CA Enterprise Log Manager

Administrationshandbuch

Release 12.5.01

CA-Produktreferenzen

Dieses Dokument bezieht sich auf die folgenden Produkte von CA:

- CA Access Control
- 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

Die folgenden Abschnitte wurden seit der letzten Version dieser Dokumentation aktualisiert: Services und CA-Adapter, Abfragen und Berichte und Agenten.

Es sind beispielsweise folgende Themen betroffen:

- Services und CA-Adapter:
  - Service-Konfigurationen: Neue und aktualisierte Themen, um die Änderungen in den Aktualisierungen der Schlüsselliste, die Integration mit ObserveIT und Überlegungen zum Berichtsserver abzudecken.
- Abfragen und Berichte:
  - Format für Datum/Uhrzeit: Neue Themen, um die Konfiguration der Funktion "Format für Datum/Uhrzeit" abzudecken.
  - Anzeigen von Abfragen: Aktualisiertes Thema, um die Änderung in der Abfrageansicht abzudecken.
  - Schlüsselliste: Aktualisiertes Thema, um die Änderung im IT PAM-Prozesses mit dynamischen Werten abzudecken.
- Agenten:
  - Konfiguration von Agenten und Agentengruppen: Aktualisierte Themen, um die Änderungen in den Agentenprozessen abzudecken.
  - Agentendiagnosedatei: Neues Thema, um das neue Hilfsprogramm zur Agentendiagnose abzudecken.

Weitere Informationen:

Konfigurieren der CA IT PAM-Integration (siehe Seite 162)
ObserveIT-Integration (siehe Seite 164)
Hinweise zum Berichtsserver (siehe Seite 177)
Format für Datum/Uhrzeit (siehe Seite 293)
Anzeigen von Abfragen (siehe Seite 297)
Erstellen einer Liste mit Schlüssel (siehe Seite 372)
Agenten konfigurieren (siehe Seite 693)
Hinzufügen von Agenten zu einer Agentengruppe (siehe Seite 703)
Erstellen einer Agentendiagnosedatei für Support (siehe Seite 715)

Inhalt

Kapitel 4: Benutzerdefinierte Rollen und Richtlinien 75

Kapitel 1: Einführung

Dieses Kapitel enthält folgende Themen:

Über dieses Handbuch

Dieses *Administrationshandbuch zu CA Enterprise Log Manager Administration Guide* behandelt Aufgaben, die nach der Installation von CA Enterprise Log Manager und der anfänglichen Serverkonfiguration durch den Administrator ausgeführt werden. Einige dieser Aufgaben werden zur Implementierung seltener Änderungen im System durchgeführt. Bei anderen handelt es sich um Routineaufgaben, die nach einem festgelegten Plan ausgeführt werden. Wiederum andere Aufgaben finden im Rahmen einer kontinuierlichen Überwachung statt.

Dieses Handbuch richtet sich an alle Benutzer. Hierzu zählen:

- Administratoren, die die Konfiguration des Produkts und die Protokollspeicherung sowie automatische Software-Updates verwalten
- Analysten, die mit Hilfe von Berichten die Umgebung überwachen, benutzerdefinierte Berichte erstellen und die Generierung von Alarmen planen
- Auditoren, die Berichte planen, mit Hilfe von Abfragen und Berichten die Einhaltung von Standards prüfen und Berichte mit Anmerkungen versehen

Dieses Handbuch schließt ein Glossar und einen Index ein. Im Folgenden finden Sie eine Übersicht über den Inhalt:

Abschnitt	Inhalt
Benutzerkonten	Benutzerkonten mit vordefinierten Rollen konfigurieren und Benutzerkonten selbst verwalten
Richtlinien	Benutzerdefinierte Rollen und zugehörige Richtlinien planen und dazu vordefinierte Rollen und Richtlinien nutzen
Benutzerdefinierte Rollen und Richtlinien	Benutzerzugriff mit benutzerdefinierten Rollen, benutzerdefinierten Richtlinien und Zugriffsfiltern beschränken

