben Sie den folgenden Wert für "RouteEventHost" an:

   ```
   <RouteEventHost>Hostname_Ihrer_CA_Enterprise_Log_Manager_Anwendung</RouteEventHost>
   ```

   Mit diesem Eintrag wird iGateway angewiesen, Ereignisse an den CA Enterprise Log Manager-Server zu senden, der seinen DNS-Namen verwendet.

7. Speichern und schließen Sie die Datei.
8. Starten Sie den iGateway-Daemon bzw. -Service mit folgendem Befehl:
   - UNIX oder Linux: ./S99igateway start
   - Windows: net start igateway

   Mit dieser Aktion werden die neuen Einstellungen im iRecorder aktiviert. Ereignisse fließen jetzt vom iRecorder zum CA Enterprise Log Manager-Server.

Importieren von CA Access Control-Ereignissen aus einer CA Audit-Collector-Datenbank

Gehen Sie wie folgt vor, um CA Access Control-Ereignisse aus einer bestehenden SEOSDATA-Tabelle zu importieren:

1. Kopieren Sie das Hilfsprogramm "LMSeosImport" auf den CA Audit-Data-Tools-Server.
2. Erstellen Sie einen Ereignisbericht, um herauszufinden, ob die Datenbank CA Access Control-Ereignisse enthält.
3. Zeigen Sie eine Vorschau des Imports mit CA Access Control-spezifischen Parametern an.
4. Importieren Sie die CA Access Control-Ereignisse.
5. Führen Sie CA Enterprise Log Manager-Abfragen für die importieren Ereignisse aus, und erstellen Sie Berichte.

Voraussetzungen für den Import von CA Access Control-Ereignissen

Führen Sie folgende Schritte durch, bevor Sie das Hilfsprogramm "LMSeosImport" verwenden:

- Besorgen Sie sich ein Datenbankbenutzerkonto, das mindestens über Lesezugriff auf die CA Audit-SEOSDATA-Tabelle verfügt.
- Kopieren Sie das Hilfsprogramm "LMSeosImport" auf den CA Audit-Data-Tools-Server.
- Rufen Sie auf dem Data-Tools-Server eine Eingabeaufforderung auf, und navigieren Sie zu dem entsprechenden Verzeichnis:

  Solaris: /opt/CA/SharedComponents/iTechnology

  Windows: \Programme\CA\SharedComponents\iTechnology

Kopieren des Importhilfsprogramms auf einen Windows-Data-Tools-Server

Bevor Sie Daten aus der SEOSDATA-Tabelle importieren können, müssen Sie das Hilfsprogramm "LMSeosImport" von der CA Enterprise Log Manager-Anwendungsinstallations-DVD-ROM auf Ihren Windows-Data-Tools-Server kopieren.

Hinweis: Für das Hilfsprogramm "LMSeosImport" müssen die Dynamic Link Libraries *etsapi* und *etbase* vorhanden sein. Diese Dateien gehören zum Umfang der Basisinstallation des Data-Tools-Servers. Vergewissern Sie sich vor der Verwendung des Hilfsprogramms "LMSeosImport", dass die PATH-Systemanweisung das Verzeichnis "Programme\CA\eTrust Audit\bin" enthält.

So kopieren Sie das Hilfsprogramm:

1. Rufen Sie auf dem Windows-Data-Tools-Server eine Eingabeaufforderung auf.
2. Legen Sie die CA Enterprise Log Manager-Anwendungsinstallations-DVD-ROM ein.
3. Navigieren Sie zu dem Verzeichnis "\CA\ELM\Windows".
4. Kopieren Sie die Datei "LMSeosImport.exe" in das iTechnology-Verzeichnis des CA Audit-Data-Tools-Servers "<Laufwerk>:\Programme\CA\SharedComponents\iTechnology".

   Sie können das Hilfsprogramm verwenden, sobald es in das vorgesehene Verzeichnis kopiert wurde. Eine eigene Installation ist nicht erforderlich.

Kopieren des Hilfsprogramms für den Ereignisimport auf einen Solaris-Data-Tools-Server

Bevor Sie Daten aus der SEOSDATA-Tabelle importieren können, müssen Sie das Hilfsprogramm "LMSeosImport" von der CA Enterprise Log Manager-Anwendungsinstallations-DVD-ROM auf Ihren Solaris-Data-Tools-Server kopieren.

Hinweis: Für das Hilfsprogramm "LMSeosImport" müssen die Bibliotheken *etsapi* und *etbase* vorhanden sein. Diese Dateien gehören zum Umfang der Basisinstallation des Data-Tools-Servers. Vergewissern Sie sich vor der Verwendung des Hilfsprogramms "LMSeosImport", dass die PATH-Systemanweisung das CA Audit-Installationsverzeichnis enthält. Das Standardverzeichnis ist "opt/CA/eTrustAudit/bin".

Legen Sie die folgenden Umgebungsvariablen mit dem Befehl *env* fest, bevor Sie das Hilfsprogramm ausführen:

- ODBC_HOME=<*CA Audit-Data-Tools-Installationsverzeichnis*>/odbc
- ODBCINI=<*CA Audit-Data-Tools-Installationsverzeichnis*>/odbc/odbc.ini

So kopieren Sie das Hilfsprogramm:

1. Rufen Sie auf dem Solaris-Data-Tools-Server eine Eingabeaufforderung auf.
2. Legen Sie die CA Enterprise Log Manager-Anwendungsinstallations-DVD-ROM ein.
3. Navigieren Sie zu dem Verzeichnis "/CA/ELM/Solaris_sparc".
4. Kopieren Sie das Hilfsprogramm "LMSeosImport" in das iTechnology-Verzeichnis des CA Audit-Data-Tools-Servers "/opt/CA/SharedComponents/iTechnology".

   Sie können das Hilfsprogramm verwenden, sobald es in das vorgesehene Verzeichnis kopiert wurde und die erforderlichen Umgebungsvariablen festgelegt wurden. Eine eigene Installation ist nicht erforderlich.

Erstellen eines SEOSDATA-Ereignisberichts für CA Access Control-Ereignisse

Erstellen Sie einen Ereignisbericht, um herauszufinden, ob eine bestehende SEOSDATA-Tabelle CA Access Control-Ereignisse enthält, und um eine Importmethode auszuwählen. Der Protokollname für CA Access Control-Ereignisse lautet *eTrust Access Control*. Im Bericht werden alle Ereignisse in der Datenbank getrennt nach Protokollname aufgeführt. Am einfachsten lassen sich CA Access Control-Ereignisse anhand ihres Protokollnamens importieren.

So erstellen Sie einen Ereignisbericht:

1. Erstellen Sie einen Ereignisbericht, so dass Sie feststellen können, welche CA Access Control-Ereignisse in der SEOSDATA-Tabelle enthalten sind.

   ```
   LMSeosImport –dsn My_Audit_DSN –user sa –password sa –report
   ```

   Nach der Verarbeitung wird ein Bericht ähnlich dem folgenden angezeigt:

   ```
   Import started on Fri Jan  2 15:20:30 2009


   No transport specified, defaulting to SAPI...

   Preparing ODBC connections...

   Successfully attached to source [My_Audit_DSN]

   ---------- SEOSDATA Event Time Range ----------

   Minimum TIME = 2008-05-27
   Maximum TIME = 2009-01-02
   ```

```
---------- Event Count Per Log ----------

Unix : 12804
ACF2 : 1483
eTrust AC : 143762
com.ca.iTechnology.iSponsor : 66456
NT-Application : 5270
CISCO PIX Firewall : 5329
MS IIS : 6765
Netscape : 530
RACF : 14
Apache : 401
N/A : 28222
SNMP-recorder : 456
Check Point FW-1 : 1057
EiamSdk : 2790
MS ISA : 609
ORACLE : 2742
eTrust PCM : 247
NT-System : 680
eTrust Audit : 513
NT-Security : 14714
CISCO Device : 41436
SNORT : 1089

---------- SEOSDATA EntryID Range ----------

Minimum ENTRYID : 1
Maximum ENTRYID : 10000010243

Report Completed.

Successfully detached from source [My_Audit_DSN]

Exiting Import...
```

2. Überprüfen Sie den Bericht, um sicherzustellen, dass CA Access Control-Ereignisse vorhanden sind.

   Die fett gedruckte Zeile in diesem Bericht zeigt, dass diese SEOSDATA-Tabelle CA Access Control-Ereignisse enthält.

```
---------- Event Count Per Log ----------

Unix : 12804
ACF2 : 1483
eTrust AC : 143762
com.ca.iTechnology.iSponsor : 66456
NT-Application : 5270
...
```

Vorschau eines CA Access Control-Ereignisimports

Sie können mit der Importvorschau die Importparameter optimieren. Das folgende Beispiel zeigt zwei Vorschauergebnisse für den Import von Ereignissen in einem bestimmten Zeitraum. Im Beispiel wird Folgendes vorausgesetzt:

- Der CA Audit-Data-Tools-Server befindet sich auf einem Windows-Computer.
- Der Datenbankname für die SEOSDATA-Tabelle lautet "My_Audit_DSN".
- Der Name des Datenbankbenutzers und das zugehörige Kennwort lauten beide "sa".
- In der Importvorschau wird lediglich der Protokollname als Such- und Importkriterium verwendet.

Die Ausgabe des Befehls mit der Option "-preview" sendet Beispielimportergebnisse an STDOUT. (In diesem Beispiel wird der Wert *My_CA-ELM_Server* für den Namen des CA Enterprise Log Manager-Servers verwendet.)

So zeigen Sie eine Vorschau des Imports an:

1. Zeigen Sie eine Vorschau des CA Access Control-Ereignisimports mit dem folgenden Befehl an:

   ```
   LMSeosImport.exe –dsn My_Audit_DSN –user sa –password sa -target My_CA-ELM_Server –log "eTrust Access Control" -preview
   ```

   Mit dem Befehl "-preview" werden Daten ähnlich der folgenden angezeigt:

   ```
   Import started on Fri Jan  2 15:35:37 2009


   No transport specified, defaulting to SAPI...

   Preparing ODBC connections...

   Successfully attached to source [My_Audit_DSN]

   No starting ENTRYID specified, using minimum ENTRYID of 1...

   Import (preview) running, please wait...

   .........

   Import (preview) Completed (143762 records in 4 minutes 12 seconds).

   ---------- Imported Events (preview) By Log ----------

   eTrust AC :     143762
   ```

```
Last EntryId processed: 101234500

Successfully detached from source [My_Audit_DSN]

Exiting Import...
```

In den Vorschauergebnissen wird angegeben, dass eine relativ große Anzahl von CA Access Control-Ereignissen importiert werden muss. Nehmen Sie für dieses Beispiel an, dass nur die Ereignisse eines Zeitraums von zwei Monaten importiert werden müssen. Sie können den Vorschaubefehl so anpassen, dass eine kleinere Gruppe von Ereignissen anhand eines Datums importiert wird.

2. Ändern Sie die Importparameter so, dass ein Zeitraum angegeben wird, und führen Sie die Vorschau noch einmal mit folgendem Befehl aus:

```
LMSeosImport.exe –dsn My_Audit_DSN –user sa –password sa -target My_CA-
ELM_Server –log "eTrust Access Control" -mintm 2008-11-01 -maxtm 2009-12-31 -
preview
```

Mit dem geänderten Befehl werden Daten wie die folgenden angezeigt:

```
Import started on Fri Jan  2 15:41:23 2009


No transport specified, defaulting to SAPI...

Preparing ODBC connections...

Successfully attached to source [My_Audit_DSN]

No starting ENTRYID specified, using minimum ENTRYID of 1...

Import (preview) running, please wait...

.........

Import (preview) Completed (143762 records in 4 minutes 37 seconds).

---------- Imported Events (preview) By Log ----------

eTrust AC :     2349

Last EntryId processed: 5167810102

Successfully detached from source [My_Audit_DSN]
```

```
Exiting Import...
```

Diese Importvorschau zeigt, dass sich durch den Zeitraum eine kleinere Untergruppe von zu importierenden Ereignissen ergibt. Jetzt können Sie den eigentlichen Import durchführen.

Weitere Informationen

Wissenswertes über die LMSeosImport-Befehlszeile (siehe Seite 243)
Vorschau der Importergebnisse (siehe Seite 247)

Importieren von CA Access Control-Ereignissen

Nachdem Sie den Ereignisbericht und eine Importvorschau erstellt haben, können Sie die CA Access Control-Ereignisse aus der SEOSDATA-Tabelle importieren.

So importieren Sie CA Access Control-Ereignisse:

Verwenden Sie den Befehl aus der Vorschau ohne die Option "-preview", um die CA Access Control-Ereignisse des angegebenen Zeitraums abzurufen:

```
LMSeosImport.exe –dsn [My_Audit_DSN] –user sa –password sa -target [My-CA-ELM-Server] –log "eTrust Access Control" -mintm 2008-11-01 -maxtm 2009-12-31
```

Das Hilfsprogramm zeigt Ergebnisse ähnlich der folgenden an:

```
Import started on Fri Jan  2 15:41:23 2009


No transport specified, defaulting to SAPI...

Preparing ODBC connections...

Successfully attached to source [My_Audit_DSN]

No starting ENTRYID specified, using minimum ENTRYID of 1...

Import running, please wait...

.........

Import Completed (143762 records in 5 minutes 18 seconds).

---------- Imported Events (preview) By Log ----------

eTrust AC :     2241

Last EntryId processed: 5167810102
```

```
Successfully detached from source [My_Audit_DSN]

Exiting Import...
```

Weitere Informationen

Wissenswertes über die LMSeosImport-Befehlszeile (siehe Seite 243)
Importieren von Ereignissen aus einer Windows-Collector-Datenbank (siehe Seite 248)
Importieren von Ereignissen aus einer Solaris-Collector-Datenbank (siehe Seite 248)

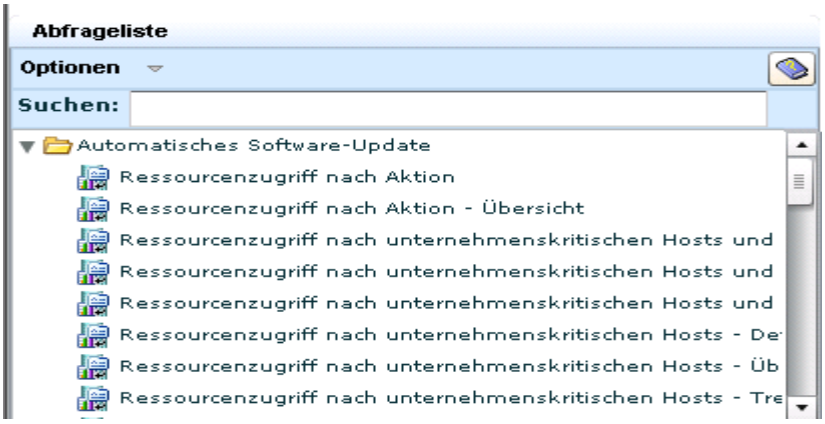
Anzeigen von Abfragen und Berichten zum Einsehen von CA Access Control-Ereignissen

CA Enterprise Log Manager bietet eine Reihe von Abfragen und Berichten, mit denen Sie die aus CA Access Control erfassten Ereignisse überprüfen können. Gehen Sie wie unten beschrieben vor, um auf CA Access Control-Abfragen und -Berichte zuzugreifen.

So greifen Sie auf CA Access Control-Abfragen zu:

1. Melden Sie sich beim CA Enterprise Log Manager-Server unter einem Benutzer mit der Berechtigung zum Anzeigen von Abfragen und Berichten an.
2. Rufen Sie auf der Registerkarte "Abfragen und Berichte" die untergeordnete Registerkarte "Abfragen" auf (sofern sie noch nicht angezeigt wird).

3. Klicken Sie auf die Abfragekennung "CA Access Control", um die verfügbaren Abfragen in einer Liste auf der linken Seite anzuzeigen.

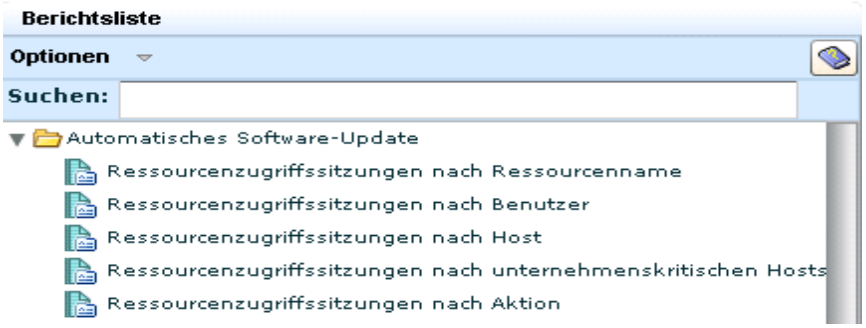


4. Wählen Sie eine Abfrage aus, um die Ereignisdaten anzuzeigen.

So greifen Sie auf CA Access Control-Berichte zu:

1. Melden Sie sich beim CA Enterprise Log Manager-Server unter einem Benutzer mit der Berechtigung zum Anzeigen von Abfragen und Berichten an.
2. Rufen Sie auf der Registerkarte "Abfragen und Berichte" die untergeordnete Registerkarte "Berichte" auf (sofern sie noch nicht angezeigt wird).

3. Klicken Sie auf die Berichtskennung "CA Access Control", um die verfügbaren Berichte in einer Liste auf der linken Seite anzuzeigen.



4. Wählen Sie einen Bericht aus, um die Ereignisdaten anzuzeigen.

Anhang C: Hinweise zu CA IT PAM

Dieses Kapitel enthält folgende Themen:

Szenario: Verwendung von CA EEM auf CA Enterprise Log Manager zur Authentifizierung von CA IT PAM

Dieser Anhang beschreibt den Vorgang, CA IT PAM auf einem Windows-Server zu installieren und CA EEM auf dem CA Enterprise Log Manager-Server zur Authentifizierung freizugeben. Diese Vorgehensweisen ergänzen die Angaben im *CA IT Process Automation-Installationshandbuch*.

Wichtig! Die Freigabe von CA EEM wird im FIPS-Modus *nicht* unterstützt, da CA IT PAM nicht FIPS-kompatibel ist. Wenn Sie für Ihren CA Enterprise Log Manager-Server den FIPS-Modus festlegen, schlägt die Integration mit CA IT PAM fehl.

Hinweis: Wenn Sie CA IT PAM auf einem UNIX-Server installieren bzw. LDAP oder lokales CA EEM zur Authentifizierung verwenden möchten, trifft die Dokumentation in diesem Anhang nicht auf Sie zu. In diesem Fall nutzen Sie nicht den gleichen CA EEM-Server. CA Enterprise Log Manager r12.1 SP1 kann im FIPS-Modus ausgeführt werden und mit CA IT PAM kommunizieren; diese Kommunikationskanäle sind jedoch nicht FIPS-kompatibel.

Laden Sie für Installationsszenarien das *Installationshandbuch* für CA IT Process Automation Manager r2.1 SP03 von Support Online herunter. Laden Sie auch Adobe Acrobat Reader herunter, damit Sie Pdfs öffnen können.

Der Vorgang bei dem Sie CA EEM auf CA Enterprise Log Manager zur Authentifizierung von CA IT PAM verwenden können, enthält zwei manuelle Schritte. Sie kopieren eine Datei vom Windows-Server auf die Anwendung und eine andere Datei von der Anwendung auf den Windows-Server. Diese Schritte werden in diesem Anhang beschrieben, sind jedoch nicht in der CA IT PAM-Dokumentation enthalten.

Implementierungsprozess der CA IT PAM-Authentifizierung

Der Implementierungsprozess der CA IT PAM-Authentifizierung, bei dem CA EEM auf dem CA Enterprise Log Manager-Verwaltungsserver verwendet wird, besteht aus folgenden Schritten:

1. Bereiten Sie die Implementierung der CA IT PAM-Authentifizierung vor.
    a. Laden Sie das CA IT PAM-Installationspaket auf den Windows-Server, auf dem CA IT PAM installiert werden soll.
    b. (Optional) Ändern Sie das Standardkennwort für das Zertifikat "itpamcert.p12".
2. Kopieren Sie die Datei "ITPAM_eem.xml" vom Host, auf dem Sie CA IT PAM installieren möchten, auf die CA Enterprise Log Manager-Anwendung, die CA EEM enthält.

3. Protokollieren Sie ITPAM als eine Anwendungsinstanz auf CA EEM, das CA Enterprise Log Manager verwendet. Durch die Ausführung des Befehls "safex" wird das Zertifikat "itpamcert.p12" generiert und die ITPAM-Anwendungsinstanz mit zwei Benutzerkonten, itpamadmin und itpamuser, wird erstellt.

   Hinweis: Geben Sie "./safex" ein, um Hilfe zur Verwendung des Befehls "safex" zu erhalten.

4. Kopieren Sie die Datei "itpamcert.p12" von der CA Enterprise Log Manager-Anwendung auf den Windows-Host, auf dem die CA IT PAM-Domäne installiert werden soll.
5. Wechseln Sie zur ITPAM-Anwendung und setzen Sie die Kennwörter für "itpamadmin" und "itpamuser" zurück.
6. Melden Sie sich beim Windows-Server an und installieren Sie die Drittanbieter-Komponenten mit Hilfe von Vorgehensweisen, die im *CA IT Process Automation Manager-Installationshandbuch* beschrieben werden.
7. Installieren Sie die CA IT PAM-Domäne mit Hilfe der Richtlinien in diesem Anhang und den CA IT PAM-Installationsanweisungen.
8. Starten Sie den CA IT PAM-Server-Dienst:
9. Starten Sie die CA IT PAM-Konsole und melden Sie sich an.