Abschnitt	Inhalt
Services und CA-Adapter	Ereignisprotokollspeicher, Berichtsserver, Service für automatische Software-Updates und bestimmte Ereignisadapter konfigurieren
Protokollspeicherung	Autoarchivierung konfigurieren und archivierte Datenbanken wiederherstellen
Automatisches Software-Update	Konfiguration für automatische Software-Updates verwalten, Updates anwenden und Sicherung von automatischen Software-Updates wiederherstellen
Filter und Profile	In einem Bericht, in einer Abfrage oder in allen Berichten und Abfragen mit Filtern angezeigte Daten begrenzen. Begrenzung der Kennungsliste, der Abfrageliste und der Berichtsliste mit Profilen
Abfragen und Berichte	Abfragen und Berichte erstellen, bearbeiten sowie importieren oder exportieren, um aktuelle und kürzlich erstellte Ereignisprotokolle anzuzeigen
Aktionsalarme	Aktionsalarme zur Benachrichtigung von Benutzern oder SNMP-Trap-Zielen oder zur Ausführung eines IT PAM-Prozesses bei bestimmten Ereignissen erstellen
Geplante Berichte	Berichtsjobs planen und verwalten sowie generierte Berichte anzeigen und mit Anmerkungen versehen
Unterdrückung und Zusammenfassung	Zusammenfassungs- und Unterdrückungsregeln erstellen und verwenden, um die Serverlast zu reduzieren und die Erfassung oder Verarbeitung von unerwünschten Ereignissen zu verhindern
Zuordnen und analysieren	Zuordnungs- und Analyseregeln erstellen und verwenden, um Rohereignisse in verschiedenen Formaten zu verfeinern und in standardisierte, CEG-kompatible Werte umzuwandeln; Regeln für die Ereignisweiterleitung erstellen
Integrationen und Connectors	Produktintegrationen erstellen, die es Ihnen bei einer Bereitstellung in Form von Connectors ermöglichen, Ereignisse von einer einzelnen Ereignisquelle zu verfeinern und an den CA Enterprise Log Manager-Server zu senden
Agenten	Verwendung von Agenten planen, Agenteninstallation vorbereiten, Agenten und Agentengruppen konfigurieren und automatische Software-Updates auf Agenten anwenden
Benutzerdefinierte Zertifikate	Benutzerdefinierte Zertifikate implementieren, um vordefinierte Zertifikate zu ersetzen

Abschnitt	Inhalt
Eingabehilfen	Steuerelemente für Eingabehilfen verwenden
Zugreifen auf erfasste Ereignisse mit ODBC/JDBC	Benutzerdefinierte Berichte mit einem Drittanbieterprogramm für die Berichterstellung konfigurieren oder ausgewählte Protokolldaten mit Drittanbieterprodukten abrufen

Hinweis: Genaue Informationen zur Betriebssystemunterstützung und zu den Systemanforderungen finden Sie in den *Versionshinweisen*. Ein Lernprogramm zur Einrichtung eines einzelnen Systems, so dass Sie Ergebnisse von Abfragen erfasster Syslog- und Windows-Ereignisse anzeigen können, finden Sie im *Übersichtshandbuch* .Schrittweise Anleitungen für die Installation von CA Enterprise Log Manager und die erste Konfiguration finden Sie im *Implementierungshandbuch.* Weitere Informationen zum Installieren von Agenten finden Sie im *Agent-Installationshandbuch*. Informationen zur Verwendung aller Seiten in CA Enterprise Log Manager finden Sie in der Online-Hilfe.

Kapitel 2: Benutzerkonten

Dieses Kapitel enthält folgende Themen:

Selbstverwaltungsaufgaben

Benutzer mit Zugriff auf CA Enterprise Log Manager können ihr eigenes Kennwort ändern und die Sperre eines gesperrten Benutzerkontos aufheben, wenn der konfigurierte Benutzerspeicher der Standardspeicher CA Enterprise Log Manager-Benutzerspeicher ist.

Wenn der Administrator ein neues Benutzerkonto erstellt, wird ein neues Kennwort zugewiesen. Der Benutzer ändert dieses Kennwort bei der ersten Anmeldesitzung in ein neues Kennwort, das den Kennwortrichtlinien entspricht, die angeben, ob ein mit dem Benutzernamen übereinstimmendes Kennwort zulässig ist, die die Mindestlänge und die maximal zulässige Länge, die maximale Anzahl an wiederholten Zeichen sowie die Mindestanzahl an numerischen Zeichen angeben. Es liegt in der Verantwortung des Benutzers, das Kennwort mit der Häufigkeit zu ändern, die durch die Kennwortrichtlinien vorgegeben wird, die sich auf das minimale und maximale Alter von Kennwörtern beziehen.

Benutzer haben folgende Möglichkeiten, ihre eigenen Konten zu verwalten:

- Ändern von Kennwörtern in Übereinstimmung mit Kennwortrichtlinien
- Aufheben von Sperren von Benutzerkonten, die gesperrt wurden, sofern gemäß der entsprechenden Kennwortrichtlinie zulässig

Entsperren von Benutzerkonten

Sofern die Kennwortrichtlinie dies zulässt, können Sie ein gesperrtes Benutzerkonto unabhängig von Ihrer Rolle entsperren. Wenn Ihr Konto gesperrt wird, muss ein anderer Benutzer es entsperren, damit Sie die Berechtigungen, die Ihrer Rolle gewährt wurden, wieder nutzen können.