Bereiten Sie die Implementierung der CA IT PAM-Authentifizierung auf freigegebenem CA EEM vor

Nachdem Ihr Installationspaket auf dem Windows-Server geladen wurde, auf dem Sie die CA IT PAM-Domäne installieren möchten, können Sie ein Kennwort für das Zertifikat "itpamcert.cer" festlegen.

So bereiten Sie die Implementierung der CA IT PAM-Authentifizierung auf dem CA Enterprise Log Manager-Verwaltungsserver vor

1. Extrahieren Sie das CA IT PAM-ISO-Image auf dem Windows Server 2003-Host, auf dem Sie CA IT PAM installieren möchten.

   Hinweis: Das CA IT PAM-ISO-Image finden Sie auf CD 2 der CA IT PAM-Installationsquelle.

2. (Optional) Ändern Sie das Standardkennwort für das IT PAM-Zertifikat.
   a. Navigieren Sie zum Ordner "<Installationspfad>\eem".
   b. Öffnen Sie die Datei "ITPAM_eem.xml".
   c. Ersetzen Sie "itpamcertpass" in der folgenden Zeile:

      ```
      <Register certfile="itpamcert.p12" password="itpamcertpass"/>
      ```

   d. Speichern Sie die Datei.

Kopieren einer XML-Datei auf den CA Enterprise Log Manager-Verwaltungsserver

Der Befehl "safex"generiert CA IT PAM-Sicherheitsobjekte aus der Datei "ITPAM_eem.xml". Sie müssen diese Datei in die CA Enterprise Log Manager-Anwendung kopieren, von wo aus während der Safex-Verarbeitung auf sie zugegriffen werden kann.

So kopieren Sie die Datei "ITPAM_eem.xml" in die CA Enterprise Log Manager-Anwendung

Kopieren Sie die Datei "ITPAM_eem.xml", die auf dem CA IT PAM-Installationsdatenträger zu finden ist, in die CA Enterprise Log Manager-Anwendung, die CA EEM enthält. Wenn Sie die ISO-Datei auf den Windows-Server extrahiert haben, verwenden Sie Winscp, um "ITPAM_eem.xml" in das Verzeichnis "/tmp" der Anwendung zu kopieren.

- Quelldatei auf dem CA IT PAM-Installationsdatenträger:

  `ITPAM_eem.xml`

- Zielpfad auf CA Enterprise Log Manager:

  `/opt/CA/SharedComponents/iTechnology`

Registrieren von CA IT PAM mit freigegebenem CA EEM

Sie können CA IT PAM mit dem im CA Enterprise Log Manager-Verwaltungsserver eingebetteten CA EEM registrieren. Die Registrierung mit CA EEM fügt CA IT PAM-Sicherheitsobjekte hinzu.

Während der Registrierung zu CA EEM hinzugefügte CA IT PAM-Sicherheitsobjekte sind unter anderem:

- Anwendungsinstanz, ITPAM.
- Richtlinien hinsichtlich CA IT PAM-Zugriff
- Gruppen und Benutzer, einschließlich vordefinierte ITPAMAdmins, ITPAMUsers, itpamadmin und itpamuser
- Zertifikat "itpamcert.p12"

Sie können die CA IT PAM-Sicherheitsobjekte auf dem CA Enterprise Log Manager-Verwaltungsserver erstellen. Gehen Sie sicher, dass Sie vor Beginn über das Kennwort für "caelmadmin" verfügen.

So registrieren Sie CA IT PAM mit CA EEM auf dem CA Enterprise Log Manager-Verwaltungsserver

1. Melden Sie sich bei der CA Enterprise Log Manager-Anwendung über "ssh" als "caelmadmin"-Benutzer an.
2. Schalten Sie Benutzer auf das "root"-Konto um.

   ```
   su -
   ```

3. Wechseln Sie die Verzeichnisse auf den Zielpfad und erstellen Sie eine Liste des Inhalts.

   ```
   cd /opt/CA/SharedComponents/iTechnology
   ls
   ```

4. Überprüfen Sie, dass die folgenden Dateien aufgelistet werden:
   - ITPAM_eem.xml
   - safex
5. Führen Sie folgenden Befehl aus:

   ```
   . /safex -h <ELM_Hostname> -u EiamAdmin -p <Kennwort> -f ITPAM_eem.xml
   ```

   Dieser Prozess erstellt die CA IT PAM-Anwendung im CA Enterprise Log Manager-Verwaltungsserver, fügt die Standardbenutzer hinzu und generiert das während der IT PAM-Installation benötigte Zertifikat. Das Zertifikat wird mit dem in der Datei "ITPAM_eem.xml" angegebenen Kennwort erstellt, oder wenn nicht verändert, mit "itpamcertpass".

   Hinweis: Geben Sie "./safex" ein, um Hilfe zur Verwendung des Befehls "safex" zu erhalten.
6. Listen Sie den Inhalt des Verzeichnisses auf und überprüfen Sie, dass "itpamcert.cer" vorhanden ist.
7. Entfernen Sie die XML-Datei zur CA IT PAM-Konfiguration. Dies wird aus Sicherheitsgründen empfohlen.

   ```
   rm ITPAM_eem.xml
   ```

Kopieren des Zertifikats auf den CA IT PAM-Server

Bei der Ausführung des Befehls "safex" auf CA Enterprise Log Manager, um CA IT PAM mit CA EEM zu registrieren, wurde das Zertifikat "itpamcert.p12" generiert. Sie müssen dieses Zertifikat auf den Windows-Server kopieren, auf dem Sie die CA IT PAM-Domäne installieren möchten. Während der CA IT PAM-Domäneninstallation suchen Sie diese Zertifikatsdatei.

So kopieren Sie das Zertifikat von der CA Enterprise Log Manager-Anwendung auf den Ziel-Windows-Server

Kopieren Sie die Datei "itpamcert.p12" von der CA Enterprise Log Manager-Anwendung, die CA EEM enthält, auf den Host, auf dem CA IT PAM installiert werden soll.

- Quelldatei auf dem CA Enterprise Log Manager-Verwaltungsserver:

  `/opt/CA/SharedComponents/iTechnology/itpamcert.p12`

- Zielpfad auf dem Ziel-Windows-Server:

  `<Installationspfad>`

  Hinweis: Sie können diese Datei an den Pfad Ihrer Wahl kopieren. Sie wählen diese Datei von ihrem Speicherort aus, wenn Sie die CA IT PAM-Domäne installieren.

Festlegen von Kennwörtern für die vordefinierten CA IT PAM-Benutzerkonten

Mit der Ausführung des Befehls "safex" wird das Folgende erstellt:

- IT PAM-Sicherheitsgruppen:
  - ITPAMAdmins
  - ITPAMUsers
- IT PAM-Benutzer
  - "itpamadmin" mit einem Standardkennwort
  - "itpamuser" mit einem Standardkennwort

Sie müssen das Kennwort für die beiden vordefinierten IT PAM-Benutzer zurücksetzen.

So setzen Sie Kennwörter für "itpamadmin" und "itpamuser" in der IT PAM-Anwendung auf CA EEM zurück

1. Suchen Sie nach der URL des Servers, auf dem CA EEM installiert ist, das von CA Enterprise Log Manager verwendet wird, zum Beispiel der CA Enterprise Log Manager-Verwaltungsserver:

   `https://<ELM_Verwaltungsserver>5250/spin/eiam`

   Das Fenster zur Anmeldung bei CA EEM wird angezeigt. Die Pulldown-Liste "Anwendung" enthält <Global>, CAELM und ITPAM.

2. Melden Sie sich bei der IT PAM-Anwendung an.

   a. Wählen Sie ITPAM als Anwendung aus.

   b. Geben Sie "EiamAdmin" als Benutzername an.

   c. Geben Sie ein Kennwort für das EiamAdmin-Benutzerkonto an.

   d. Klicken Sie auf "Anmelden".

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

4. Geben Sie im Dialogfeld "Benutzer suchen" für "Wert" "itpam" ein und klicken Sie anschließend auf "Los".

   Die folgenden Benutzer werden in der Liste angezeigt

   - itpamadmin
   - itpamuser

5. Setzen Sie das Kennwort für "itpamadmin" zurück:

   a. Wählen Sie "itpamadmin" aus der Liste aus und scrollen Sie zu "Authentifizierung" im rechten Bereich.

   b. Wählen Sie "Kennwort zurücksetzen" aus.

   c. Geben Sie im Feld "Neues Kennwort" das Kennwort für dieses Konto ein und bestätigen Sie das Kennwort.

   d. Klicken Sie auf "Speichern".

6. Setzen Sie das Kennwort für "itpamuser" zurück:

   a. Wählen Sie "itpamuser" aus der Liste aus und scrollen Sie zu "Authentifizierung" im rechten Bereich.

   b. Wählen Sie "Kennwort zurücksetzen" aus.

   c. Geben Sie im Feld "Neues Kennwort" das Kennwort für dieses Konto ein und bestätigen Sie das Kennwort.

   d. Klicken Sie auf "Speichern".

7. Klicken Sie auf "Abmelden".

Installieren der für CA IT PAM erforderlichen Komponenten von Drittanbietern

Vor der Installation der Komponenten von Drittanbietern muss JDK 1.6 oder höher auf Ihrem System installiert sein. Führen Sie auf dem Windows-Server, auf dem CA IT PAM installiert werden soll, die Datei "Third_Party_Installer_windows.exe" aus. Details finden Sie im *CA IT Process Automation Manager-Installationshandbuch*.

Installieren der CA IT PAM-Domäne

Durch das Ausführen des CA IT PAM-Assistenten mit den hier angegebenen Spezifikationen wird das Zertifikat verknüpft, so dass CA IT PAM und CA EEM auf dem CA Enterprise Log Manager-Verwaltungsserver nun als vertrauenswürdig gelten.

Halten Sie die folgenden Informationen bereit:

- Kennwort für die EEM-Zertifikatsdatei "itpamcert.p12". Sie haben möglicherweise die Standardeinstellung in der Datei "ITPAM_eem.xml" während des Schrittes "Bereiten Sie die Implementierung der CA IT PAM-Authentifizierung auf freigegebenem CA EEM vor" abgeändert.
- Hostname des CA Enterprise Log Manager-Verwaltungsservers. Dies ist der Server, bei dem Sie sich für den Schritt "Registrieren von CA IT PAM mit freigegebenem CA EEM"angemeldet haben.
- Das itpamadmin-Kennwort, das im Rahmen von "Festlegen von Kennwörtern für die vordefinierten CA IT PAM-Benutzerkonten" festgelegt wurde.
- Das Zertifikatskennwort, das zur Kontrolle des Zugriff auf die Schlüssel verwendet wird, die Kennwörter verschlüsseln. Dabei handelt es sich um eine neue, nicht bereits vorhandene Einstellung.

Weitere Informationen zur Installation der CA IT PAM-Domäne finden Sie im *CA IT Process Automation Manager-Installationshandbuch*, das der Software beiliegt. In der folgenden Vorgehensweise werden Einzelheiten beschrieben, wie EEM-Sicherheitseinstellungen konfiguriert werden können.

So installieren Sie die CA IT PAM-Domäne

1. Wenn der IT PAM-Installationsassistent nicht im Anschluss an die Installation von Drittanbieter-Komponenten gestartet wird, starten Sie "CA_ITPAM_Domain_windows.exe" manuell.
2. Folgen Sie den Anweisungen in der CA IT PAM-Dokumentation, bis Sie zum Dialogfeld "Sicherheitsservertyp auswählen" kommen.

3. Wenn dieses Dialogfeld angezeigt wird, wählen Sie EEM als Sicherheitsserver aus und klicken Sie auf "Weiter".

   Das Fenster "EEM-Sicherheitseinstellungen" wird angezeigt.

4. Geben Sie die folgenden EEM-Sicherheitseinstellungen an:

   a. Geben Sie den Hostnamen des CA Enterprise Log Manager-Verwaltungsservers im Feld "EEM-Server" ein.

   b. Geben Sie ITPAM im Feld "EEM-Anwendung" an.

   c. Klicken Sie auf "Durchsuchen" und gehen Sie zum Ordner, in dem "itpamcert.p12" zu finden ist.

   d. Wählen Sie "itpamcert.p12" aus.

   e. Füllen Sie das Feld "EEM-Zertifikatskennwort" aus, indem Sie eine der beiden folgenden Vorgehensweisen wählen:

      – Geben Sie das Kennwort ein, das Sie in der Datei "ITPAM_eem.xml" bei der Vorbereitung ersetzt haben.

      – Geben Sie "itpamcertpass", das Standardkennwort, ein.

5. Klicken Sie auf "EEM-Einstellungen testen".

   Die Meldung "Ein Test wird durchgeführt. Dies dauert möglicherweise ein paar Minuten." wird angezeigt.

6. Klicken Sie auf OK.

   Das Dialogfeld "EEM-Einstellungen überprüfen" wird angezeigt.

7. Geben Sie "itpamadmin" als Benutzername ein. Geben Sie das Kennwort ein, das Sie für das itpamadmin-Benutzerkonto festgelegt haben und klicken Sie anschließend auf "OK".

8. Klicken Sie auf "Weiter". Folgen Sie den Anweisungen der IT PAM-Dokumentation, um den Rest des Assistenten abzuschließen.

Starten des CA ITPAM-Server-Service

Starten Sie den CA ITPAM-Server-Service, damit Sie und andere Personen den CA IT PAM-Server starten können.

So starten Sie den CA ITPAM-Server-Service:

1. Melden Sie sich bei dem Windows-Server an, auf dem Sie die CA IT PAM-Domäne installiert haben.
2. Wählen Sie im Menü "Start" nacheinander "Programme", "ITPAM-Domäne" und "Server-Service starten".

   Hinweis: Falls diese Menüoption nicht angezeigt wird, wählen Sie "Verwaltung" und "Komponentendienste". Klicken Sie auf "Dienste", "CA IT PAM-Server" und dann auf "Dienst starten".

Starten der CA IT PAM-Serverkonsole und Anmelden an der Konsole

Über einen Browser können Sie den CA IT PAM-Server auf jedem System starten, auf dem Java JRE 1.6 oder die JDK 1.6-API installiert und integriert ist.

So starten Sie die CA IT PAM-Verwaltungskonsole:

1. Geben Sie in der Adresszeile eines Browsers die folgende URL ein:

   `http://<itpam_server_hostname>:8080/itpam/`

   Der Anmeldebildschirm von CA IT Process Automation Manager wird angezeigt.
2. Geben Sie in das Feld "Benutzeranmeldung" den Benutzer "itpamadmin".
3. Geben Sie in das Feld "Kennwort" das Kennwort ein, das Sie diesem Benutzer zugewiesen haben.
4. Klicken Sie auf "Anmelden".

   Ihre Anmeldeinformationen werden von CA EEM in der CA Enterprise Log Manager-Anwendung authentifiziert, und CA IT Process Automation Manager wird geöffnet.

Details zur Integration und Verwendung von CA IT PAM mit CA Enterprise Log Manager finden Sie im *CA Enterprise Log Manager-Administrationshandbuch* im Kapitel "Aktionsalarme" im Abschnitt "Arbeiten mit CA IT PAM Ereignis-/Ausgabeprozessen".

Anhang D: Disaster Recovery

Dieses Kapitel enthält folgende Themen:

Planen einer effizienten Zurückgewinnung (Disaster Recovery)

Das Planen einer effizienten Zurückgewinnung (Disaster Recovery genannt) ist unumgänglicher Teil eines jeden guten Plans für die Netzwerkverwaltung. Die Disaster-Recovery-Planung für CA Enterprise Log Manager ist relativ einfach und unkompliziert. Der Schlüssel zu einer erfolgreichen Disaster Recovery für CA Enterprise Log Manager liegt in regelmäßigen Sicherungen.

Sie müssen folgende Daten sichern:

- die CA Enterprise Log Manager-Anwendungsinstanz auf dem Verwaltungsserver
- den Ordner "/opt/CA/LogManager/data" auf jedem CA Enterprise Log Manager-Server
- die Zertifikatsdateien im Ordner "/opt/CA/SharedComponents/iTechnology" auf jedem CA Enterprise Log Manager-Server

Falls ein hoher Durchsatz für Ihre Implementierung wichtig ist, können Sie einen Reserveserver unterhalten, der dieselben Hardwaremerkmale aufweist wie der Server, auf dem Sie die anderen CA Enterprise Log Manager-Server installieren. Falls ein CA Enterprise Log Manager-Server ausfällt, können Sie einen anderen mit genau demselben Namen installieren. Wenn der neue Server gestartet wird, erhält er die notwendigen Konfigurationsdateien vom Verwaltungsserver. Falls eine solche Leistungsvorgabe für Ihre Implementierung nicht von Bedeutung ist, können Sie einen CA Enterprise Log Manager-Server auf jedem leeren Server installieren, der als Host für das grundlegende Betriebssystem geeignet ist und die Mindestanforderungen an Speicherplatz und Festplattenkapazität erfüllt.

Weitere Informationen zu Hardware- und Softwareanforderungen finden Sie in den *CA Enterprise Log Manager-Versionshinweisen*.

Der interne, auf dem Verwaltungsserver installierte CA EEM-Server verfügt ebenfalls über seine eigenen Failover-Konfigurationsprozesse, mit denen ein dauerhafter Betrieb sichergestellt wird. Genaue Informationen finden Sie im *CA EEM-Handbuch "Erste Schritte"*.

Wissenswertes über das Sichern des CA EEM-Servers

Die Konfigurationen für die einzelnen CA Enterprise Log Manager-Server, Agenten und Connectors sowie für Abfragen, Berichte, Alarme usw. werden separat im CA EEM-Repository des CA Enterprise Log Manager-Servers verwaltet. Wesentlich für eine erfolgreiche Wiederherstellung des Servers ist, dass Sie regelmäßig Sicherungskopien der in der CA Enterprise Log Manager-Anwendungsinstanz gespeicherten Daten anlegen.

Bei einer *Anwendungsinstanz* handelt es sich um allgemeinen Speicherplatz im CA EEM-Repository, in dem folgende Informationen gespeichert werden:

- Benutzer, Gruppen und Zugriffsrichtlinien
- Konfigurationen für Agenten, Integrationen, Listener und Connectors sowie gespeicherte Konfigurationen
- Benutzerdefinierte Abfragen, Berichte sowie Unterdrückungs- und Zusammenfassungsregeln
- Föderationsbeziehungen
- Informationen zur Binärcodeverwaltung
- Verschlüsselungscodes

Sie können die CA EEM-Sicherung über die CA EEM-Webbrowseroberfläche durchführen. Normalerweise verwenden alle CA Enterprise Log Manager-Server in einem Unternehmen dieselbe Anwendungsinstanz. Der Wert für die standardmäßige CA Enterprise Log Manager-Anwendungsinstanz lautet CAELM. Sie können CA Enterprise Log Manager-Server mit verschiedenen Anwendungsinstanzen installieren, es können allerdings nur Server mit derselben Anwendungsinstanz in einem Verbund (Föderation) zusammengeschlossen werden. Server, die denselben CA EEM-Server, aber unterschiedliche Anwendungsinstanzen verwenden, weisen nur denselben Benutzerspeicher sowie dieselben Kennwortrichtlinien und globalen Gruppen auf.

Im *CA EEM-Handbuch "Erste Schritte"* finden Sie weitere Informationen zu Sicherung und Wiederherstellung.

Sichern einer CA EEM-Anwendungsinstanz

Sie können eine CA Enterprise Log Manager-Anwendungsinstanz über den internen CA EEM-Server auf dem Verwaltungsserver sichern.

So sichern Sie eine Anwendungsinstanz:

1. Greifen Sie mit der folgenden URL auf den CA EEM-Server zu:

   `https://<Servername>:5250/spin/eiam`

2. Erweitern Sie die Anwendungsliste auf der Anmeldeseite, und wählen Sie den Anwendungsinstanznamen aus, den Sie bei der Installation der CA Enterprise Log Manager-Server verwendet haben.

   Der standardmäßige Anwendungsinstanzname für CA Enterprise Log Manager lautet CAELM.

3. Melden Sie sich als "EiamAdmin"-Benutzer oder als ein Benutzer mit der CA EEM-Administratorrolle an.

4. Rufen Sie die Registerkarte für die Konfiguration auf, und wählen Sie die untergeordnete Registerkarte für den EEM-Server aus.

5. Wählen Sie im Navigationsfenster auf der linken Seite das Element für den Anwendungsexport aus.

6. Aktivieren Sie alle Optionen mit Ausnahme des Kontrollkästchens für das Überschreiben der maximalen Suchgröße.

   Hinweis: Falls Sie ein externes Verzeichnis verwenden, lassen Sie die Optionen für globale Benutzer, globale Gruppen und globale Ordner deaktiviert.

7. Klicken Sie auf die Schaltfläche "Exportieren", um eine XML-Exportdatei für die Anwendungsinstanz zu erstellen.

   Im Dialogfeld für den Dateidownload werden der Dateiname "<*Anwendungsinstanzname*>.xml.gz", beispielsweise "CAELM.xml.gz", und die Schaltfläche "Speichern" angezeigt.

8. Klicken Sie auf die Schaltfläche "Speichern", und wählen Sie einen Speicherort für die Sicherung auf einem zugeordneten Remote-Server aus. Alternativ können Sie die Datei auch auf dem lokalen Rechner speichern und dann an den gewünschten Speicherort auf einem anderen Server kopieren bzw. verschieben.

Wiederherstellen eines CA EEM-Servers für die Verwendung mit CA Enterprise Log Manager

Sie können eine CA Enterprise Log Manager-Anwendungsinstanz auf einem Verwaltungsserver wiederherstellen. Zum Wiederherstellen der CA EEM-Funktionen des Verwaltungsservers müssen Sie das Hilfsprogramm "safex" ausführen, mit dem die gesicherte Anwendungsinstanz importiert wird.

So stellen Sie die CA EEM-Funktionen eines Verwaltungsservers mit Hilfe einer Sicherungskopie wieder her:

1. Installieren Sie die CA Enterprise Log Manager-Software-Appliance auf einem neuen Hardwareserver.
2. Rufen Sie eine Eingabeaufforderung auf, und navigieren Sie zu dem Verzeichnis "/opt/CA/LogManager/EEM".
3. Kopieren Sie die Sicherungsdatei "<*Anwendungsinstanzname*>.xml.gz" vom externen Sicherungsserver in dieses Verzeichnis.
4. Führen Sie folgenden Befehl aus, um die XML-Exportdatei abzurufen:

   `gunzip <Anwendungsinstanzname>.xml.gz`

5. Führen Sie folgenden Befehl aus, um die Exportdatei auf dem neuen Verwaltungsserver wiederherzustellen:

   `./safex –h eem-Serverhostname –u EiamAdmin –p Kennwort –f Anwendungsinstanzname.xml`

   Wenn der FIPS-Modus aktiviert ist, stellen Sie sicher, dass Sie die Option "-fips" verwenden.

6. Navigieren Sie zu dem Verzeichnis "/opt/CA/ELMAgent/bin".
7. Ersetzen Sie die Standarddatei "AgentCert.cer" durch die Sicherungsdatei "CAELM_AgentCert.cer", um sicherzustellen, dass der Agent ordnungsgemäß gestartet wird.

Sichern eines CA Enterprise Log Manager-Servers

Sie können den gesamten CA Enterprise Log Manager-Server über den Ordner "/opt/CA/LogManager/data" sichern. Bei diesem Datenordner handelt es sich um einen symbolischen Link zum Datenordner unter dem "root"-Verzeichnis (/data).

So sichern Sie einen CA Enterprise Log Manager-Server:

1. Melden Sie sich als "caelmadmin"-Benutzer beim CA Enterprise Log Manager-Server an.
2. Greifen Sie mit dem Hilfsprogramm "su" auf das "root"-Konto zu.
3. Navigieren Sie zu dem Verzeichnis "/opt/CA/LogManager".
4. Führen Sie den folgenden TAR-Befehl aus, um eine Sicherungskopie der CA Enterprise Log Manager-Serverdateien zu erstellen:

   ```
   tar –hzcvf backupData.tgz /data
   ```

   Mit diesem Befehl wird die komprimierte Ausgabedatei "backupData.tgz" mit den Dateien aus dem Verzeichnis "/data" erstellt.
5. Navigieren Sie zu dem Verzeichnis "/opt/CA/SharedComponents/iTechnology".
6. Führen Sie den folgenden TAR-Befehl aus, um eine Sicherungskopie der digitalen Zertifikate (d. h. aller Dateien mit der Dateierweiterung ".cer") zu erstellen:

   ```
   tar –zcvf backupCerts.tgz *.cer
   ```

   Mit diesem Befehl wird die komprimierte Ausgabedatei "backupCerts.tgz" erstellt.

   ```
   tar –hzcvf backupCerts.tgz /data
   ```

Wiederherstellen eines CA Enterprise Log Manager-Servers mit Hilfe von Sicherungsdateien

Sie können einen CA Enterprise Log Manager-Server mit Hilfe von Sicherungsdateien wiederherstellen, nachdem Sie die CA Enterprise Log Manager-Software-Appliance auf dem neuen Server installiert haben.

So stellen Sie einen CA Enterprise Log Manager-Server mit Hilfe von Sicherungen wieder her:

1. Stoppen Sie den iGateway-Prozess auf dem neuen Server.

   Navigieren Sie hierfür zu dem Ordner "/opt/CA/SharedComponents/iTechnology", und führen Sie den folgenden Befehl aus:

   ```
   ./S99igateway stop
   ```

2. Kopieren Sie die Dateien "backupData.tgz" und "backupCerts.tgz" in das Verzeichnis "/opt/CA/LogManager" auf dem neuen Server.
3. Erweitern Sie den Inhalt der Datei "backupData.tgz" mit folgendem Befehl:

   ```
   tar –xzvf  backupData.tgz
   ```

   Mit diesem Befehl wird der Inhalt des Datenordners mit dem Inhalt der Sicherungsdatei überschrieben.

4. Navigieren Sie zu dem Verzeichnis "/opt/CA/SharedComponents/iTechnology".
5. Erweitern Sie den Inhalt der Datei "backupCerts.tgz" mit folgendem Befehl:

   ```
   tar –xzvf  backupCerts.tgz
   ```

   Mit diesem Befehl werden die Zertifikatdateien (.p12) im aktuellen Ordner mit den Zertifikatdateien aus der Sicherungsdatei überschrieben.

6. Starten Sie den iGateway-Prozess.

   Geben Sie hierfür folgenden Befehl ein:

   ```
   ./S99igateway start
   ```

Ersetzen eines CA Enterprise Log Manager-Servers

Gehen Sie wie unten beschrieben vor, um einen (agentenlosen) CA Enterprise Log Manager-Quellserver für Protokolldateien nach einem großen Ausfall oder Notfall zu ersetzen. Mit dieser Vorgehensweise können Sie einer Notfallsituation begegnen, indem Sie einen neuen CA Enterprise Log Manager-Server erstellen, der die Ereigniserfassung anstelle des ausgefallenen Servers übernimmt.

Hinweis: Bei dieser Vorgehensweise werden Ereignisdaten im Ereignisprotokollspeicher des ausgefallenen Servers nicht wiederhergestellt. Verwenden Sie die regulären Methoden zur Datenwiederherstellung, um Ereignisdaten aus dem Ereignisprotokollspeicher des fehlerhaften Servers abzurufen.

So ersetzen Sie einen funktionsuntüchtigen CA Enterprise Log Manager-Server:

1. Installieren Sie die CA Enterprise Log Manager-Software-Appliance auf einem anderen Server, und verwenden Sie dabei den Hostnamen des ausgefallenen Servers.

   Wenn Sie während der Installation nach dem Namen der CA EEM-Anwendungsinstanz gefragt werden, müssen Sie die Anwendungsinstanz des alten Servers verwenden. Durch die erfolgreiche Registrierung kann der CA EEM-Server die Konfiguration synchronisieren.

2. Starten Sie den neuen CA Enterprise Log Manager-Server, und melden Sie sich unter dem standardmäßigen administrativen Benutzer "EiamAdmin" an.

   Wenn der neue CA Enterprise Log Manager-Server gestartet wird, stellt er automatisch eine Verbindung mit dem CA EEM-Server her, der dann die Konfigurationsdateien herunterlädt. Nachdem die Konfigurationsdateien heruntergeladen wurden, nimmt der neue CA Enterprise Log Manager-Server die Protokollerfassung auf.

Anhang E: CA Enterprise Log Manager und Virtualisierung

Dieses Kapitel enthält folgende Themen:

Voraussetzungen für die Bereitstellung

Für die Verwendung von CA Enterprise Log Manager in einer virtuellen Umgebung bzw. einer gemischten Umgebung mit Appliance-Servern und virtuellen Servern gelten folgende Punkte:

- Installieren Sie in einer ausschließlich virtuellen Umgebung mindestens einen CA Enterprise Log Manager-Server als Verwaltungsserver. Dieser Verwaltungsserver verwaltet Konfigurationen, Software-Updates und Kommunikationen mit Agenten. Auf dem Verwaltungsserver werden keine Ereignisprotokolle empfangen und keine Abfragen oder Berichte ausgeführt.
- Installieren Sie in einer gemischten Umgebung den CA Enterprise Log Manager-Verwaltungsserver auf zertifizierter Hardware.
- Jeder virtuelle Rechnerhost verfügt über die bei VMware ESX Server 3.5 zulässige maximale Anzahl von vier dedizierten Prozessoren.

Besondere Aspekte

Ein dedizierter CA Enterprise Log Manager-Server funktioniert optimal mit mindestens acht Prozessoren. VMware ESX Server erlaubt bis zu vier Prozessoren für einen einzelnen virtuellen Rechner. Um eine Leistung zu erzielen, die der eines dedizierten Servers mit acht Prozessoren entspricht, installieren Sie CA Enterprise Log Manager auf zwei oder mehr virtuellen Rechnern und bilden dann einen Verbund (Föderation), damit konsolidierte Berichte erstellt werden können.

Zwei CA Enterprise Log Manager-Server, die als Gastrechner unter VMware ESX Server v3.5 ausgeführt werden, entsprechen in etwa der Kapazität eines einzelnen dedizierten CA Enterprise Log Manager-Servers. Ziehen Sie folgende Tabelle bei der Planung Ihres virtuellen Netzwerks heran:

Rolle des CA Enterprise Log Manager-Servers	Anzahl der Prozessoren (mind.)	Speicher (pro CPU)	Gesamtspeicher (Mindestanforderung)
Verwaltungsserver*	4	2	8
Berichtsserver	4	2	8
Quellserver	4	2	8

* Die Installation von CA Enterprise Log Manager als Verwaltungsserver auf einem virtuellen Rechner wird nur dann empfohlen, wenn Sie eine ausschließlich virtuelle Umgebung installieren müssen.

Erstellen virtueller CA Enterprise Log Manager-Server

Sie können anhand der folgenden Szenarien virtuelle CA Enterprise Log Manager-Server für Ihre Umgebung zur Ereignisprotokollerfassung erstellen:

- Hinzufügen virtueller Server zu einer bestehenden CA Enterprise Log Manager-Umgebung (gemischte Umgebung)
- Erstellen einer virtuellen Protokollerfassungsumgebung
- Klonen und Bereitstellen virtueller CA Enterprise Log Manager-Server für eine schnelle Skalierbarkeit

Hinzufügen virtueller Server zu Ihrer Umgebung

Falls Sie bereits über eine CA Enterprise Log Manager-Implementierung verfügen, können Sie virtuelle CA Enterprise Log Manager-Quellserver für Protokolldateien hinzufügen, um ein gesteigertes Ereignisvolumen im Netzwerk zu verarbeiten. In diesem Szenario wird vorausgesetzt, dass bereits ein CA Enterprise Log Manager-Verwaltungsserver und mindestens ein CA Enterprise Log Manager-Server für Erfassung und Berichterstellung installiert wurden.

Hinweis: Um eine optimale Leistung zu erzielen, installieren Sie CA Enterprise Log Manager auf virtuellen Servern ausschließlich für die Erfassung und Berichterstellung.

Zum Hinzufügen von virtuellen Quellservern in der Umgebung sind folgende Schritte notwendig:

1. Erstellen Sie einen neuen virtuellen Rechner.
2. Fügen Sie virtuelle Festplattenlaufwerke hinzu.
3. Installieren Sie CA Enterprise Log Manager auf dem virtuellen Rechner.
4. Konfigurieren Sie den CA Enterprise Log Manager-Server wie im Abschnitt zur Installation beschrieben.

Nachdem Sie den virtuellen Quellserver installiert haben, können Sie ihn für Abfragen und Berichte zur Föderation hinzufügen.

Erstellen eines neuen virtuellen Rechners

Gehen Sie wie unten beschrieben vor, um mit dem VMware Infrastructure Client einen neuen virtuellen Rechner zu erstellen. Verwenden Sie für jeden virtuellen CA Enterprise Log Manager-Server vier Prozessoren, um eine akzeptable Leistung zu erzielen.

So erstellen Sie einen virtuellen Rechner:

1. Rufen Sie den VMware Infrastructure Client auf.
2. Klicken Sie im linken Fenster auf den ESX-Host, und wählen Sie "New Virtual Machine" aus, um den Assistenten für neue virtuelle Rechner aufzurufen. Hierdurch wird ein Konfigurationsdialogfeld angezeigt.
3. Wählen Sie "Custom configuration" aus, und klicken Sie auf "Next". Es wird ein Dialogfeld für den Namen und Speicherort angezeigt.
4. Geben Sie einen Namen für den CA Enterprise Log Manager-Server ein, der auf diesem virtuellen Rechner installiert werden soll, und klicken Sie auf "Next".
5. Legen Sie die Speichereinstellungen für den virtuellen Rechner fest, und klicken Sie auf "Next".

   Vergewissern Sie sich, dass die Speichereinstellungen für Ihren CA Enterprise Log Manager-Server ausreichend sind. Empfohlen wird eine Mindestgröße von 500 GB.

   Hinweis: In einem anderen Verfahren werden weitere virtuelle Festplattenlaufwerke für die Speicherung von erfassten Ereignisprotokollen eingerichtet.
6. Wählen Sie "Red Hat Enterprise Linux 5 (32 bit)" als "Guest Operating System" aus, und klicken Sie auf "Next".

7. Wählen Sie in der Dropdown-Liste "Number of virtual processors" den Eintrag "4" als Anzahl der virtuellen Prozessoren aus.

   Ihr physischer Hostserver muss in der Lage sein, vier physische CPUs *ausschließlich* für diese CA Enterprise Log Manager-Instanz bereitzustellen. Klicken Sie auf "Next".

8. Konfigurieren Sie die Speichergröße für den virtuellen Rechner, und klicken Sie auf "Next". Die *minimal* akzeptable Speichergröße für CA Enterprise Log Manager beträgt 8 GB bzw. 8192 MB.

9. Konfigurieren Sie die Netzwerkschnittstellenverbindung (NIC). CA Enterprise Log Manager erfordert mindestens eine Netzwerkverbindung. Wählen Sie in der Liste der verfügbaren NICs "NIC x" aus, und legen Sie als Adapterwert "Flexible" fest.

   Hinweis: Sie müssen nicht für jeden auf diesem physischen Server gehosteten CA Enterprise Log Manager-Server eine eigene NIC einrichten. Sie müssen jedoch für jede NIC eine statische IP-Adresse zuweisen.

10. Wählen Sie die Option "Connect at Power On" aus, und klicken Sie auf "Next". Das Dialogfeld "I/O Adapter Types" wird angezeigt.

11. Wählen Sie "LSI Logic" für den I/O-Adapter aus, und klicken Sie auf "Next". Das Dialogfeld "Select a Disk" wird angezeigt.

12. Wählen Sie die Option "Create a new virtual disk" aus, und klicken Sie auf "Next". Ein Dialogfeld für die Festplattenkapazität und den Speicherort wird angezeigt.

13. Legen Sie die Optionen "Disk Capacity" und "Location" fest, und klicken Sie auf "Next". Ein Dialogfeld mit erweiterten Optionen wird angezeigt.

    Sie können diese Festplatte entweder mit dem virtuellen Rechner speichern oder einen anderen Speicherort angeben. Empfohlen wird eine Mindestgröße von 500 GB.

14. Übernehmen Sie im Dialogfeld "Advanced Options" die Standardwerte, und klicken Sie auf "Next".

15. Bestätigen Sie die Einstellungen, und klicken Sie auf "Finish", um den neuen virtuellen Rechner zu erstellen.

Hinzufügen virtueller Festplattenlaufwerke

Gehen Sie wie unten beschrieben vor, um virtuelle Festplattenlaufwerke für die Speicherung von Ereignisprotokollen hinzuzufügen. Verwenden Sie dieselben Einstellungen, unabhängig davon, welche Rolle ein bestimmter CA Enterprise Log Manager-Server im Netzwerk spielt.

So bearbeiten Sie die Einstellungen:

1. Klicken Sie im VMware Infrastructure Client mit der rechten Maustaste auf den virtuellen Rechner, und wählen Sie "Edit Settings" aus.

   Das Dialogfeld "Virtual Machine Properties" wird angezeigt.

2. Markieren Sie die Eigenschaft "CD/DVD Drive 1".

3. Klicken Sie auf die Optionsschaltfläche "Host Device", und wählen Sie in der Dropdown-Liste Ihr DVD-ROM-Laufwerk aus.

4. Wählen Sie unter "Device Status" die Option "Connect at power on" aus.

5. Klicken Sie auf "Add", um den "Add Hardware Wizard" zu starten, und fügen Sie eine zweite Festplatte hinzu.

6. Markieren Sie in der Geräteliste den Eintrag "Hard Disk", und klicken Sie auf "Next". Das Dialogfeld "Select a Disk" wird angezeigt.

7. Wählen Sie die Option "Create a new virtual disk" aus, und klicken Sie auf "Next".

8. Legen Sie die Größe der neuen Festplatte fest, und wählen Sie die Option "Specify a datastore", um den Standort festzulegen.

   CA Enterprise Log Manager erkennt das zusätzliche Laufwerk während der Installation, und weist es dem Datenspeicher zu. Es wird empfohlen, CA Enterprise Log Manager möglichst viel Speicherplatz zur Verfügung zu stellen.

   Hinweis: Die Standardeinstellung für "Block Size" in VMware ESX Server ist 1 MB, wodurch der maximal erstellbare Speicherplatz auf 256 GB begrenzt wird. Falls Sie mehr Platz (bis zu 512 GB) benötigen, erhöhen Sie die Einstellung "Block Size" mit folgendem Befehl auf 2 MB:

   ```
   Vmkfstools --createfs vmfs3 --blocksize 2M vmhba0:0:0:3
   ```

   Starten Sie den ESX-Server neu, damit die neue Einstellung wirksam wird. Weitere Informationen zu diesem und anderen Befehlen finden Sie in der Dokumentation zu VMware ESX Server.

   Klicken Sie auf "Next", um das Dialogfeld "Specify Advanced Options" aufzurufen.

9. Übernehmen Sie im Dialogfeld "Advanced Options" die Standardwerte, und klicken Sie auf "Next". Das Dialogfeld "Ready to Complete" wird angezeigt.

10. Klicken Sie auf "Finish", um die Änderungen an diesem virtuellen Rechner zu speichern. Hierdurch kehren Sie zum Dialogfeld "VMware Infrastructure Client" zurück.

Installieren von CA Enterprise Log Manager auf dem virtuellen Rechner

Gehen Sie wie unten beschrieben vor, um CA Enterprise Log Manager auf einem zuvor erstellten virtuellen Rechner zu installieren.

Sie können im Anschluss an die Installation einen virtuellen bzw. dedizierten CA Enterprise Log Manager-Server so einrichten, dass er eine der verschiedenen funktionellen Rollen, wie etwa Verwaltungs-, Quell- oder Berichtsserver, übernimmt. Falls Sie einen CA Enterprise Log Manager-Verwaltungsserver installieren, sollten auf diesem Server keine Ereignisprotokolle empfangen und keine Abfragen und Berichte ausgeführt werden. Installieren Sie eigene virtuelle CA Enterprise Log Manager-Server als Berichts- und Quellserver, um eine optimale Leistung zu erzielen.

Lesen Sie die normalen Installationsanleitungen, bevor Sie CA Enterprise Log Manager in einer virtuellen Umgebung installieren. Auf dem Arbeitsblatt für die Installation können Sie sich die erforderlichen Informationen notieren.

So installieren Sie CA Enterprise Log Manager auf einem virtuellen Rechner:

1. Legen Sie den Datenträger für die Installation des CA Enterprise Log Manager-Betriebssystems in das physische DVD-ROM-Laufwerk ein, oder navigieren Sie zu dem Verzeichnis, in das Sie das Installations-Image kopiert haben.
2. Wählen Sie Ihren virtuellen Rechner in der Inventarliste der virtuellen Rechner aus, klicken Sie mit der rechten Maustaste auf den Eintrag, und wählen Sie "Power On" aus.
3. Fahren Sie mit der normalen CA Enterprise Log Manager-Installation fort.
4. Konfigurieren Sie den installierten CA Enterprise Log Manager-Server für die gewünschte funktionelle Rolle. Verwenden Sie dabei die Informationen im Abschnitt zur Installation eines CA Enterprise Log Manager-Servers.

Weitere Informationen

Installation von CA Enterprise Log Manager (siehe Seite 81)

Erstellen einer ausschließlich virtuellen Umgebung

Falls zuvor noch keine CA Enterprise Log Manager-Umgebung implementiert wurde, können Sie eine ausschließlich virtuelle Umgebung für die Protokollerfassung erstellen. In diesem Szenario wird vorausgesetzt, dass eine ausreichende Anzahl von physischen Servern mit jeweils einer Gruppe von mindestens vier Prozessoren verfügbar ist, um alle gewünschten CA Enterprise Log Manager-Server zu installieren.

Installieren Sie einen CA Enterprise Log Manager-Server als Verwaltungsserver. Während der Konfiguration sollten auf diesem Server keine Ereignisprotokolle eingehen und keine Berichte erstellt werden. Indem Sie Ihre Umgebung auf diese Weise konfigurieren, erzielen Sie den für die Produktion auf Unternehmensniveau erforderlichen Durchsatz bei der Ereignisprotokollerfassung.

Im Allgemeinen installieren Sie zwei CA Enterprise Log Manager-Server mit jeweils vier Prozessoren für jeden normalerweise auf zertifizierter Hardware installierten Appliance-Server. (Appliance-Server verfügen über mindestens acht Prozessoren.)

Zum Erstellen einer virtuellen Umgebung sind folgende Schritte notwendig:

1. Erstellen Sie für jeden CA Enterprise Log Manager-Server, der installiert werden soll, einen neuen virtuellen Rechner.
2. Fügen Sie virtuelle Festplattenlaufwerke hinzu.
3. Installieren Sie auf einem der virtuellen Rechnerhosts einen virtuellen CA Enterprise Log Manager-Server für Verwaltungsfunktionen.
4. Installieren Sie mindestens zwei CA Enterprise Log Manager-Server für Erfassung und Berichterstellung.
5. Konfigurieren Sie die CA Enterprise Log Manager-Server wie im Abschnitt zur Installation eines CA Enterprise Log Manager-Servers beschrieben.

Erstellen eines neuen virtuellen Rechners

Gehen Sie wie unten beschrieben vor, um mit dem VMware Infrastructure Client einen neuen virtuellen Rechner zu erstellen. Verwenden Sie für jeden virtuellen CA Enterprise Log Manager-Server vier Prozessoren, um eine akzeptable Leistung zu erzielen.

So erstellen Sie einen virtuellen Rechner:

1. Rufen Sie den VMware Infrastructure Client auf.
2. Klicken Sie im linken Fenster auf den ESX-Host, und wählen Sie "New Virtual Machine" aus, um den Assistenten für neue virtuelle Rechner aufzurufen. Hierdurch wird ein Konfigurationsdialogfeld angezeigt.
3. Wählen Sie "Custom configuration" aus, und klicken Sie auf "Next". Es wird ein Dialogfeld für den Namen und Speicherort angezeigt.
4. Geben Sie einen Namen für den CA Enterprise Log Manager-Server ein, der auf diesem virtuellen Rechner installiert werden soll, und klicken Sie auf "Next".
5. Legen Sie die Speichereinstellungen für den virtuellen Rechner fest, und klicken Sie auf "Next".

   Vergewissern Sie sich, dass die Speichereinstellungen für Ihren CA Enterprise Log Manager-Server ausreichend sind. Empfohlen wird eine Mindestgröße von 500 GB.

   Hinweis: In einem anderen Verfahren werden weitere virtuelle Festplattenlaufwerke für die Speicherung von erfassten Ereignisprotokollen eingerichtet.
6. Wählen Sie "Red Hat Enterprise Linux 5 (32 bit)" als "Guest Operating System" aus, und klicken Sie auf "Next".
7. Wählen Sie in der Dropdown-Liste "Number of virtual processors" den Eintrag "4" als Anzahl der virtuellen Prozessoren aus.

   Ihr physischer Hostserver muss in der Lage sein, vier physische CPUs *ausschließlich* für diese CA Enterprise Log Manager-Instanz bereitzustellen. Klicken Sie auf "Next".
8. Konfigurieren Sie die Speichergröße für den virtuellen Rechner, und klicken Sie auf "Next". Die *minimal* akzeptable Speichergröße für CA Enterprise Log Manager beträgt 8 GB bzw. 8192 MB.
9. Konfigurieren Sie die Netzwerkschnittstellenverbindung (NIC). CA Enterprise Log Manager erfordert mindestens eine Netzwerkverbindung. Wählen Sie in der Liste der verfügbaren NICs "NIC x" aus, und legen Sie als Adapterwert "Flexible" fest.

   Hinweis: Sie müssen nicht für jeden auf diesem physischen Server gehosteten CA Enterprise Log Manager-Server eine eigene NIC einrichten. Sie müssen jedoch für jede NIC eine statische IP-Adresse zuweisen.

10. Wählen Sie die Option "Connect at Power On" aus, und klicken Sie auf "Next". Das Dialogfeld "I/O Adapter Types" wird angezeigt.
11. Wählen Sie "LSI Logic" für den I/O-Adapter aus, und klicken Sie auf "Next". Das Dialogfeld "Select a Disk" wird angezeigt.
12. Wählen Sie die Option "Create a new virtual disk" aus, und klicken Sie auf "Next". Ein Dialogfeld für die Festplattenkapazität und den Speicherort wird angezeigt.
13. Legen Sie die Optionen "Disk Capacity" und "Location" fest, und klicken Sie auf "Next". Ein Dialogfeld mit erweiterten Optionen wird angezeigt.

    Sie können diese Festplatte entweder mit dem virtuellen Rechner speichern oder einen anderen Speicherort angeben. Empfohlen wird eine Mindestgröße von 500 GB.
14. Übernehmen Sie im Dialogfeld "Advanced Options" die Standardwerte, und klicken Sie auf "Next".
15. Bestätigen Sie die Einstellungen, und klicken Sie auf "Finish", um den neuen virtuellen Rechner zu erstellen.

Hinzufügen virtueller Festplattenlaufwerke

Gehen Sie wie unten beschrieben vor, um virtuelle Festplattenlaufwerke für die Speicherung von Ereignisprotokollen hinzuzufügen. Verwenden Sie dieselben Einstellungen, unabhängig davon, welche Rolle ein bestimmter CA Enterprise Log Manager-Server im Netzwerk spielt.

So bearbeiten Sie die Einstellungen:

1. Klicken Sie im VMware Infrastructure Client mit der rechten Maustaste auf den virtuellen Rechner, und wählen Sie "Edit Settings" aus.

   Das Dialogfeld "Virtual Machine Properties" wird angezeigt.
2. Markieren Sie die Eigenschaft "CD/DVD Drive 1".
3. Klicken Sie auf die Optionsschaltfläche "Host Device", und wählen Sie in der Dropdown-Liste Ihr DVD-ROM-Laufwerk aus.
4. Wählen Sie unter "Device Status" die Option "Connect at power on" aus.
5. Klicken Sie auf "Add", um den "Add Hardware Wizard" zu starten, und fügen Sie eine zweite Festplatte hinzu.
6. Markieren Sie in der Geräteliste den Eintrag "Hard Disk", und klicken Sie auf "Next". Das Dialogfeld "Select a Disk" wird angezeigt.
7. Wählen Sie die Option "Create a new virtual disk" aus, und klicken Sie auf "Next".

8. Legen Sie die Größe der neuen Festplatte fest, und wählen Sie die Option "Specify a datastore", um den Standort festzulegen.

   CA Enterprise Log Manager erkennt das zusätzliche Laufwerk während der Installation, und weist es dem Datenspeicher zu. Es wird empfohlen, CA Enterprise Log Manager möglichst viel Speicherplatz zur Verfügung zu stellen.

   Hinweis: Die Standardeinstellung für "Block Size" in VMware ESX Server ist 1 MB, wodurch der maximal erstellbare Speicherplatz auf 256 GB begrenzt wird. Falls Sie mehr Platz (bis zu 512 GB) benötigen, erhöhen Sie die Einstellung "Block Size" mit folgendem Befehl auf 2 MB:

   ```
   Vmkfstools --createfs vmfs3 --blocksize 2M vmhba0:0:0:3
   ```

   Starten Sie den ESX-Server neu, damit die neue Einstellung wirksam wird. Weitere Informationen zu diesem und anderen Befehlen finden Sie in der Dokumentation zu VMware ESX Server.

   Klicken Sie auf "Next", um das Dialogfeld "Specify Advanced Options" aufzurufen.

9. Übernehmen Sie im Dialogfeld "Advanced Options" die Standardwerte, und klicken Sie auf "Next". Das Dialogfeld "Ready to Complete" wird angezeigt.

10. Klicken Sie auf "Finish", um die Änderungen an diesem virtuellen Rechner zu speichern. Hierdurch kehren Sie zum Dialogfeld "VMware Infrastructure Client" zurück.

Installieren von CA Enterprise Log Manager auf dem virtuellen Rechner

Gehen Sie wie unten beschrieben vor, um CA Enterprise Log Manager auf einem zuvor erstellten virtuellen Rechner zu installieren.

Sie können im Anschluss an die Installation einen virtuellen bzw. dedizierten CA Enterprise Log Manager-Server so einrichten, dass er eine der verschiedenen funktionellen Rollen, wie etwa Verwaltungs-, Quell- oder Berichtsserver, übernimmt. Falls Sie einen CA Enterprise Log Manager-Verwaltungsserver installieren, sollten auf diesem Server keine Ereignisprotokolle empfangen und keine Abfragen und Berichte ausgeführt werden. Installieren Sie eigene virtuelle CA Enterprise Log Manager-Server als Berichts- und Quellserver, um eine optimale Leistung zu erzielen.

Lesen Sie die normalen Installationsanleitungen, bevor Sie CA Enterprise Log Manager in einer virtuellen Umgebung installieren. Auf dem Arbeitsblatt für die Installation können Sie sich die erforderlichen Informationen notieren.

So installieren Sie CA Enterprise Log Manager auf einem virtuellen Rechner:

1. Legen Sie den Datenträger für die Installation des CA Enterprise Log Manager-Betriebssystems in das physische DVD-ROM-Laufwerk ein, oder navigieren Sie zu dem Verzeichnis, in das Sie das Installations-Image kopiert haben.
2. Wählen Sie Ihren virtuellen Rechner in der Inventarliste der virtuellen Rechner aus, klicken Sie mit der rechten Maustaste auf den Eintrag, und wählen Sie "Power On" aus.
3. Fahren Sie mit der normalen CA Enterprise Log Manager-Installation fort.
4. Konfigurieren Sie den installierten CA Enterprise Log Manager-Server für die gewünschte funktionelle Rolle. Verwenden Sie dabei die Informationen im Abschnitt zur Installation eines CA Enterprise Log Manager-Servers.

Weitere Informationen

Installation von CA Enterprise Log Manager (siehe Seite 81)

Schneller Einsatz der virtuellen CA Enterprise Log Manager-Server

Sie können einen virtuellen CA Enterprise Log Manager-Server klonen, um ein installierbares Image für die schnelle Skalierbarkeit Ihrer Protokollerfassungsumgebung zu erstellen.

Hinweis: Um eine optimale Leistung zu erzielen, empfehlen wir, CA Enterprise Log Manager auf virtuellen Servern ausschließlich für die Erfassung zu installieren. Klonen Sie keine virtuellen Rechner, die einen CA Enterprise Log Manager-Verwaltungsserver enthalten.

Überprüfen Sie, ob eine Umgebung vorhanden ist, bevor Sie mit diesem Szenario beginnen, oder installieren Sie einen CA Enterprise Log Manager-Server, um Verwaltungsfunktionen entweder auf einem dedizierten oder einem virtuellen Server durchzuführen. Für die Klonfunktion benötigen Sie auch die richtige Version der VMware-Software.

Zum Erstellen und Klonen eines virtuellen CA Enterprise Log Manager-Servers für die Erfassung sind folgende Schritte notwendig:

1. Erstellen Sie einen neuen virtuellen Rechner.
2. Fügen Sie virtuelle Festplattenlaufwerke hinzu.
3. Installieren Sie einen CA Enterprise Log Manager-Server auf dem virtuellen Rechner.

4. Klonen Sie den virtuellen Rechner, der Ihren neuen CA Enterprise Log Manager-Server enthält, anhand der Anweisungen des Herstellers.

   Hinweis: Erstellen Sie nur ein reines Klon-Image. Verwenden Sie mit CA Enterprise Log Manager keine verknüpften Klone.

5. Importieren Sie den geklonten virtuellen Rechner in einen physischen Zielserver.

6. Aktualisieren Sie den geklonten virtuellen Rechner, bevor Sie ihn mit dem Netzwerk verbinden.

7. Konfigurieren Sie den CA Enterprise Log Manager-Server wie im *Implementierungshandbuch* beschrieben.

Erstellen eines neuen virtuellen Rechners

Gehen Sie wie unten beschrieben vor, um mit dem VMware Infrastructure Client einen neuen virtuellen Rechner zu erstellen. Verwenden Sie für jeden virtuellen CA Enterprise Log Manager-Server vier Prozessoren, um eine akzeptable Leistung zu erzielen.

So erstellen Sie einen virtuellen Rechner:

1. Rufen Sie den VMware Infrastructure Client auf.

2. Klicken Sie im linken Fenster auf den ESX-Host, und wählen Sie "New Virtual Machine" aus, um den Assistenten für neue virtuelle Rechner aufzurufen. Hierdurch wird ein Konfigurationsdialogfeld angezeigt.

3. Wählen Sie "Custom configuration" aus, und klicken Sie auf "Next". Es wird ein Dialogfeld für den Namen und Speicherort angezeigt.

4. Geben Sie einen Namen für den CA Enterprise Log Manager-Server ein, der auf diesem virtuellen Rechner installiert werden soll, und klicken Sie auf "Next".

5. Legen Sie die Speichereinstellungen für den virtuellen Rechner fest, und klicken Sie auf "Next".

   Vergewissern Sie sich, dass die Speichereinstellungen für Ihren CA Enterprise Log Manager-Server ausreichend sind. Empfohlen wird eine Mindestgröße von 500 GB.

   Hinweis: In einem anderen Verfahren werden weitere virtuelle Festplattenlaufwerke für die Speicherung von erfassten Ereignisprotokollen eingerichtet.

6. Wählen Sie "Red Hat Enterprise Linux 5 (32 bit)" als "Guest Operating System" aus, und klicken Sie auf "Next".

7. Wählen Sie in der Dropdown-Liste "Number of virtual processors" den Eintrag "4" als Anzahl der virtuellen Prozessoren aus.

   Ihr physischer Hostserver muss in der Lage sein, vier physische CPUs *ausschließlich* für diese CA Enterprise Log Manager-Instanz bereitzustellen. Klicken Sie auf "Next".

8. Konfigurieren Sie die Speichergröße für den virtuellen Rechner, und klicken Sie auf "Next". Die *minimal* akzeptable Speichergröße für CA Enterprise Log Manager beträgt 8 GB bzw. 8192 MB.

9. Konfigurieren Sie die Netzwerkschnittstellenverbindung (NIC). CA Enterprise Log Manager erfordert mindestens eine Netzwerkverbindung. Wählen Sie in der Liste der verfügbaren NICs "NIC x" aus, und legen Sie als Adapterwert "Flexible" fest.

   Hinweis: Sie müssen nicht für jeden auf diesem physischen Server gehosteten CA Enterprise Log Manager-Server eine eigene NIC einrichten. Sie müssen jedoch für jede NIC eine statische IP-Adresse zuweisen.

10. Wählen Sie die Option "Connect at Power On" aus, und klicken Sie auf "Next". Das Dialogfeld "I/O Adapter Types" wird angezeigt.

11. Wählen Sie "LSI Logic" für den I/O-Adapter aus, und klicken Sie auf "Next". Das Dialogfeld "Select a Disk" wird angezeigt.

12. Wählen Sie die Option "Create a new virtual disk" aus, und klicken Sie auf "Next". Ein Dialogfeld für die Festplattenkapazität und den Speicherort wird angezeigt.

13. Legen Sie die Optionen "Disk Capacity" und "Location" fest, und klicken Sie auf "Next". Ein Dialogfeld mit erweiterten Optionen wird angezeigt.

    Sie können diese Festplatte entweder mit dem virtuellen Rechner speichern oder einen anderen Speicherort angeben. Empfohlen wird eine Mindestgröße von 500 GB.

14. Übernehmen Sie im Dialogfeld "Advanced Options" die Standardwerte, und klicken Sie auf "Next".

15. Bestätigen Sie die Einstellungen, und klicken Sie auf "Finish", um den neuen virtuellen Rechner zu erstellen.

Hinzufügen virtueller Festplattenlaufwerke

Gehen Sie wie unten beschrieben vor, um virtuelle Festplattenlaufwerke für die Speicherung von Ereignisprotokollen hinzuzufügen. Verwenden Sie dieselben Einstellungen, unabhängig davon, welche Rolle ein bestimmter CA Enterprise Log Manager-Server im Netzwerk spielt.

So bearbeiten Sie die Einstellungen:

1. Klicken Sie im VMware Infrastructure Client mit der rechten Maustaste auf den virtuellen Rechner, und wählen Sie "Edit Settings" aus.

   Das Dialogfeld "Virtual Machine Properties" wird angezeigt.

2. Markieren Sie die Eigenschaft "CD/DVD Drive 1".

3. Klicken Sie auf die Optionsschaltfläche "Host Device", und wählen Sie in der Dropdown-Liste Ihr DVD-ROM-Laufwerk aus.

4. Wählen Sie unter "Device Status" die Option "Connect at power on" aus.

5. Klicken Sie auf "Add", um den "Add Hardware Wizard" zu starten, und fügen Sie eine zweite Festplatte hinzu.

6. Markieren Sie in der Geräteliste den Eintrag "Hard Disk", und klicken Sie auf "Next". Das Dialogfeld "Select a Disk" wird angezeigt.

7. Wählen Sie die Option "Create a new virtual disk" aus, und klicken Sie auf "Next".

8. Legen Sie die Größe der neuen Festplatte fest, und wählen Sie die Option "Specify a datastore", um den Standort festzulegen.

   CA Enterprise Log Manager erkennt das zusätzliche Laufwerk während der Installation, und weist es dem Datenspeicher zu. Es wird empfohlen, CA Enterprise Log Manager möglichst viel Speicherplatz zur Verfügung zu stellen.

   Hinweis: Die Standardeinstellung für "Block Size" in VMware ESX Server ist 1 MB, wodurch der maximal erstellbare Speicherplatz auf 256 GB begrenzt wird. Falls Sie mehr Platz (bis zu 512 GB) benötigen, erhöhen Sie die Einstellung "Block Size" mit folgendem Befehl auf 2 MB:

   ```
   Vmkfstools --createfs vmfs3 --blocksize 2M vmhba0:0:0:3
   ```

   Starten Sie den ESX-Server neu, damit die neue Einstellung wirksam wird. Weitere Informationen zu diesem und anderen Befehlen finden Sie in der Dokumentation zu VMware ESX Server.

   Klicken Sie auf "Next", um das Dialogfeld "Specify Advanced Options" aufzurufen.

9. Übernehmen Sie im Dialogfeld "Advanced Options" die Standardwerte, und klicken Sie auf "Next". Das Dialogfeld "Ready to Complete" wird angezeigt.
10. Klicken Sie auf "Finish", um die Änderungen an diesem virtuellen Rechner zu speichern. Hierdurch kehren Sie zum Dialogfeld "VMware Infrastructure Client" zurück.

Installieren von CA Enterprise Log Manager auf dem virtuellen Rechner

Gehen Sie wie unten beschrieben vor, um CA Enterprise Log Manager auf einem zuvor erstellten virtuellen Rechner zu installieren.

Sie können im Anschluss an die Installation einen virtuellen bzw. dedizierten CA Enterprise Log Manager-Server so einrichten, dass er eine der verschiedenen funktionellen Rollen, wie etwa Verwaltungs-, Quell- oder Berichtsserver, übernimmt. Falls Sie einen CA Enterprise Log Manager-Verwaltungsserver installieren, sollten auf diesem Server keine Ereignisprotokolle empfangen und keine Abfragen und Berichte ausgeführt werden. Installieren Sie eigene virtuelle CA Enterprise Log Manager-Server als Berichts- und Quellserver, um eine optimale Leistung zu erzielen.

Lesen Sie die normalen Installationsanleitungen, bevor Sie CA Enterprise Log Manager in einer virtuellen Umgebung installieren. Auf dem Arbeitsblatt für die Installation können Sie sich die erforderlichen Informationen notieren.

So installieren Sie CA Enterprise Log Manager auf einem virtuellen Rechner:

1. Legen Sie den Datenträger für die Installation des CA Enterprise Log Manager-Betriebssystems in das physische DVD-ROM-Laufwerk ein, oder navigieren Sie zu dem Verzeichnis, in das Sie das Installations-Image kopiert haben.
2. Wählen Sie Ihren virtuellen Rechner in der Inventarliste der virtuellen Rechner aus, klicken Sie mit der rechten Maustaste auf den Eintrag, und wählen Sie "Power On" aus.
3. Fahren Sie mit der normalen CA Enterprise Log Manager-Installation fort.
4. Konfigurieren Sie den installierten CA Enterprise Log Manager-Server für die gewünschte funktionelle Rolle. Verwenden Sie dabei die Informationen im Abschnitt zur Installation eines CA Enterprise Log Manager-Servers.

Weitere Informationen

Installation von CA Enterprise Log Manager (siehe Seite 81)

Klonen eines virtuellen CA Enterprise Log Manager-Servers

Mit dieser Vorgehensweise können Sie einen virtuellen CA Enterprise Log Manager-Server klonen. In dieser Vorgehensweise wird davon ausgegangen, dass Sie bereits einen neuen virtuellen Rechner erstellt, Festplattenlaufwerke hinzugefügt und CA Enterprise Log Manager installiert haben.

So klonen Sie einen virtuellen Server:

1. Greifen Sie auf VMware VirtualCenter zu, und suchen Sie den virtuellen Rechner, der CA Enterprise Log Manager enthält.
2. Schalten Sie den virtuellen Rechner aus, falls dieser ausgeführt wird.
3. Wählen Sie die Option "Exportieren" aus, und legen Sie einen Ort für den exportierten virtuellen Rechner fest.

   Der VMware ESX Server bietet alternative Methoden zum Klonen virtueller Rechner. Hinweis: Weitere Informationen finden Sie in der VMware-Dokumentation.

Importieren eines geklonten virtuellen Rechners in einen Zielserver

Verwenden Sie diese Vorgehensweise, um einen geklonten virtuellen Rechner in einen anderen Server zu importieren, um ihn zu aktivieren.

So importieren Sie einen geklonten virtuellen Rechner:

1. Überprüfen Sie, ob Sie einen Netzwerkzugriff auf den Zielhostserver haben.
2. Greifen Sie vom Server mit VMware ESC auf VMware VirtualCenter zu.
3. Wählen Sie die Option "Importieren" aus, und suchen Sie den Zielserver. Reagieren Sie bei Bedarf auf zusätzliche Eingabeaufforderungen.

   Durch das Importieren wird der geklonte virtuelle Rechner zum Zielserver verschoben. Weitere Informationen finden Sie in der VMware ESX-Dokumentation.

Aktualisieren eines geklonten CA Enterprise Log Manager-Servers vor der Bereitstellung

Gehen Sie wie unten beschrieben vor, um einen geklonten, virtuellen CA Enterprise Log Manager-Server zu aktualisieren.

Ein geklonter, virtueller CA Enterprise Log Manager-Server behält den Hostnamen, den Sie ihm während der Installation gegeben haben. Der Hostname für jeden aktiven CA Enterprise Log Manager-Server muss jedoch innerhalb Ihrer Implementierung der Protokollerfassung eindeutig sein. Ändern Sie also den Hostnamen und die IP-Adresse des Servers mit dem Skript *Rename_ELM.sh*, bevor Sie einen geklonten virtuellen Server aktivieren.

Das Aktualisierungsskript führt folgende Maßnahmen durch:

- Automatischer Stopp und Neustart des Standardagenten
- Automatischer Stopp und Neustart des iGateway-Dienstes
- Sie werden aufgefordert, den Hostnamen, die IP-Adresse und die DNS-IP-Adresse zu ändern
- Automatische Aktualisierung der Konfigurationsdateien mit verschlüsselten Kennwörtern für die verschiedenen Zertifikate.

So aktualisieren Sie einen geklonten virtuellen CA Enterprise Log Manager-Server:

1. Melden Sie sich beim physischen Zielserver als Root-Benutzer an.
2. Greifen Sie auf das ISO-Image oder die DVD der Anwendung zu, und navigieren Sie zum Verzeichnis /CA/Linux_x86.

   Sie können das Skript auch im Dateisystem eines installierten CA Enterprise Log Manager-Servers finden. Das Skript bleibt im Verzeichnis opt/CA/LogManager.
3. Kopieren Sie das Skript Rename_ELM.sh zum Zielserver.
4. Ändern Sie die Informationen für den virtuellen CA Enterprise Log Manager-Server mit folgendem Befehl:

   ```
   ./Rename_ELM.sh
   ```
5. Reagieren Sie auf die Eingabeaufforderungen.
6. Starten Sie den virtuellen Rechner, der den aktuellen virtuellen Server enthält.

Terminologieglossar

Abfrage

Eine *Abfrage* ist ein Satz von Kriterien, mit denen die Ereignisprotokollspeicher der aktiven CA Enterprise Log Manager-Server und, sofern angegeben, seiner föderierten Server durchsucht werden. Eine Abfrage richtet sich an die heißen, warmen oder verfügbaren gemachten Datenbanken, die in der Where-Klausel der Abfrage angegeben wurden. Beispiel: Wenn die Where-Klausel die Abfrage auf Ereignisse mit source_username="myname" in einem bestimmten Zeitrahmen beschränkt und nur zehn von 1000 Datenbanken Datensätze enthalten, die diesen Kriterien (basierend auf den Informationen in der Katalogdatenbank) entsprechen, wird die Abfrage nur in diesen zehn Datenbanken durchgeführt. Eine Abfrage kann maximal 5000 Datenzeilen zurückgeben. Ein Benutzer mit einer vordefinierten Rolle kann eine Abfrage durchführen. Nur Analysten und Administratoren können eine Abfrage planen, um einen Aktionsalarm zu verteilen, einen Bericht unter Auswahl der enthaltenen Abfragen erstellen oder eine benutzerdefinierte Abfrage mithilfe des Abfragedesign-Assistenten erstellen. Siehe auch Archivabfrage.

Abfragebibliothek

Die *Abfragebibliothek* ist der Speicher für alle vordefinierten und benutzerdefinierten Abfragen, Abfragekennungen und Prompt-Filter.

Administratorrolle

Die *Administratorrolle* erteilt Benutzern die Berechtigung, alle gültigen Aktionen in allen Ressourcen von CA Enterprise Log Manager auszuführen. Nur Administratoren dürfen Protokollerfassung und Services konfigurieren oder Benutzer, Zugriffsrichtlinien und Zugriffsfilter verwalten.

Agent

Ein *Agent* ist ein generischer Service, der mit Connectors konfiguriert wurde, von denen jeder Rohereignisse von einer einzelnen Ereignisquelle erfasst und diese dann zur Verarbeitung an CA Enterprise Log Manager sendet. Jeder CA Enterprise Log Manager verfügt über einen integrierten Agent. Außerdem können Sie einen Agenten auf einem Remote-Sammelpunkt installieren und Ereignisse auf Hosts erfassen, auf denen keine Agenten installiert werden können. Sie können einen Agenten auch auf dem Host installieren, auf dem die Ereignisquellen ausgeführt werden, und so die Möglichkeit nutzen, für einen CA Enterprise Log Manager Unterdrückungsregeln anzuwenden und Übertragungen zu verschlüsseln.

Agenten-Explorer

Der *Agenten-Explorer* bezeichnet den Speicher für die Einstellungen der Agentenkonfiguration. (Agenten können in einem Erfassungspunkt oder in Endpunkten installiert werden, an denen Ereignisquellen vorhanden sind.)

Agentengruppe

Eine *Agentengruppe* ist eine Kennung, die Benutzer auf ausgewählte Agenten anwenden können, mit denen Benutzer eine Agentenkonfiguration gleichzeitig auf mehrere Agenten anwenden und Berichte auf der Basis der Gruppen abrufen können. Ein bestimmter Agent kann jeweils nur zu einer Gruppe gehören. Agentengruppen basieren auf benutzerdefinierten Kriterien wie der geografischen Region oder der Wichtigkeit.

Agenten-Management

Agenten-Management ist der Software-Prozess, der alle Agenten steuert, die mit allen föderierten CA Enterprise Log Managers verknüpft sind. Dabei werden die Agenten, mit denen kommuniziert wird, authentifiziert.

Aktionsabfrage

Eine *Aktionsabfrage* ist eine Abfrage, die einen Aktionsalarm unterstützt. Sie wird in einem wiederkehrenden Plan ausgeführt, um die Bedingungen zu testen, die von dem zugehörigen Aktionsalarm definiert sind.

Aktionsalarm

Ein *Aktionsalarm* ist ein geplanter Abfragejob, mit dessen Hilfe Richtlinienverletzungen, Nutzungstrends, Anmeldemuster und andere Ereignisaktionen, die ein kurzfristiges Eingreifen erfordern, ermittelt werden können. Wenn Alarmabfragen Ergebnisse zurückgeben, werden diese standardmäßig auf der Seite "Alarme" in CA Enterprise Log Manager angezeigt und außerdem einem RSS-Feed hinzugefügt. Wenn Sie einen Alarm planen, können Sie zusätzliche Ziele angeben, einschließlich E-Mail, einen CA IT PAM-Ereignis-/Alarmausgabeprozess und SNMP-Traps.

Alarmserver

Der *Alarmserver* ist der Speicher für Aktionsalarme und Aktionsalarmjobs.

Analystenrolle

Die *Analystenrolle* erteilt Benutzern die Berechtigung, benutzerdefinierte Berichte und Abfragen zu erstellen, Berichte zu bearbeiten und Anmerkungen dazu einzugeben, Kennungen zu erstellen und Berichte und Aktionswarnungen zu planen. Analysten können auch alle Auditor-Aufgaben durchführen.

Anwendungsbenutzer

Ein *Anwendungsbenutzer* ist ein globaler Benutzer, dem Detaildaten auf Anwendungsebene zugewiesen wurden. Zu den CA Enterprise Log Manager-Anwendungsbenutzerdetails gehören die Benutzergruppe und Einschränkungen der Zugriffsrechte. Wenn der Benutzerspeicher das lokale Repository ist, umfassen die Anwendungsbenutzerdetails auch die Anmeldedaten und die Kennwortrichtlinien.

Anwendungsgruppe

Eine *Anwendungsgruppe* ist eine produktspezifische Gruppe, die einem globalen Benutzer zugewiesen werden kann. Vordefinierte Anwendungsgruppen für CA Enterprise Log Manager oder Rollen sind "Administrator", "Analyst" und "Auditor". Diese Anwendungsgruppen stehen nur CA Enterprise Log Manager-Benutzern zur Verfügung. Sie können Benutzern anderer Produkte, die auf demselben CA EEM-Server registriert wurden, nicht zugewiesen werden. Benutzerdefinierte Anwendungsgruppen müssen zur Standardrichtlinie für den CALM-Anwendungszugriff hinzugefügt werden, damit die Benutzer auf CA Enterprise Log Manager zugreifen können.

Anwendungsinstanz

Eine *Anwendungsinstanz* ist ein allgemeiner Bereich imCA EEM-Repository, in dem alle Berechtigungsrichtlinien, Benutzer, Gruppen, Inhalte und Konfigurationen gespeichert werden. Normalerweise verwenden alle CA Enterprise Log Manager-Server in einem Unternehmen dieselbe Anwendungsinstanz (standardmäßig CAELM). Sie können CA Enterprise Log Manager-Server mit verschiedenen Anwendungsinstanzen installieren, aber nur die Server, die dieselbe Anwendungsinstanz gemeinsam nutzen, können föderiert werden. Server, die für die Verwendung desselben CA EEM-Servers, aber mit verschiedenen Anwendungsinstanzen konfiguriert wurden, nutzen nur den Benutzerspeicher, die Kennwortrichtlinien und die globalen Gruppen gemeinsam. Verschiedene CA-Produkte verfügen über verschiedene Standardanwendungsinstanzen.

Anwendungsressource

Eine *Anwendungsressource* ist eine der CA Enterprise Log Manager-spezifischen Ressourcen, in denen CALM-Zugriffsrichtlinien bestimmten Identitäten die Durchführung bestimmter anwendungsspezifischer Aktionen (wie der Erstellung, Planung und Bearbeitung) gewähren oder verweigern. Beispiele hierfür sind Berichte, Alarme und Integration. Sieh auch globale Ressource.

AppObjects

AppObjects oder Anwendungsobjekte sind produktspezifische Ressourcen, die in CA EEM unter der Anwendungsinstanz eines bestimmten Produkts gespeichert sind. Für die CAELM-Anwendungsinstanz umfassen diese Ressourcen Berichts- und Abfrageinhalte, geplante Berichts- und Alarmjobs, Agenteninhalte und -konfigurationen, Service-, Adapter- und Integrationskonfigurationen, Datenzuordnungs- und Nachrichtenanalysedateien sowie Unterdrückungs- und Zusammenfassungsregeln.

Archivabfrage

Eine *Archivabfrage* ist eine Abfrage des Katalogs, anhand dessen die kalten Datenbanken identifiziert werden, die wiederhergestellt und für die Abfrage verfügbar gemacht werden müssen. Eine Archivabfrage unterscheidet sich darin von einer normalen Abfrage, dass sie sich auf kalte Datenbanken bezieht, während sich normale Abfragen auf heiße, warme und verfügbar gemachte Datenbanken beziehen. Administratoren können eine Archivabfrage über die Registerkarte "Verwaltung", die Unterregisterkarte "Protokollerfassung" und die Option "Archivkatalogabfrage" starten.

Archivierte Datenbanken

Die *archivierten Datenbanken* auf einem bestimmten CA Enterprise Log Manager-Server umfassen alle warmen Datenbanken, die für die Abfrage zur Verfügung stehen, jedoch manuell gesichert werden müssen, bevor sie ablaufen, alle kalten Datenbanken, die als gesichert erfasst wurden, und alle Datenbanken, die als von einer Datensicherung wiederhergestellt erfasst wurden.

Archivkatalog

Siehe Katalog.

Assistent für Analysedateien

Der *Assistent für Analysedateien* ist eine CA Enterprise Log Manager-Funktion, mit der Administratoren XMP-Dateien (eXtensible Message Parsing), die auf dem CA Enterprise Log Manager-Verwaltungsserver gespeichert werden, erstellen, bearbeiten und analysieren können. Die Anpassung der Analyse eingehender Ereignisdaten umfasst auch die Bearbeitung vorabgestimmter Zeichenfolgen und Filter. Neue und bearbeitete Dateien werden im Protokollerfassung-Explorer, in der Ereignisverfeinerungsbibliothek, in den Analysedateien und im Benutzerordner angezeigt.

Audit-Datensätze

Audit-Datensätze enthalten Sicherheitsereignisse, wie Authentifizierungsversuche, Dateizugriffe und Änderungen an Sicherheitsrichtlinien, Benutzerkonten und Benutzerrechten. Administratoren geben an, welche Ereignistypen auditiert und welche protokolliert werden sollten.

Auditorenrolle

Die *Auditorenrolle* gewährt den Benutzern Zugriff auf Berichte und die darin enthaltenen Daten. Auditoren können Berichte, die Listen mit den Berichtvorlagen, den geplanten Berichtaufträgen und mit den generierten Berichten anzeigen. Auditoren können Berichte planen und mit Anmerkungen versehen. Auditoren haben keinen Zugriff auf die RSS-Feeds (Rich Site Summary), außer die Konfiguration erfordert keine Authentifizierung für die Anzeige von Aktionsalarmen.

Aufgezeichnetes Ereignis

Ein *aufgezeichnetes Ereignis* bezeichnet die Informationen des Rohereignisses oder des verfeinerten Ereignisses, nachdem diese in die Datenbank eingefügt wurden. Rohereignisse werden immer als verfeinerte Ereignisse erfasst, außer sie wurden unterdrückt oder zusammengefasst. Diese Informationen werden gespeichert und können durchsucht werden.

Auto-Archivierung

Auto-Archivierung ist ein konfigurierbarer Prozess, der das Verschieben von Archivdatenbanken von einem Server zu einem anderen automatisiert. In der ersten Phase der Auto-Archivierung sendet der Erfassungsserver neu archivierte Datenbanken in der von Ihnen angegebenen Häufigkeit zum Berichtsserver. In der zweiten Phase der Auto-Archivierung sendet der Berichtsserver ältere Datenbanken zur langfristigen Speicherung an den Remote-Speicher, wodurch die Notwendigkeit eines manuellen Sicherungs- und Verschiebevorgangs entfällt. Für die Auto-Archivierung müssen Sie eine Authentifizierung ohne Kennwörter vom Quell- zum Zielserver konfigurieren.

Automatische Software-Updates

Automatische Software-Updates betreffen binäre und nicht-binäre Dateien, die vom CA-Server für automatische Software-Updates zur Verfügung gestellt werden. Binärdateien sind Produktmodulaktualisierungen, die normalerweise in CA Enterprise Log Manager installiert sind. Nicht-binäre Dateien oder Inhaltsaktualisierungen werden auf dem Management-Server gespeichert.

Benutzerdefinierte MIB

Eine *benutzerdefinierte MIB* ist eine MIB, die Sie für einen an ein SNMP-Traps-Ziel wie CA NSM gesendeten Aktionsalarm erstellen. Die im Aktionsalarm festgelegte benutzerdefinierte Trap-ID geht von der Existenz einer zugeordneten benutzerdefinierten MIB aus, die die ausgewählten, als Trap gesendeten CEG-Felder definiert.

Benutzergruppe

Eine *Benutzergruppe* kann eine Anwendungsgruppe, eine globale oder eine dynamische Gruppe sein. Vordefinierte CA Enterprise Log Manager-Anwendungsgruppen sind Administrator, Analyst und Auditor. CA Enterprise Log Manager-Benutzer können über Mitgliedschaften außerhalb von CA Enterprise Log Manager zu globalen Gruppen gehören. Dynamische Gruppen sind benutzerdefiniert und werden über eine dynamische Gruppenrichtlinie erstellt.

Benutzername "EiamAdmin"

EiamAdmin ist der Standardname für den Superuser, der dem Benutzer zugewiesen wird, der die CA Enterprise Log Manager-Server installiert. Bei der Installation der ersten CA Enterprise Log Manager-Software erstellt der Installierende ein Kennwort für dieses Superuser-Konto, wenn nicht bereits ein Remote-CA EEM-Server vorhanden ist. In diesem Fall muss der Installierende das vorhandene Kennwort eingeben. Nach der Installation der Soft-Appliance öffnet der Installierende einen Browser von einer Workstation aus, gibt die URL für CA Enterprise Log Manager ein und meldet sich als "EiamAdmin" mit dem zugehörigen Kennwort an. Dieser erste Benutzer richtet den Benutzerspeicher ein, erstellt Kennwortrichtlinien sowie das erste Benutzerkonto mit Administratorrolle. Optional kann der Benutzer "EiamAdmin" jede Operation durchführen, die von CA EEM gesteuert wird.

Benutzerrolle

Eine *Benutzerrolle* kann eine vordefinierte oder eine benutzerdefinierte Anwendungsgruppe sein. Benutzerdefinierte Benutzerrollen werden benötigt, wenn die vordefinierten Anwendungsgruppen (Administrator, Analyst und Auditor) nicht ausreichend differenziert sind, um Arbeitszuweisungen zu reflektieren. Für benutzerdefinierte Benutzerrollen sind benutzerdefinierte Zugriffsrichtlinien erforderlich. Zudem muss vordefinierten Richtlinien die neue Rolle hinzugefügt werden.

Benutzerspeicher

Ein *Benutzerspeicher* ist das Repository für globale Benutzerinformationen und Kennwortrichtlinien. Der CA Enterprise Log Manager-Benutzerspeicher ist standardmäßig das lokale Repository, das jedoch so konfiguriert werden kann, dass CA SiteMinder oder ein unterstütztes LDAP-Verzeichnis wie Microsoft Active Directory, Sun One oder Novell eDirectory referenziert werden. Unabhängig davon, wie der Benutzerspeicher konfiguriert wird, enthält das lokale Repository auf dem Management-Server anwendungsspezifische Informationen über die Benutzer, wie ihre Benutzerrolle und dazugehörige Zugriffsrichtlinien.

Beobachtetes Ereignis

Ein *beobachtetes Ereignis* ist ein Ereignis, das eine Quelle, ein Ziel und einen Agenten umfasst, wobei das Ereignis von einem Ereigniserfassungsagenten beobachtet und erfasst wird.

Bericht

Ein *Bericht* ist eine grafische oder tabellarische Darstellung von Ereignisprotokolldaten, die beim Ausführen von vordefinierten oder benutzerdefinierten Abfragen mit Filtern erstellt wird. Die Daten können aus heißen, warmen und verfügbar gemachten Datenbanken im Ereignisprotokollspeicher des ausgewählten Servers und, sofern angefordert, der zugehörigen föderierten Server stammen.

Berichtsbibliothek

Die *Berichtsbibliothek* ist der Speicher für alle vordefinierten und benutzerdefinierten Berichte, Berichtskennungen und geplanten Berichtsjobs.

Berichtsserver

Der *Berichtsserver* ist der Service, der folgenden Konfigurationsinformationen speichert: den beim Mailen von Alarmen zu verwendenden E-Mail-Server, die Anzeige von Berichten, die im PDF-Format gespeichert werden, und die Beibehaltung von Richtlinien für Berichte, die auf dem Berichtsserver gespeichert werden, sowie von Alarmen, die an den RSS-Feed gesendet werden.

Berichtsserver

Ein *Berichtsserver* ist eine Rolle, die von einem CA Enterprise Log Manager-Server ausgeführt wird. Ein Berichtsserver empfängt automatisch archivierte warme Datenbanken von einem oder mehreren Erfassungsservern. Ein Berichtsserver verwaltet Abfragen, Berichte, geplante Alarme und geplante Berichte.

CA Enterprise Log Manager

CA Enterprise Log Manager ist ein Lösung, mit der Sie Protokolle weit verteilter Ereignisquellen verschiedenster Art sammeln, nach Übereinstimmungen von Abfragen und Berichten suchen und Datensätze von Datenbanken mit komprimierten Protokollen speichern können, die Sie in externe Langzeitspeicher verschoben haben.

CA IT PAM

CA IT PAM ist die Abkürzung für CA IT Process Automation Manager. Dieses CA-Produkt automatisiert von Ihnen definierte Prozesse. CA Enterprise Log Manager verwendet zwei Prozesse: den Prozess zur Erstellung eines Ereignis-/Alarmausgabeprozesses für ein lokales Produkt, wie z. B. CA Service Desk, und den Prozess zur dynamischen Erstellung von Listen, die als Schlüsselwerte importiert werden können. Für die Integration ist CA IT PAM r2.1 erforderlich.

CA Spectrum

CA Spectrum ist ein Neztwerkfehlerverwaltungsprogramm, das in CA Enterprise Log Manager integriert werden kann, um als Ziel für Alarme in Form von SNMP-Traps zu dienen.

CA-Adapter

Die *CA-Adapter* sind eine Gruppe von Listenern, die Ereignisse von CA Audit-Komponenten erhalten. Diese Komponenten umfassen CA Audit-Clients, iRecorder und SAPI-Recorder sowie Quellen, die Ereignisse nativ über iTechnology senden.

CAELM

CAELM ist der Name der Anwendungsinstanz, die CA EEM für CA Enterprise Log Manager verwendet. Um die CA Enterprise Log Manager-Funktionen in CA Embedded Entitlements Manager aufzurufen, geben Sie die URL "https://<ip_address>:5250/spin/eiam/eiam.csp" ein, dann wählen Sie "CAELM" als Anwendungsnamen und geben das Kennwort des Benutzers "EiamAdmin" ein.

caelmadmin

Der Benutzername und das Kennwort *caelmadmin* sind Anmeldeinformationen, die für den Zugriff auf das Betriebssystem der Soft-Appliance benötigt werden. Die Benutzerkennung "caelmadmin" wird während der Installation des Betriebssystems erstellt. Während der Installation der Software-Komponente muss der Installierende das Kennwort für das CA EEM-Superuser-Konto, EiamAdmin, eingeben. Dem Konto "caelmadmin" wird dasselbe Konto zugewiesen. Es empfiehlt sich, dass sich der Server-Administrator über "ssh" als "caelmadmin"-Benutzer anmeldet und dieses Kennwort ändert. Auch wenn der Administrator sich nicht über "ssh" als Root anmelden kann, kann er bei Bedarf Benutzer zu "Root" (su root) wechseln lassen.

caelmservice

Der *caelmservice* bezeichnet eine Service-Konto, das es ermöglicht, dass iGateway und die lokalen CA EEM-Services als Nicht-Root-Benutzer ausgeführt werden können. Das caelmservice-Konto wird für die Installation von Betriebssystemaktualisierungen verwendet, die mit automatischen Software-Updates heruntergeladen werden.

CALM

CALM ist eine vordefinierte Ressourcenklasse, die folgende CA Enterprise Log Manager-Ressourcen umfasst: Alarm, ArchiveQuery, calmTag, Daten, EventGrouping, Integration und Bericht. Folgende Aktionen sind in dieser Ressourcenklasse zulässig: Anmerken (Berichte), Erstellen (Alarm, calmTag, EventGrouping, Integration und Bericht), Datenzugriff (Daten), Ausführen (ArchiveQuery) und Planen (Alarm, Bericht).

CALM-Anwendungszugriffsrichtlinie

Die *CALM-Anwendungszugriffsrichtlinie* ist ein Zugriffssteuerungslistentyp einer Richtlinie zur Bereichsdefinierung, die festlegt, wer sich in CA Enterprise Log Manager anmelden darf. Anmeldungszugriff wird standardmäßig dem [Gruppen-]Administrator, dem [Gruppen-] Analysen und dem [Gruppen-]Auditor erteilt.

calmTag

calmTag ist ein benanntes Attribut für das Anwendungsobjekt, das bei der Erstellung einer Richtlinie zur Bereichsdefinierung verwendet wird, um Benutzer auf bestimmte Berichte und Abfragen zu beschränken, die zu bestimmten Kennungen gehören. Alle Berichte und Abfrage sind Anwendungsobjekte und haben "calmTag" als Attribut. (Dies ist nicht zu verwechseln mit der Ressource "Kennung".)

CA-Server für automatische Software-Updates

Der *CA-Server für automatische Software-Updates* ist die Quelle für automatische Aktualisierungen aus CA.

CEG-Felder

CEG-Felder sind Label, mit denen die Darstellung von Rohereignisfeldern aus unterschiedlichen Ereignisquellen standardisiert wird. Während der Verfeinerung von Ereignissen wandelt CA Enterprise Log Manager Rohereignismeldungen in Namen-/Wertepaare um und ordnet die Namen der Rohereignisse Standard-CEG-Feldern zu. Bei dieser Verfeinerung entstehen Namen-/Wertepaare, die aus CEG-Feldern und -Werten aus dem Rohereignis bestehen. So werden unterschiedliche Labels aus Rohelementen für dasselbe Datenobjekt oder Netzwerkelement bei der Verfeinerung von Rohereignissen in denselben CEG-Feldnamen umgewandelt. CEG-Felder werden in der MIB der SNMP-Traps bestimmten OIDs zugeordnet.

Client für automatische Software-Updates

Ein *Client für automatische Software-Updates* ist ein CA Enterprise Log Manager-Server, der Inhaltsaktualisierungen von einem anderen CA Enterprise Log Manager-Server erhält, der als Proxy-Server für automatische Software-Updates bezeichnet wird. Clients für automatische Software-Updates fragen den konfigurierten Proxy-Server in regelmäßigen Abständen ab und rufen neue Aktualisierungen bei Verfügbarkeit ab. Nach dem Abrufen der Aktualisierungen installiert der Client die heruntergeladenen Komponenten.

Computersicherheitsprotokoll-Verwaltung

Die *Computersicherheitsprotokoll-Verwaltung* wird durch NIST als "der Prozess zum Generieren, Übertragen, Speichern, Analysieren und Entsorgen von Computersicherheitsprotokoll-Daten" definiert.

Connector

Ein *Connector* ist eine Integration für eine bestimmte Ereignisquelle, die in einem bestimmten Agenten konfiguriert wurde. Ein Agent kann mehrere Connectors ähnlicher oder verschiedener Typen in den Speicher laden. Der Connector ermöglicht die Erfassung von Rohereignissen von einer Ereignisquelle und die regelbasierte Übertragung konvertierter Ereignisse in einen Ereignisprotokollspeicher, wo sie in die heiße Datenbank eingefügt werden. Standardisierte Integrationen liefern eine optimierte Erfassung einer breiten Palette von Ereignisquellen, einschließlich Betriebssystemen, Datenbanken, Webservern, Firewalls und diversen Arten von Sicherheitsanwendungen. Sie können einen Connector für eine selbstentwickelte Ereignisquelle von Anfang an selbst definieren, oder Sie verwenden eine Integration als Vorlage.

Datenbankstatus "heiß"

Der *Datenbankstatus "heiß"* bezeichnet den Status der Datenbank im Ereignisprotokollspeicher, wenn neue Ereignisse eingefügt werden. Wenn die heiße Datenbank eine konfigurierbare Größe auf dem Erfassungsserver erreicht, wird sie komprimiert, katalogisiert und in den warmen Speicher auf dem Berichtsserver verschoben. Außerdem speichern alle Server neue selbstüberwachende Ereignisse in einer heißen Datenbank.

Datenbankstatus "kalt"

Der *Datenbankstatus "kalt"* wird einer warmen Datenbank zugewiesen, wenn ein Administrator das Hilfsprogramm "LMArchive" ausführt, um CA Enterprise Log Manager zu benachrichtigen, dass die Datenbank gesichert wurde. Administratoren müssen warmen Datenbanken sichern und dieses Hilfsprogramm ausführen, bevor die Datenbanken gelöscht werden. Eine warme Datenbank wird automatisch gelöscht, wenn ihr Alter den für "Maximale Anzahl an Archivtagen" konfigurierten Wert erreicht oder wenn der für "Festplattenspeicher für Archiv" konfigurierte Schwellenwert erreicht wird, je nachdem, welcher Wert zuerst erreicht wird. Sie können die Archivdatenbank abfragen, um kalte und warme Datenbanken zu ermitteln.

Datenbankstatus "verfügbar gemacht"

Der *Datenbankstatus "verfügbar gemacht"* ist der Status, der einer Datenbank zugewiesen wird, die im Archivverzeichnis wiederhergestellt wurde, nachdem der Administrator das Hilfsprogramm "LMArchive" ausgeführt hat, um CA Enterprise Log Manager mitzuteilen, dass die Datenbank wiederhergestellt wurde. Verfügbar gemachte Datenbanken bleiben für die Anzahl der Stunden erhalten, die für die Exportrichtlinie konfiguriert wurde. Ereignisprotokolle können in Datenbanken mit dem Status "heiß", "warm" und "verfügbar gemacht" abgefragt werden.

Datenbankstatus "warm"

Der *Datenbankstatus "warm"* bezeichnet den Status, in dem eine heiße Datenbank von Ereignisprotokollen verschoben wird, wenn die Größe (Maximale Zeilenanzahl) der heißen Datenbank überschritten wird oder wenn nach der Wiederherstellung einer kalten Datenbank in einem neuen Ereignisprotokollspeicher eine Neukatalogisierung durchgeführt wird. Warme Datenbanken werden komprimiert und im Ereignisprotokollspeicher beibehalten, bis ihr Alter (in Tagen) den konfigurierten Wert für "Maximale Anzahl an Archivtagen" überschreitet. Ereignisprotokolle können in Datenbanken mit dem Status "heiß", "warm" und "verfügbar gemacht" abgefragt werden.

Datenbankstatuswerte

Es gibt folgende *Datenbankstatuswerte:* "heiß" für eine nicht komprimierte Datenbank mit neuen Ereignissen, "warm" für eine Datenbank mit komprimierten Ereignissen, "kalt" für eine gesicherte Datenbank und "verfügbar gemacht" für eine Datenbank, die im Ereignisprotokollspeicher wiederhergestellt wurde, auf dem sie gesichert wurde. Sie können heiße, warme und verfügbar gemachte Datenbanken abfragen. Eine Archivabfrage zeigt die Informationen von kalten Datenbanken an.

Datenzugriff

Datenzugriff ist eine Art der Berechtigung, die allen CA Enterprise Log Managers über die Standarddatenzugriffsrichtlinie in der CALM-Ressourcenklasse gewährt wird. Alle Benutzer haben Zugriff auf alle Daten, außer wenn diese durch Datenzugriffsfilter eingeschränkt sind.

Datenzuordnung

Datenzuordnung ist der Prozess der Zuordnung der Schlüsselwertpaare in CEG. Die Datenzuordnung wird durch eine DM-Datei gesteuert.

Datenzuordnung von Dateien

Unter der *Datenzuordnung von Dateien* versteht man XML-Dateien, die die CA-ELM-Schemadefinition (CEG) verwenden, um Ereignisse vom Ursprungsformat in ein CEG-kompatibles Format zu übertragen, das zur Berichterstellung und Analyse im Ereignisprotokollspeicher gespeichert werden kann. Für jeden Protokollnamen wird eine Datenzuordnungsdatei benötigt, bevor die Ereignisdaten gespeichert werden können. Die Benutzer können eine Kopie der Datenzuordnungsdatei ändern und diese auf einen angegebenen Connector anwenden.

Delegierungsrichtlinie

Eine *Delegierungsrichtlinie* ist eine Zugriffsrichtlinie, mit der ein Benutzer seine Rechte auf einen anderen Benutzer, eine andere Anwendungsgruppe, eine andere globale oder dynamische Gruppe übertragen kann. Delegierungsrichtlinien, die von einem gelöschten oder deaktivierten Benutzer erstellt wurden, müssen explizit gelöscht werden.

Direkte Protokollerfassung

Direkte Protokollerfassung bezeichnet die Protokollerfassungsmethode, bei der es keinen unmittelbaren Agenten zwischen Ereignisquelle und der CA Enterprise Log Manager-Software gibt.

Dynamische Benutzergruppe

Eine *dynamische Benutzergruppe* setzt sich aus globalen Benutzern zusammen, die ein oder mehrere Attribute gemeinsam haben. Eine dynamische Benutzergruppe wird über eine spezielle Richtlinie für dynamische Benutzergruppen erstellt, wobei der Ressourcenname der Name der dynamischen Benutzergruppe ist und die Mitgliedschaft auf einer Gruppe von Filtern basiert, die anhand von Benutzer- und Gruppenattributen erstellt wird.

EEM-Benutzer

Der *EEM-Benutzer*, der im Auto-Archivierungsbereich des Ereignisprotokollspeichers konfiguriert wird, gibt den Benutzer an, der eine Archivabfrage durchführen, die Archivdatenbank neu katalogisieren, das Hilfsprogramm "LMArchive" und das Shellskript "restore-ca-elm" zur Wiederherstellung von Archivdatenbanken zur Prüfung ausführen kann. Dem Benutzer muss die vordefinierte Rolle des Administrators oder eine benutzerdefinierte Rolle mit einer benutzerdefinierten Richtlinie zugewiesen werden, die die Aktion "Bearbeiten" in der Datenbankressource zulässt.

Eingabeaufforderung

Eine *Eingabeaufforderung* ist ein besonderer Typ von Abfrage, durch die Ergebnisse basierend auf dem eingegebenen Wert und den ausgewählten CEG-Feldern angezeigt werden. Es werden nur Zeilen für Ereignisse zurückgegeben, bei denen der eingegebene Wert in mindestens einem der ausgewählten CEG-Felder angezeigt wird.

ELM-Schemadefinition (CEG)

Die *ELM-Schemadefinition* ist das Schema, das ein Standardformat enthält, in das CA Enterprise Log Manager-Ereignisse mithilfe von Analysen und Zuordnungen konvertiert werden, bevor diese im Ereignisprotokollspeicher gespeichert werden. CEG verwendet allgemeine, normalisierte Felder, um die Sicherheitsereignisse von verschiedenen Plattformen und Produkten zu definieren. Ereignisse, die nicht analysiert oder zugeordnet werden können, werden als Rohereignisse gespeichert.

EPHI-Berichte

Die *EPHI-Berichte* sind Berichte, die sich auf die HIPAA-Sicherheit beziehen, wobei EPHI für Electronic Protected Health Information (Elektronisch geschützte Gesundheitsinformationen) steht. Mit diesen Berichten können Sie einfach demonstrieren, dass alle einzeln feststellbaren Gesundheitsinformationen der Patienten, die elektronisch erstellt, verwaltet oder übertragen werden, auch geschützt sind.

Ereignis-/Alarmausgabeprozess

Der *Ereignis-/Alarmausgabeprozess* ist der IT PAM-Prozess von CA, durch den ein Produkt eines anderen Herstellers aufgerufen wird, um auf Alarmdaten zu reagieren, die in CA Enterprise Log Manager konfiguriert werden. Sie können einen CA IT PAM-Prozess beim Planen eines Alarmjobs als Ziel auswählen. Wenn ein Alarm zur Ausführung des CA IT PAM-Prozesses führt, sendet CA Enterprise Log Manager CA IT PAM-Alarmdaten. CA IT PAM leitet diese zusammen mit eigenen Verarbeitungsparametern als Teil des Ereignis-/Alarmausgabeprozesses an das Produkt des anderen Herstellers weiter.

Ereignisaggregation

Unter *Ereignisaggregation* versteht man den Prozess, in dem ähnliche Protokolleinträge in einen Eintrag konsolidiert werden, der die Anzahl der Vorkommnisse des Ereignisses enthält. Über Zusammenfassungsregeln wird definiert, wie Ereignisse aggregiert werden.

Ereignisaktion (event_action)

Die *Ereignisaktion* ist das ereignisspezifische Feld auf der vierten Ebene der Ereignisnormalisierung, das von CEG verwendet wird. Es beschreibt allgemeine Aktionen. Beispieltypen für Ereignisaktionen sind Start und Stopp eines Prozesses oder Anwendungsfehler.

Ereigniserfassung

Ereigniserfassung bezeichnet das Lesen der Rohereigniszeichenfolge aus einer Ereignisquelle und das Senden dieser an den konfigurierten CA Enterprise Log Manager. Auf die Ereigniserfassung folgt die Ereignisverfeinerung.

Ereignisfilterung

Ereignisfilterung ist der Prozess, in dem Ereignisse auf der Basis von CEG-Filtern verworfen werden.

Ereigniskategorie (event_category)

Die *Ereigniskategorie* ist das ereignisspezifische Feld auf der zweiten Ebene der Ereignisnormalisierung, das von CEG verwendet wird. Es dient der weiteren Klassifizierung von Ereignissen mit einen speziellen Idealmodell. Ereigniskategorietypen umfassen die Betriebssicherheit, das Identitäten-Management, das Konfigurations-Management, den Ressourcen- und Systemzugriff.

Ereigniskategorien

Ereigniskategorien sind Kennungen, anhand derer CA Enterprise Log Manager-Ereignisse nach ihrer Funktion klassifiziert, bevor sie in den Ereignisspeicher eingefügt werden.

Ereignisklasse (event_class)

Die *Ereignisklasse* ist das ereignisspezifische Feld auf der dritten Ebene der Ereignisnormalisierung, das von CEG verwendet wird. Es dient der weiteren Klassifizierung von Ereignissen mit einer speziellen Ereigniskategorie.

Ereignisprotokollspeicher

Der Ereignisprotokollspeicher ist das Ergebnis des Archivierungsprozesses, bei dem der Benutzer eine warme Datenbank sichert, CA Enterprise Log Manager durch Ausführen des Hilfsprogramms "LMArchive" benachrichtigt und die gesicherte Datenbank aus dem Ereignisprotokollspeicher in den langfristigen Speicher verschiebt.

Ereignisprotokollspeicher

Der *Ereignisprotokollspeicher* ist eine Komponente im CA Enterprise Log Manager-Server, bei der eingehende Ereignisse in Datenbanken gespeichert werden. Die Datenbanken im Ereignisprotokollspeicher müssen vor dem Zeitpunkt, der für den Löschvorgang konfiguriert wurde, manuell gesichert werden und zu einer Remote-Protokollspeicherlösung verschoben werden. Archivierte Datenbanken können in einem Ereignisprotokollspeicher wiederhergestellt werden.

Ereignisquelle

Eine *Ereignisquelle* ist der Host, von dem ein Connector Rohereignisse erfasst. Eine Ereignisquelle kann mehrere Protokollspeicher enthalten, auf die jeweils durch einen separaten Connector zugegriffen wird. Die Bereitstellung eines neuen Connectors umfasst gewöhnlich die Konfiguration der Ereignisquelle, so dass der Agent darauf zugreifen und Rohereignisse aus einem der zugehörigen Protokollspeicher lesen kann. Rohereignisse für das Betriebssystem, andere Datenbanken und verschiedene Sicherheitsanwendungen werden separat für die Ereignisquelle gespeichert.

Ereignisse

Ereignisse in CA Enterprise Log Manager sind Protokolldatensätze, die von jeder angegebenen Ereignisquelle generiert werden.

Ereignisverfeinerung

Ereignisverfeinerung bezeichnet den Prozess, in dem die Zeichenfolge eines erfassten Rohereignisses in die jeweiligen Ereignisfelder und die zugeordneten CEG-Felder analysiert wird. Benutzer können Abfragen durchführen, um die Ergebnisse der verfeinerten Ereignisdaten anzuzeigen. Die Ereignisverfeinerung findet nach der Ereigniserfassung und vor der Ereignisspeicherung statt.

Ereignisverfeinerungs-Bibliothek

Die *Ereignisverfeinerungs-Bibliothek* ist der Speicher für vordefinierte und benutzerdefinierte Integrationen, für Zuordnungs- und Analysedateien sowie für Unterdrückungs- und Zusammenfassungsregeln.

Ereignisweiterleitungsregeln

Ereignisweiterleitungsregeln geben an, dass ausgewählte Ereignisse nach der Speicherung im Ereignisprotokoll-Speicher an Produkte anderer Hersteller weitergeleitet werden sollen, beispielsweise an Produkte zur Korrelation von Ereignissen.

Erfassungspunkt

Ein *Erfassungspunkt* ist ein Server, auf dem ein Agent installiert ist und bei dem sich der Server in unmittelbarer Netzwerknähe zu allen Servern mit Ereignisquellen befindet, die mit den Connectors des Agenten verknüpft sind.

Erfassungsserver

Ein *Erfassungsserver* ist eine Rolle, die von einem CA Enterprise Log Manager-Server ausgeführt wird. Ein Erfassungsserver verfeinert eingehende Ereignisprotokolle, fügt sie in die heiße Datenbank ein, komprimiert die heiße Datenbank und archiviert oder kopiert sie automatisch auf den entsprechenden Berichtsserver. Der Erfassungsserver komprimiert die heiße Datenbank, sobald diese die konfigurierte Größe erreicht hat, und archiviert sie automatisch entsprechend dem konfigurierten Plan.

Filter

Ein *Filter* ist ein Mittel, mit dem Sie eine Abfrage für den Ereignisprotokollspeicher eingrenzen können.

FIPS 140-2

FIPS 140-2 ist der Federal Information Processing Standard (FIPS). Dieser Bundesstandard gibt die Sicherheitsanforderungen für kryptographische Module an, die innerhalb eines Sicherheitssystems zum Schutz von sensiblen, nicht klassifizierten Daten verwendet werden. Der Standard gibt vier Qualitätsstufen der Sicherheit vor, die darauf abzielen, einen großen Bereich potenzieller Anwendungen und Umgebungen abzudecken.

FIPS-Modus

FIPS-Modus ist die Einstellung, die erfordert, dass CA Enterprise Log Manager-Server und -Agenten FIPS-zertifizierte kryptographische Module aus RSA zur Verschlüsselung verwenden. Die alternative Einstellung dazu ist der Nicht-FIPS-Modus.

Föderationsserver

Föderationsserver sind CA Enterprise Log Manager-Server, die in einem Netzwerk miteinander verbunden sind, um die erfassten Protokolldaten zu verteilen, aber um die erfassten Daten für die Berichterstellung zu aggregieren. Föderationsserver können hierarchisch oder über eine vernetzte Topologie verbunden werden. Berichte von föderierten Daten umfassen Daten vom Zielserver sowie Daten von Unter- oder Gleichordnungen dieses Servers, sofern vorhanden.

Funktionszuordnungen

Funktionszuordnungen sind ein optionaler Teil der Datenzuordnungsdatei für eine Produktintegration. Mit einer Funktionszuordnung kann ein CEG-Feld gefüllt werden, wenn der benötigte Wert nicht direkt vom Quellereignis abgerufen werden kann. Alle Funktionszuordnungen bestehen aus dem Namen des CEG-Feldes, einem vordefinierten oder Klassenfeldwert und der Funktion, mit der der Wert abgerufen oder berechnet wird.

Gespeicherte Konfiguration

Eine *gespeicherte Konfiguration* ist eine gespeicherte Konfiguration mit den Werten für die Datenzugriffsattribute einer Integration, die als Vorlage bei der Erstellung einer neuen Integration verwendet werden kann.

Globale Gruppe

Eine *globale Gruppe* ist eine Gruppe, die von mehreren Anwendungsinstanzen gemeinsam verwendet wird, die im selben CA Enterprise Log Manager-Management-Server registriert sind. Jeder Benutzer kann einer oder mehreren globalen Gruppen zugeordnet werden. Zugriffsrichtlinien können mit globalen Gruppen als Identitäten definiert werden, denen die Durchführung bestimmter Aktionen in ausgewählten Ressourcen gewährt oder verweigert wird.

Globale Konfiguration

Die *global Konfiguration* bezeichnet eine Reihe von Einstellungen, die alle CA Enterprise Log Manager-Server betreffen, die denselben Management-Server verwenden.

Globale Ressource

Eine *globale Ressource* für das CA Enterprise Log Manager-Produkt ist eine Ressource, die mit anderen CA-Anwendungen gemeinsam genutzt wird. Sie können Richtlinien zur Bereichsdefinierung mit globalen Ressourcen erstellen. Beispiele hierfür sind Benutzer, Richtlinien und Kalender. Siehe auch Anwendungsressource.

Globaler Benutzer

Bei einem *globalen Benutzer* handelt es sich um die Benutzerkontoinformationen ohne anwendungsspezifische Details. Die Details und eines globalen Benutzers und die Mitgliedschaften einer globalen Gruppe werden gemeinsam in allen CA-Anwendungen genutzt, die mit dem Standardbenutzerspeicher integriert werden können. Die Details globaler Benutzer können im eingebetteten Repository oder in einem externen Verzeichnis gespeichert werden.

Globaler Filter

Ein *globaler Filter* ist ein Satz von Kriterien, die Sie angeben können und mit denen die in den Berichten angezeigten Daten begrenzt werden können. Beispielsweise zeigt ein globaler Filter für die letzten 7 Tage nur die Ereignisse an, die in den letzten sieben Tagen generiert wurden.

Hierarchische Föderation

Eine *hierarchische Föderation* von CA Enterprise Log Manager-Servern ist eine Topologie, die eine hierarchische Beziehung zwischen Servern einrichtet. In seiner einfachsten Form ist dies der Fall, wenn Server 2 ein untergeordneter Server von Server 1 ist, Server 1 jedoch nicht Server 2 untergeordnet ist. Dies bedeutet, dass die Beziehung nur in eine Richtung geht. Eine hierarchische Föderation kann mehrere Ebenen von über- und untergeordneten Beziehungen haben, und ein einzelner übergeordneter Server kann mehrere untergeordnete Server haben. Eine föderierte Abfrage gibt die Ergebnisse vom ausgewählten Server und all seinen untergeordneten Servern zurück.

Hilfsprogramm "LMArchive"

Das *Hilfsprogramm "LMArchive"* ist das Befehlszeilenhilfsprogramm, mit dem die Sicherung und Wiederherstellung von Archivdatenbanken zum Ereignisprotokollspeicher auf einem CA Enterprise Log Manager-Server verfolgt wird. Mit "LMArchive" können Sie die Liste der warmen Datenbankdateien abfragen, die für die Archivierung bereit sind. Nach der Sicherung der aufgelisteten Datenbank und nach deren Verschieben in den langfristigen (kalten) Speicher können Sie mit "LMArchive" einen Datensatz im CA Enterprise Log Manager erstellen, dass diese Datenbank gesichert wurde. Nach der Wiederherstellung einer kalten Datenbank in ihrem ursprünglichen CA Enterprise Log Manager können Sie mit "LMArchive" CA Enterprise Log Manager benachrichtigen, der dann die Datenbankdateien wiederum verfügbar macht, so dass sie abgefragt werden können.

Hilfsprogramm "LMSEOSImport"

Das Hilfsprogramm *LMSEOSImport* ist ein Befehlszeilenhilfsprogramm, mit dem SEOSDATA oder vorhandene Ereignisse als Teil der Migration von Audit Reporter, Viewer oder Audit Collector in CA Enterprise Log Manager importiert werden. Dieses Hilfsprogramm wird nur von Microsoft Windows und Sun Solaris Sparc unterstützt.

Hilfsprogramm "scp"

Die Sicherheitskopie *scp* (Kopierprogramm für Remote-Dateien) ist ein UNIX-Hilfsprogramm, das Dateien zwischen UNIX-Computern in einem Netzwerk transferiert. Dieses Hilfsprogramm wird während der CA Enterprise Log Manager-Installation für Sie zur Verfügung gestellt, damit Sie Dateien für automatische Software-Updates vom Online-Proxy zum Offline-Proxy für Software-Updates transferieren können.

HTTP-Proxy-Server

Ein *HTTP-Proxy-Server* ist ein Proxy-Server, der wie eine Firewall agiert und dafür sorgt, dass Internet-Traffic das Unternehmen nur über den Proxy betritt und wieder verlässt. Wenn bei ausgehendem Verkehr eine ID und ein Kennwort angegeben werden, kann der Proxy-Server umgangen werden. Beim Verwalten automatischer Software-Updates kann die Verwendung eines lokalen HTTP-Proxy-Servers konfiguriert werden.

Idealmodell (ideal_model)

Das *Idealmodell* stellt die Technologie dar, die das Ereignis ausdrückt. Dies ist das erste CEG-Feld in einer Hierarchie von Feldern, die für die Ereignisklassifikation und -normalisierung verwendet werden. Beispiele eines Idealmodells sind z. B. Antivirus, DBMS, Firewall, Betriebssystem und Webserver. Die Firewall-Produkte Check Point, Cisco PIX und Netscreen/Juniper könnten mit dem Wert "Firewall" im Feld "ideal_model" normalisiert werden.

Identität

Eine *Identität* in CA Enterprise Log Manager ist eine Benutzergruppe, die Zugriff auf die CAELM-Anwendungsinstanz und ihre Ressourcen hat. Eine Identität für ein CA-Produkt kann ein globaler Benutzer, ein Anwendungsbenutzer, eine globale Gruppe, eine Anwendungsgruppe oder eine dynamische Gruppe sein.

Inhaltsaktualisierungen

Inhaltsaktualisierungen sind der nicht-binäre Anteil der automatischen Software-Updates, die auf dem CA Enterprise Log Manager-Management-Server gespeichert werden. Inhaltsaktualisierungen umfassen Inhalte, wie XMP-Dateien, Datenzuordnungsdateien, Konfigurationsaktualisierungen für CA Enterprise Log Manager-Module und Aktualisierungen öffentlicher Schlüssel.

Installierender

Der *Installierende* ist derjenige, der die Soft-Appliance und die Agenten installiert. Während des Installationsprozesses werden die Benutzernamen "caelmadmin" und "EiamAdmin" erstellt, und das für "EiamAdmin" angegebene Kennwort wird "caelmadmin" zugewiesen. Diese "caelmadmin"-Anmeldeinformationen werden für den ersten Zugriff auf das Betriebssystem benötigt, die "EiamAdmin"-Anmeldeinformationen werden für den ersten Zugriff auf die CA Enterprise Log Manager-Software und für die Installation der Agenten benötigt.

Integration

Integration ist das Mittel, mit dem nicht klassifizierte Ereignisse in verfeinerte Ereignisse verarbeitet werden, so dass sie in Abfragen und Berichten angezeigt werden. Die Integration wird mit einem Satz von Elementen implementiert, die es einem bestimmten Agenten und Connector ermöglichen, Ereignisse von einem oder mehreren Typen von Ereignisquellen zu erfassen und zu CA Enterprise Log Manager zu senden. Der Satz von Elementen umfasst den Protokollsensor und die XMP- und DM-Dateien, die aus einem bestimmten Produkt lesen sollen. Beispiele für vordefinierte Integrationen sind die für die Verarbeitung von Syslog- und WMI-Ereignissen. Sie können benutzerdefinierte Integrationen erstellen, um die Verarbeitung nicht klassifizierter Ereignisse zu ermöglichen.

Integrationselemente

Integrationselemente umfassen einen Sensor, eine Konfigurationshilfe, eine Datenzugriffsdatei, eine oder mehrere XMP-Nachrichtenanalysedateien und eine oder mehrere Datenzuordnungsdateien.

iTech-Ereignis-Plugin

Das *iTech-Ereignis-Plugin* ist ein CA-Adapter, den ein Administrator mit ausgewählten Zuordnungsdateien konfigurieren kann. Er erhält Ereignisse von Remote-iRecorders, CA EEM, iTechnology selbst oder von einem Produkt, das Ereignisse über iTechnology sendet.

Kalender

Ein *Kalender* ist ein Mittel, mit dem Sie die Gültigkeitsdauer einer Zugriffsrichtlinie begrenzen können. Eine Richtlinie ermöglicht bestimmten Identitäten die Durchführung bestimmter Aktionen in einer angegebenen Ressource während eines definierten Zeitraums.

Katalog

Der *Katalog* ist die Datenbank auf jedem CA Enterprise Log Manager, die den Status der archivierten Datenbanken beibehält und gleichzeitig als Index höchster Ebene für alle Datenbanken agiert. Die Statusinformationen (warm, kalt oder verfügbar gemacht) werden für alle Datenbanken beibehalten, die sich je auf diesem CA Enterprise Log Manager befunden haben, und für jede Datenbank, die auf diesem CA Enterprise Log Manager als verfügbar gemachte Datenbank wiederhergestellt wurde. Die Indizierungsfähigkeit erstreckt sich auf alle heißen und warmen Datenbanken im Ereignisprotokollspeicher auf diesem CA Enterprise Log Manager.

Kennung

Eine *Kennung* ist ein Term oder eine Schlüsselphrase, mit der Abfragen oder Berichte identifiziert werden, die zur selben geschäftsrelevanten Gruppierung gehören. Kennungen ermöglichen Suchläufe, die auf geschäftsrelevanten Gruppierungen basieren. Eine Kennung ist außerdem der Ressourcenname, der in einer Richtlinie verwendet wird, die dem Benutzer die Berechtigung zur Erstellung einer Kennung erteilt.

Kompatibel mit FIPS 140-2

Kompatibel mit FIPS 140-2 ist die Bezeichnung für ein Produkt, das *optional* FIPS-konforme kryptographische Bibliotheken und Algorithmen nutzen kann, um sensible Daten zu verschlüsseln und zu entschlüsseln. CA Enterprise Log Manager ist ein FIPS-kompatibles Protokollerfassungsprodukt, da Sie auswählen können, ob es im FIPS-Modus oder im Nicht-FIPS-Modus ausgeführt werden soll.

Konform mit FIPS 140-2

Konform mit FIPS 140-2 ist die Bezeichnung für ein Produkt, das standardmäßig *nur* Verschlüsselungsalgorithmen verwendet, die von einem akkreditierten Labor für Cryptographic Module Testing (CMT) zertifiziert sind. CA Enterprise Log Manager kann auf zertifizierte RSA BSAFE Crypto-C ME-und Crypto-J-Bibliotheken basierte kryptographische Module in FIPS-Modus verwenden, tut dies jedoch möglicherweise nicht standardmäßig.

Konto

Ein *Konto* bezeichnet einen globalen Benutzer, der auch ein CALM-Anwendungsbenutzer ist. Eine einzelne Person kann mehr als ein Konto haben, jedoch muss die benutzerdefinierte Rolle eine andere sein.

Lokaler Filter

Ein *lokaler Filter* ist ein Satz von Kriterien, die Sie während der Berichtsanzeige angeben können, um die angezeigten Daten für den aktuellen Bericht zu begrenzen.

Lokales Ereignis

Ein *lokales Ereignis* ist ein Ereignis, das eine einzelne Einheit umfasst, bei der sich Quelle und Ziel des Ereignisses auf demselben Hostrechner befinden. Ein lokales Ereignis entspricht Typ 1 der vier Ereignistypen, die in der ELM-Schemadefinition (CEG) verwendet werden.

Management-Server

Der *Management-Server* ist eine Rolle, die dem ersten installierten CA Enterprise Log Manager-Server zugewiesen ist. Dieser CA Enterprise Log Manager-Server enthält das Repository, in dem gemeinsam genutzte Inhalte, wie Richtlinien, für all seine CA Enterprise Log Managers gespeichert werden. Dieser Server ist normalerweise der Standard-Proxy für automatische Software-Updates. Auch wenn dies in den meisten produktiven Umgebungen nicht empfehlenswert ist, so kann der Management-Server alle Rollen ausführen.

MIB (Management Information Base)

Die *MIB (Management Information Base)* für CA Enterprise Log Manager, CA-ELM.MIB, muss für jedes Produkt, das Alarme in Form von SNMP-Traps von CA Enterprise Log Manager erfassen soll, importiert und konfiguriert werden. Die MIB zeigt die Quelle der numerischen OIDs (Objekt-ID) an, die in einer SNMP-Trap-Meldung verwendet werden, zusammen mit einer Beschreibung des Datenobjekts oder Netzwerkelements. In der MIB für SNMP-Traps, die von CA Enterprise Log Manager gesendet werden, bezieht sich die Beschreibung der einzelnen Datenobjekte auf das entsprechende CEG-Feld. Die MIB stellt sicher, dass alle Namen-/Wertepaare aus einer SNMP-Trap am Ziel korrekt interpretiert werden.

Modul für automatische Software-Updates

Das *Modul für automatische Software-Updates* ist ein Dienst, bei dem automatische Software-Updates über den CA-Software-Update-Server automatisch heruntergeladen und an CA Enterprise Log Manager-Server und an alle Agenten verteilt werden können. Globale Einstellungen gelten für lokale CA Enterprise Log Manager-Server. Lokale Einstellungen geben an, ob der Server ein Offline-Proxy, ein Online-Proxy oder ein Client für automatische Software-Updates ist.

Module (zum Herunterladen)

Ein *Modul* ist eine logische Gruppierung von Komponentenaktualisierungen, die über ein automatisches Software-Update zum Herunterladen zur Verfügung gestellt wird. Ein Modul kann binäre Aktualisierungen, Inhaltsaktualisierungen oder beides enthalten. Beispielsweise bilden alle Berichte ein Modul und alle Sponsor-Binäraktualisierungen ein anderes. CA definiert, was ein Modul ausmacht.

Nachrichtenanalyse

Die *Analyse*, auch als Nachrichtenanalyse bezeichnet, umfasst den Prozess der Umwandlung roher Gerätedaten in Schlüsselwertpaare. Die Nachrichtenanalyse wird durch eine XMP-Datei gesteuert. Die Analyse, die der Datenzuordnung vorausgeht, ist ein Schritt des Integrationsprozesses, der das von einer Ereignisquelle erfasste Rohereignis in ein verfeinertes Ereignis umwandelt, das Sie anzeigen können.

Nachrichtenanalyse

Nachrichtenanalyse bezeichnet die Anwendung von Regeln auf die Analyse eines Rohereignisprotokolls, um relevante Informationen (wie Zeitstempel, IP-Adresse und Benutzername) abzurufen. Analyseregeln arbeiten mit der Zeichenübereinstimmung, um einen bestimmten Ereignistext zu suchen und diesen mit den ausgewählten Werten zu verknüpfen.

Nachrichtenanalysebibliothek

Die *Nachrichtenanalysebibliothek* ist eine Bibliothek, die Ereignisse aus den Listener-Warteschlangen übernimmt und reguläre Ausdrücke verwendet, um Zeichenfolgen in Token-Namenwertpaare zu übersetzen.

Nachrichtenanalysedatei (XMP)

Eine *Nachrichtenanalysedatei (XMP)* ist eine XML-Datei, die mit einem bestimmten Ereignisquellentyp verknüpft ist, der Analyseregeln anwendet. Analyseregeln zerlegen die relevanten Daten in einem erfassten Rohereignis in Namenswertepaare, die dann zur weiteren Verarbeitung an die Datenzuordnungsdatei weitergeleitet werden. Dieser Dateityp wird in allen Integrationen sowie in Connectors verwendet, die auf Integrationen basieren. Im Falle von CA-Adaptern können XMP-Dateien auch auf dem CA Enterprise Log Manager-Server angewendet werden.

Nachrichtenanalyse-Token (ELM)

Ein *Nachrichtenanalyse-Token* ist eine wiederverwendbare Vorlage für die Erstellung einer regulären Ausdruckssyntax, die bei der CA Enterprise Log Manager-Nachrichtenanalyse verwendet wird. Ein Token verfügt über einen Namen, einen Typ und eine entsprechende Zeichenfolge für den regulären Ausdruck.

Natives Ereignis

Ein *natives Ereignis* ist der Zustand oder die Aktion, die ein Rohereignis auslöst. Native Ereignisse werden empfangen, entsprechend analysiert/zugeordnet und dann als Rohereignisse oder verfeinerte Ereignisse übertragen. Eine fehlgeschlagene Authentifizierung ist ein natives Ereignis.

Neukatalogisierung

Eine *Neukatalogisierung* ist eine erzwungene Neuerstellung des Katalogs. Die Neukatalogisierung ist nur erforderlich, wenn Daten im Ereignisprotokollspeicher eines anderen Servers wiederhergestellt werden als auf dem Server, auf dem sie generiert wurden. Wenn Sie einen CA Enterprise Log Manager als Wiederherstellungspunkt für Untersuchungen von kalten Daten bestimmen, müssen Sie eine Neukatalogisierung der Datenbank immer dann erzwingen, nachdem diese auf dem festgelegten Wiederherstellungspunkt wiederhergestellt wurde. Eine Neukatalogisierung wird ggf. automatisch durchgeführt, wenn iGateway erneut gestartet wird. Die Neukatalogisierung einer einzelnen Datenbank kann mehrere Stunden in Anspruch nehmen.

Nicht interaktive ssh-Authentifizierung

Nicht interaktive Authentifizierung aktiviert Dateien dazu, sich von einem Server zum anderen zu verschieben, ohne dass die Eingabe einer Passphrase zur Authentifizierung erforderlich ist. Legen Sie, bevor Sie automatische Archivierung konfigurieren oder das restore-ca-elm.sh-Skript verwenden, die nicht interaktive Authentifizierung vom Quellserver zum Zielserver fest.

Nicht-FIPS-Modus

Nicht-FIPS-Modus ist die Standardeinstellung, die es CA Enterprise Log Manager-Servern und -Agenten ermöglicht, eine Kombination aus verschiedenen Verschlüsselungsverfahren zu verwenden, von denen einige nicht FIPS-konform sind. Die alternative Einstellung dazu ist der FIPS-Modus.

NIST

Das *National Institute of Standards and Technology (NIST)* ist die Bundesagentur, die Empfehlungen in ihrer Special Publication 800-92 *Guide to Computer Security Log Management* (Leitfaden für die Computersicherheitsprotokoll-Verwaltung) gibt, die als Basis für CA Enterprise Log Manager verwendet wurde.

ODBC- und JDBC-Zugriff

Durch den *ODBC- und JDBC-Zugriff* auf CA Enterprise Log Manager-Ereignisprotokoll-Speicher wird die Verwendung von Ereignisdaten mit einer Vielzahl von Produkten anderer Hersteller unterstützt, darunter die benutzerdefinierte Berichterstellung zu Ereignissen mit Berichterstellungstools anderer Hersteller, die Ereigniskorrelation mit Korrellations-Engines und die Ereignisauswertung durch Produkte für die Erkennung von Sicherheitsverletzungen (Intrusion Detection) und Malware. Auf Systemen mit Windows-Betriebssystemen wird der ODBC-Zugriff verwendet, auf UNIX- und Linux-Systemen hingegen der JDBC-Zugriff.

ODBC-Server

Der *ODBC-Server* ist der konfigurierte Service, der den für die Kommunikation zwischen dem ODBC- oder JDBC-Client und dem CA Enterprise Log Manager-Server verwendeten Port festlegt und angibt, ob SSL-Verschlüsselung verwendet werden soll.

OID (Objekt-ID)

Eine *OID (Objekt-ID)* ist eine eindeutige numerische ID für ein Datenobjekt, das mit Werten in einer SNMP-Trap-Meldung verbunden wird. Alle OIDs, die in einer CA Enterprise Log Manager-SNMP-Trap verwendet werden, werden einem CEG-Textfeld in der MIB zugeordnet. Jede OID, die einem CEG-Feld zugeordnet ist, hat folgende Syntax: 1.3.6.1.4.1.791.9845.x.x.x, wobei 791 die Unternehmensnummer für CA und 9845 die Produkt-ID für CA Enterprise Log Manager ist.

Ordner

Ein *Ordner* ist ein Verzeichnispfad-Speicherort, an dem der CA Enterprise Log Manager-Management-Server die CA Enterprise Log Manager-Objekttypen speichert. Sie sollten Ordner in Richtlinien zur Bereichsdefinierung referenzieren, um Benutzern die Berechtigung zum Zugriff auf einen bestimmten Objekttyp zu erteilen oder zu verweigern.

Pflichtrichtlinie

Eine *Pflichtrichtlinie* ist eine Richtlinie, die beim Erstellen eines Zugriffsfilters automatisch erstellt wird. Sie sollten nicht versuchen, eine Pflichtrichtlinie direkt zu erstellen, zu bearbeiten oder zu löschen. Erstellen, bearbeiten oder löschen Sie stattdessen den Zugriffsfilter.

pozFolder

Der *pozFolder* ist ein Attribut des Anwendungsobjekts, wobei der Wert dem übergeordneten Pfad des Anwendungsobjekt entspricht. Attribut und Wert von "pozFolder" werden in Filtern für Zugriffsrichtlinien verwendet, die den Zugriff auf Ressourcen wie Berichte, Abfragen und Konfigurationen einschränken.

Profil

Ein *Profil* ist ein optionaler, konfigurierbarer Satz von Kennungs- und Datenfiltern, die produktspezifisch, technologiespezifisch oder auf eine ausgewählte Kategorie beschränkt sind. Ein Kennungsfilter für ein Produkt beschränkt beispielsweise die gelisteten Kennungen auf die ausgewählte Produktkennung. Datenfilter für ein Produkt zeigen in den von Ihnen generierten Berichten, den von Ihnen geplanten Alarmen und den von Ihnen angezeigten Abfrageergebnissen nur die Daten für das angegebene Produkt an. Nachdem Sie das gewünschte Profil erstellt haben, können Sie es, sobald Sie angemeldet sind, jederzeit aktivieren. Wenn Sie mehrere Profile erstellen, können Sie in einer Sitzung verschiedene Profile, jeweils eins nach dem anderen auf Ihre Aktivitäten anwenden. Vordefinierte Filter erhalten Sie mit den automatischen Software-Updates.

Protokoll

Ein *Protokoll* ist ein Audit-Datensatz oder eine erfasste Nachricht eines Ereignisses oder mehrerer Ereignisse. Ein Protokoll kann ein Audit-Protokoll, ein Transaktionsprotokoll, ein Intrusionsprotokoll, ein Verbindungsprotokoll, ein Systemleistungsdatensatz, ein Benutzeraktivitätsprotokoll oder ein Alarm sein.

Protokollanalyse

Protokollanalyse ist eine Untersuchung der Protokolleinträge, um relevante Ereignisse festzustellen. Wenn Protokolle nicht zeitnah analysiert werden, verringert sich ihr Wert beträchtlich.

Protokollanalyse

Protokollanalyse ist der Prozess der Datenextraktion aus einem Protokoll, damit die analysierten Werte in einem Folgestadium der Protokollverwaltung verwendet werden können.

Protokollarchivierung

Protokollarchivierung bezeichnet den Prozess, der auftritt, wenn die heiße Datenbank ihre Maximalgröße erreicht, wenn eine Komprimierung auf Zeilenebene durchgeführt wird und der Status von heiß in warm geändert wird. Administratoren müssen die warme Datenbank sichern, bevor die Schwelle zum Löschen erreicht wird, und sie müssen das Hilfsprogramm "LMArchive" ausführen, um den Namen der Sicherungen zu erfassen. Diese Informationen stehen dann zur Anzeige über die Archivabfrage zur Verfügung.

Protokolldatensatz

Ein *Protokolldatensatz* ist ein einzelner Audit-Datensatz.

Protokolleintrag

Ein *Protokolleintrag* ist ein Eintrag in einem Protokoll, der Informationen zu einem bestimmten Ereignis enthält, das in einem System oder Netzwerk aufgetreten ist.

Protokollsensor

Ein *Protokollsensor* ist eine Integrationskomponente, die Daten aus einem bestimmten Typ lesen soll, wie z. B. aus Datenbank, Syslog, Datei oder SNMP. Protokollsensoren werden wiederverwendet. Normalerweise erstellen die Benutzer keine benutzerdefinierten Protokollsensoren.

Proxy für automatische Software-Updates (offline)

Ein *Offline-Proxy für automatische Software-Updates* ist ein CA Enterprise Log Manager-Server, der automatische Software-Updates über eine manuelle Verzeichniskopie (unter Verwendung von scp) von einem Online-Proxy für automatische Software-Updates erhält. Offline-Proxys für automatische Software-Updates können so konfiguriert werden, dass Sie binäre Updates zu Clients herunterladen, die diese anfordern, und dass sie die aktuellste Version der Inhaltsaktualisierungen an den Management-Server weiterleiten, wenn dieser sie noch nicht erhalten hat. Offline-Proxys für automatische Software-Updates benötigen keinen Internetzugang.

Proxy für automatische Software-Updates (online)

Ein *Online-Proxy für automatische Software-Updates* ist ein CA Enterprise Log Manager-Server mit Internetzugang, der automatische Software-Updates nach einem wiederkehrenden Zeitplan von einem CA-Server für automatische Software-Updates erhält. Ein bestimmter Online-Proxy für automatische Software-Updates kann für einen oder mehrere Clients in die Proxy-List aufgenommen werden. Dieser kontaktiert die aufgelisteten Proxys im Ringversuch, um binäre Aktualisierungen anzufordern. Ein bestimmter Online-Proxy leitet, wenn er so konfiguriert wurde, neue Inhalts- und Konfigurationsaktualisierungen an den Management-Server weiter, wenn diese nicht bereits von einem anderen Proxy weitergeleitet wurden. Das Verzeichnis für automatische Software-Updates eines ausgewählten Online-Proxys wird beim Kopieren von Aktualisierungen in Offline-Proxys automatischer Software-Updates als Quelle verwendet.

Proxy für automatische Software-Updates (Standardwert)

Der *Standard-Proxy für automatische Software-Updates* ist normalerweise der CA Enterprise Log Manager-Server, der als erster installiert wurde und der auch der primäre CA Enterprise Log Manager sein kann. Der Standard-Proxy für automatische Software-Updates ist außerdem ein Online-Proxy für automatische Software-Updates und muss daher über einen Internetzugang verfügen. Wenn keine anderen Online-Proxys für automatische Software-Updates definiert werden, erhält dieser Server die automatischen Software-Updates vom CA-Server für automatische Software-Updates, lädt die Binäraktualisierungen an alle Clients herunter und leitet die Inhaltsaktualisierungen an CA EEM weiter. Wenn andere Proxys definiert sind, erhält dieser Server die automatischen Software-Updates immer noch, aber er wird von Clients nur dann wegen Aktualisierungen kontaktiert, wenn keine Proxy-Liste für automatische Software-Updates konfiguriert wurde bzw. wenn die konfigurierte Liste erschöpft ist.

Proxys für Software-Updates (für Client)

Die *Proxys für Software-Updates für den Client* bilden die Proxy-Liste für automatische Software-Updates, die der Client in einem Ringversuch kontaktiert, um die CA Enterprise Log Manager-Software- und die Betriebssystem-Software-Updates abzurufen. Wenn ein Proxy beschäftigt ist, wird der nächste in der Liste kontaktiert. Wenn keiner zur Verfügung steht und der Client online ist, wird der Standard-Proxy für Software-Updates verwendet.

Proxys für Software-Updates (für Inhaltsaktualisierungen)

Proxys für Software-Updates (für Inhaltsaktualisierungen) sind die Proxys, die für die Aktualisierung des CA Enterprise Log Manager-Management-Servers mit Inhaltsaktualisierungen ausgewählt wurden, die vom CA-Server für automatische Software-Updates heruntergeladen werden. Ein bewährtes Verfahren ist die Konfiguration mehrerer Proxys aus Gründen der Redundanz.

Prozess mit dynamischen Werten

Ein *Prozess mit dynamischen Werten* ist ein CA IT PAM-Prozess, den Sie aufrufen, um die Werteliste für einen in Berichten oder Alarmen verwendeten, ausgewählten Schlüssel aufzufüllen oder zu aktualisieren. Sie stellen den Pfad zum Prozess mit dynamischen Werten als Teil der IT PAM-Konfiguration für die Service-Liste des Berichtsservers auf der Registerkarte "Verwaltung" bereit. Im Abschnitt "Werte", der mit den Schlüsselwerten auf derselben Seite der Benutzeroberfläche verknüpft ist, klicken Sie auf "Liste der dynamischen Werte importieren". Das Aufrufen des Prozesses mit dynamischen Werten ist eine von drei Möglichkeiten, wie Sie den Schlüsseln Werte hinzufügen können.

Remote-Ereignis

Ein *Remote-Ereignis* ist ein Ereignis, das zwei verschiedene Hostrechner umfasst, die Quelle und das Ziel. Ein Remote-Ereignis entspricht Typ 2 der vier Ereignistypen, die in der ELM-Schemadefinition (CEG) verwendet werden.

Remote-Speicher-Server

Ein *Remote-Speicher-Server* ist eine Rolle, die einem Server zugewiesen wird, der automatisch archivierte Datenbanken von einem oder mehreren Berichtsservern empfängt. In einem Remote-Speicher-Server können kalte Datenbanken für die benötigte Anzahl an Jahren gespeichert werden. Auf dem Remote-Host, der zum Speichern verwendet wird, sind normalerweise kein CA Enterprise Log Manager oder andere Produkte installiert. Konfigurieren Sie für die Auto-Archivierung eine nicht-interaktive Authentifizierung.

Richtlinie zur Bereichsdefinierung

Eine *Richtlinie zur Bereichsdefinierung* ist ein Typ einer Zugriffsrichtlinie, die den Zugriff auf Ressourcen, die auf dem Management-Server gespeichert sind, (wie z. B. Anwendungsobjekte, Benutzer, Gruppen, Ordner und Richtlinien) gewährt oder verweigert. Mit der Richtlinie zur Bereichsdefinierung werden die Identitäten festgelegt, die auf die angegebenen Ressourcen zugreifen dürfen.

Rohereignis

Ein *Rohereignis* stellt die Informationen dar, die von einem nativen Ereignis ausgelöst werden, das von einem Überwachungsagenten zum Protokollmanager-Collector gesendet wird. Das Rohereignis wird häufig als Syslog-Zeichenfolge oder als Namenswertpaare formatiert. Es ist möglich, ein Ereignis in seiner Rohform in CA Enterprise Log Manager anzuzeigen.

RSS-Ereignis

Ein *RSS-Ereignis* ist ein Ereignis, das von CA Enterprise Log Manager generiert wird, um einen Aktionsalarm an Drittanbieterprodukte und -benutzer zu leiten. Das Ereignis besteht aus einer Zusammenfassung aller Aktionsalarmergebnisse und einem Link zur Ergebnisdatei. Die Dauer eines bestimmten RSS-Feed-Elements ist konfigurierbar.

RSS-Feed-URL für Aktionsalarme

Die *RSS-Feed-URL für Aktionsalarme* lautet: https://{elmhostname}:5250/spin/calm/getActionQueryRssFeeds.csp. Von dieser URL können Sie das maximale Alter sowie die maximale Menge für Aktionsalarme anzeigen, die zu dieser Konfiguration gehören.

RSS-Feed-URL für Software-Updates

Die *RSS-Feed-URL für Software-Updates* ist ein vorkonfigurierter Link, der von Online-Proxy-Servern für Software-Updates bei der Abfrage von automatischen Software-Updates verwendet wird. Diese URL ist für den CA-Server für automatische Software-Updates bestimmt.

SafeObject

SafeObject ist eine vordefinierte Ressourcenklasse in CA EEM. Es ist die Ressourcenklasse, zu der Anwendungsobjekte, die im Bereich der Anwendung gespeichert sind, gehören. Benutzer, die Richtlinien und Filter für die Erteilung des Zugriffs auf Anwendungsobjekte definieren, beziehen sich auf diese Ressourcenklasse.

SAPI-Collector

Der *SAPI-Collector* ist ein CA-Adapter, der Ereignisse von CA Audit-Clients erhält. CA Audit-Clients senden mit der Aktion "Collector", die über einen integrierten Failover verfügt. Administratoren konfigurieren den CA Audit-SAPI-Collector beispielsweise mit ausgewähltem Chiffre und Datenzuordnungsdateien.

SAPI-Recorder

Ein *SAPI-Recorder* bezeichnet die Technologie, die vor iTechnology zum Versenden von Informationen an CA Audit verwendet wurde. SAPI steht für Submit Application Programming Interface (API starten). CA Audit-Recorder für CA ACF2, CA Top Secret, RACF, Oracle, Sybase und DB2 sind Beispiele für SAPI-Recorder.

SAPI-Router

Der *SAPI-Router* ist ein CA-Adapter, der Ereignisse aus Integrationen erhält, wie z. B. Mainframe, und diese an einen CA Audit-Router.

Schlüsselwerte

Schlüsselwerte sind benutzerdefinierte Werte, die einer benutzerdefinierten Liste (Schlüsselgruppe) zugewiesen werden. Wenn eine Abfrage eine Schlüsselgruppe verwendet, enthalten die Suchergebnisse Übereinstimmungen mit beliebigen Schlüsselwerten in der Schlüsselgruppe. Es gibt mehrere vordefinierte Schlüsselgruppen, einige von diesen enthalten vordefinierte Schlüsselwerte, die in vordefinierten Abfragen und Berichten verwendet werden.

Selbstüberwachendes Ereignis

Ein *selbstüberwachendes Ereignis* ist ein Ereignis, das von CA Enterprise Log Manager protokolliert wird. Solche Ereignisse werden automatisch durch Aktionen generiert, die von angemeldeten Benutzern und Funktionen durchgeführt wurden, die wiederum von verschiedenen Modulen wie den Services oder Listeners ausgeführt wurden. Der Bericht für SIM-Operationen/selbstüberwachende Ereignisdetails kann angezeigt werden, indem Sie einen Berichtsserver auswählen und die Registerkarte "Selbstüberwachende Ereignisse" öffnen.

Services

Die CA Enterprise Log Manager-*Services* sind Ereignisprotokollspeicher, Berichtsserver und automatisches Software-Update. Administratoren konfigurieren diese Services auf einer globalen Ebene, bei der standardmäßig alle Einstellungen auf alle CA Enterprise Log Managers angewendet werden. Die meisten globalen Einstellungen für Services können auf der lokalen Ebene, also für jeden angegebenen CA Enterprise Log Manager, überschrieben werden.

SNMP

SNMP ist ein Akronym und steht für "Simple Network Management Protocol", einen offenen Standard zum Senden von Warnmeldungen in Form von SNMP-Traps von einem Agentensystem an mehrere Managementsysteme.

SNMP-Trap-Inhalte

Eine *SNMP-Trap* besteht aus Namen-/Wertepaaren, wobei jeder Name eine OID (Objekt-ID) und jeder Wert ein zurückgegebener Wert aus dem geplanten Alarm ist. Abfrageergebnisse, die von einem Aktionsalarm zurückgegeben werden, bestehen aus CEG-Feldern und ihren Werten. SNMP-Traps werden ausgefüllt, indem die CEG-Felder der Namen in den Namen-/Wertepaaren durch OIDs ersetzt werden. Die Zuordnung zwischen CEG-Feld und OID wird in der MIB gespeichert. Die SNMP-Trap enthält nur Namen-/Wertepaare für Felder, die Sie beim Konfigurieren des Alarms ausgewählt haben.

SNMP-Trap-Ziele

Beim Planen von Aktionsalarmen können ein oder mehrere *SNMP-Trap-Ziele* hinzugefügt werden. Für jedes SNMP-Trap-Ziel wird eine IP-Adresse und eine Port konfiguriert. Das Ziel ist typischerweise ein NOC oder ein Verwaltungsserver, z. B. CA Spectrum oder CA NSM. Eine SNMP-Trap wird an die konfigurierten Ziele gesendet, wenn Abfragen für einen geplanten Alarmjob Ergebnisse zurückgeben.

Soft-Appliance

Soft-Appliance ist ein vollständig funktionelles Softwarepaket, das sowohl die Software als auch das zugrunde liegende Betriebssystem und alle abhängigen Pakete enthält. Es wird durch Starten auf dem Installationsdatenträger von Soft-Appliance auf vom Endbenutzer zur Verfügung gestellter Hardware installiert.

Standardagent

Der *Standardagent* ist der integrierte Agent, der mit dem CA Enterprise Log Manager-Server installiert wird. Er kann für die direkte Erfassung von Syslog-Ereignissen sowie von Ereignissen von verschiedenen Nicht-Syslog-Ereignisquellen wie CA Access Control r12 SP1, Microsoft Active Directory-Zertifikatdiensten und Oracle9i-Datenbanken konfiguriert werden.

Unterdrückung

Unterdrückung ist der Prozess, in dem Ereignisse auf der Basis von CEG-Filtern verworfen werden. Die Unterdrückung wird durch eine SUP-Datei gesteuert.

Unterdrückungsregeln

Unterdrückungsregeln sind Regeln, die Sie konfigurieren, um zu verhindern, dass bestimmte verfeinerte Ereignisse in Ihren Berichten angezeigt werden. Sie können permanente Unterdrückungsregeln erstellen, um nicht sicherheitsrelevante Routineereignisse zu unterdrücken. Sie können aber auch temporäre Regeln erstellen, um die Protokollierung geplanter Ereignisse, wie die Erstellung vieler neuer Benutzer, zu unterdrücken.

URL für CA Embedded Entitlements Manager

Die *URL für CA Embedded Entitlements Manager* (CA EEM) lautet: https://<ip_address>:5250/spin/eiam. Um sich anzumelden, wählen Sie "CAELM" als die Anwendung und geben das Kennwort ein, das mit dem Benutzernamen "EiamAdmin" verknüpft ist.

URL für CA Enterprise Log Manager

Die *URL für CA Enterprise Log Manager* lautet: https://<ip_address>:5250/spin/calm. Um sich anzumelden, geben Sie den Benutzernamen, der vom Administrator für dieses Konto definiert wurde, sowie den zugehörige Kennwort ein. Oder Sie geben "EiamAdmin", den Standardnamen des Superusers, und das zugehörige Kennwort ein.

Varbind

Eine *Varbind* ist eine SNMP-variable Verbindung. Jede Varbind besteht aus einem OID, einem Typ, und einem Wert. Sie fügen Varbinds zu einer benutzerdefinierten MIB hinzu.

Verfeinertes Ereignis

Ein *verfeinertes Ereignis* sind zugeordnete oder verfeinerte Ereignisdaten, die von einem Rohereignis oder von zusammengefassten Ereignissen stammen. CA Enterprise Log Manager führt die Zuordnung und Analyse aus, damit die gespeicherten Informationen durchsucht werden können.

Verfügbarmachung

Die *Verfügbarmachung* bezeichnet die Statusänderung einer Datenbank von "kalt" in "verfügbar gemacht". Der Prozess wird von CA Enterprise Log Manager durchgeführt, wenn dieser vom Hilfsprogramm "LMArchive" benachrichtigt wird, dass eine bekannte kalte Datenbank wiederhergestellt wurde. (Wenn die kalte Datenbank nicht auf ihrem ursprünglichen CA Enterprise Log Manager wiederhergestellt wird, das Hilfsprogramm "LMArchive" nicht verwendet wird und eine Verfügbarmachung nicht erforderlich ist, wird die wiederhergestellte Datenbank bei der Neukatalogisierung als warme Datenbank hinzugefügt.)

Vernetzte Föderation

Eine *Vernetzte Föderation* von CA Enterprise Log Manager-Servern ist eine Topologie, die eine gleichartige Beziehung zwischen Servern einrichtet. In seiner einfachsten Form ist dies der Fall, wenn Server 2 ein untergeordneter Server von Server 1 ist und umgekehrt. Ein vernetztes Paar von Servern hat eine Beziehung, die in beide Richtungen geht. Eine vernetzte Föderation kann so definiert werden, dass viele Server alle untereinander gleichrangig sind. Eine föderierte Abfrage gibt die Ergebnisse vom ausgewählten Server und all seinen gleichrangigen Servern zurück.

Verwaltung von Berechtigungen

Die *Verwaltung von Berechtigungen* ist ein Mittel zur Steuerung der Aktionen, die Benutzer durchführen dürfen, sobald sie sich authentifiziert und an der CA Enterprise Log Manager-Oberfläche angemeldet haben. Dies geschieht über Zugriffsrichtlinien, die mit den Rollen, die den Benutzern zugewiesen wurden, verknüpft werden. Rollen, oder Anwendungsbenutzergruppen, und Zugriffsrichtlinien können vordefiniert oder benutzerdefiniert sein. Die Verwaltung von Berechtigungen wird über den internen CA Enterprise Log Manager-Benutzerspeicher gehandhabt.

Visualisierungskomponenten

Visualisierungskomponenten sind verfügbare Optionen, mit denen Berichtsdaten einschließlich Tabelle, Diagramm (Zeilendiagramm, Balkendiagramm, Spaltendiagramm, Kreisdiagramm) oder ein Ereignis angezeigt werden können.

Wiederherstellungspunkt-Server

Ein *Wiederherstellungspunkt-Server* ist eine Rolle, die von einem CA Enterprise Log Manager-Server ausgeführt wird. Um "kalte" Ereignisse zu untersuchen, können Sie Datenbanken mit einem Hilfsprogramm vom Remote-Speicher zum Wiederherstellungspunkt-Server verschieben, dann die Datenbanken zum Katalog hinzufügen und Abfragen durchführen. Das Verschieben kalter Datenbanken zu einem bestimmten Wiederherstellungspunkt-Server ist eine alternative Methode dazu, sie aus Untersuchungsgründen zurück zum ursprünglichen Server zu verschieben.

XMP-Dateianalyse

XMP-Dateianalyse ist der Prozess, der vom Nachrichtenanalyse-Hilfsprogramm durchgeführt wird, um alle Ereignisse zu suchen, die jede vorabgestimmte Zeichenfolge enthalten, und um bei einem übereinstimmendem Ereignis das Ereignis mit dem ersten gefundenen Filter, der dieselbe vorabgestimmte Zeichenfolge verwendet, in Tokens zu analysieren.

Zertifikate

Die vordefinierten *Zertifikate*, die von CA Enterprise Log Manager verwendet werden, sind CAELMCert.cer und CAELM_AgentCert.cer. Alle CA Enterprise Log Manager-Services verwenden CAELMCert.cer, um mit dem Verwaltungsserver zu kommunizieren. Alle Agenten verwenden CAELM_AgentCert.cer, um mit ihrem Sammelserver zu kommunizieren.

Zugriffsfilter

Ein *Zugriffsfilter* kann vom Administrator festgelegt werden, um zu steuern, welche Ereignisdaten Benutzer oder Gruppen ohne Administratorrechte anzeigen können. So kann ein Zugriffsfilter beispielsweise den Datenumfang in Berichten einschränken, der von bestimmten Identitäten eingesehen werden kann. Zugriffsfilter werden automatisch in Pflichtrichtlinien konvertiert.

Zugriffsrichtlinie

Eine *Zugriffsrichtlinie* ist eine Regel, die einer Identität (Benutzer oder Benutzergruppe) Zugriffsrechte auf eine Anwendungsressource gewährt oder verweigert. CA Enterprise Log Manager bestimmt anhand der Übereinstimmung von Identitäten, Ressourcen, Ressourcenklassen und der Auswertung der Filter, welche Richtlinien für einen bestimmten Benutzer gelten.

Zugriffssteuerungsliste für Identitäten

Mit der *Zugriffssteuerungsliste für Identitäten* können Sie verschiedene Aktionen angeben, die ausgewählten Identitäten in ausgewählten Ressourcen gewährt werden sollen. Beispielsweise können Sie mit der Zugriffssteuerungsliste für Identitäten angeben, dass eine Identität Berichte erstellen und eine andere Berichte planen und anmerken kann. Eine Zugriffssteuerungsliste für Identitäten unterscheidet sich darin von einer Zugriffssteuerungsliste, dass sie sich auf Identitäten und nicht auf Ressourcen richtet.

Zuordnungsanalyse

Eine *Zuordnungsanalyse* ist ein Schritt im Assistenten zur Dateizuordnung, bei dem Sie eine Datenzuordnungsdatei testen und ändern können. Beispielereignisse werden mit der Datenzuordnungsdatei verglichen, und die Ergebnisse werden mit CEG geprüft.

Zusammenfassungsregeln

Zusammenfassungsregeln fassen bestimmte gängige, native Ereignistypen zu einem verfeinerten Ereignis zusammen. Eine Zusammenfassungsregel kann beispielsweise so konfiguriert werden, dass sie bis zu 1000 doppelte Ereignisse, die dieselben Quell- und Ziel-IP-Adressen und Ports haben, durch ein Zusammenfassungsereignis ersetzt. Diese Regeln vereinfachen die Ereignisanalyse und verringen das Protokollaufkommen.

Index

F

G

H

I

K

N

P

S

U

V