Sperren und Entsperrungen werden durch die folgenden beiden Kennwortrichtlinien gesteuert:

- Benutzerkonto nach <n> fehlgeschlagenen Anmeldungen sperren
- Benutzer dürfen Kennwortsperre aufheben

Benutzerkonten können gesperrt werden, wenn die Kennwortrichtlinie so eingestellt ist, dass Benutzerkonten nach einer bestimmten Anzahl von fehlgeschlagenen Anmeldungen gesperrt werden. Dies kann auch der Fall sein, wenn die Anzahl der Anmeldeversuche mit ungültigen Anmeldeinformationen eines Benutzers den angegebenen Schwellenwert überschreitet.

Jeder Benutzer kann das Konto eines anderen Benutzers entsperren, wenn die Kennwortrichtlinie eingestellt ist, bei der Benutzer die Kennwortsperre aufheben dürfen. Sie benötigen das Kennwort des Benutzers, damit Sie das entsprechende Benutzerkonto entsperren können.

So entsperren Sie ein Benutzerkonto:

1. Klicken Sie auf die Registerkarte "Verwaltung" und auf die Unterregisterkarte "Benutzer- und Zugriffsverwaltung".
2. Klicken Sie im linken Fensterbereich auf "Benutzer entsperren".
3. Geben Sie den Benutzernamen mit zugehörigem Kennwort ein, und klicken Sie auf "Entsperren".

   Das Benutzerkonto wird entsperrt.

Ändern Ihres Kennworts

Sie können Ihr eigenes Kennwort unabhängig von Ihrer Rolle ändern. Wenn die Kennwortrichtlinie für das maximale Alter von Kennwörtern eingestellt ist, sollten Sie Ihr Kennwort so oft ändern, dass diese Richtlinie eingehalten wird.

Achten Sie darauf, dass Sie Ihr Kennwort in folgenden Fällen möglichst häufig ändern:

- Sie geben einem anderen Benutzer Ihr Kennwort, damit er Ihr Konto entsperrt.
- Sie haben Ihr Kennwort vergessen, und der Administrator setzt es für Sie zurück.

So ändern Sie Ihr Kennwort:

1. Klicken Sie auf die Registerkarte "Verwaltung" und auf die Unterregisterkarte "Benutzer- und Zugriffsverwaltung".
2. Klicken Sie im linken Fensterbereich auf "Kennwort ändern".
3. Geben Sie Ihr altes Kennwort ein.
4. Geben Sie zwei Mal Ihr neues Kennwort ein.
5. Klicken Sie auf "OK".

Aufgaben im Zusammenhang mit Rollen

Administratoren können Benutzern basierend auf den Aufgaben, die sie ausführen sollen, Rollen zuweisen. Sie können Benutzern die vordefinierten Rollen "Auditor", "Analyst" und "Administrator" oder benutzerdefinierte Rollen zuweisen, die Sie erstellen. Überprüfen Sie die Aufgaben, die den einzelnen Rollen zugeordnet sind, um die Auswirkung der Verwendung vordefinierter Rollen zu bewerten.

Weitere Informationen

Auditor-Aufgaben (siehe Seite 28)
Aufgaben von Analysten (siehe Seite 30)
Administratoraufgaben (siehe Seite 31)

Auditor-Aufgaben

Interne Auditoren führen unter Umständen folgende oder ähnliche Aufgaben aus:

- Nach Abfragen suchen und diese auswählen sowie Abfrageergebnisse anzeigen
- Für ausgewählte Abfrageergebniszeilen einen Ereignis-/Alarmausgabeprozess ausführen, der in CA IT PAM konfiguriert ist
- Aktuelle Berichte anzeigen
- Berichte planen
- Liste der geplanten Berichtsjobs anzeigen
- Generierte Berichtsliste anzeigen
- generierte Berichte anzeigen und anmerken
- Einstellen von Filtern und Profilen

Sie können die Rolle mit den geringsten Berechtigungen wählen, also die Auditor-Rolle, wenn Sie Benutzerkonten für Benutzer von Drittanbieterprodukten einrichten. Wenn beispielsweise ein geplanter Alarm einen Ereignis-/Alarmausgabeprozess auf Abfrageebene ausführt, sendet der Alarm eine URL an CA Enterprise Log Manager, die an die Beschreibung angehängt wird. Damit Benutzer von Drittanbieterprodukten zu CA Enterprise Log Manager wechseln können, benötigen sie ein Benutzerkonto.

Hinweis: Analysten und Administratoren können alle Aufgaben von Auditoren sowie ihre rollenspezifischen Aufgaben ausführen.

Externe Auditoren, denen für den Zeitraum der Standortprüfung vorübergehend Zugriff auf CA Enterprise Log Manager gewährt wird, überprüfen unter Umständen das Bestehen von Konformität mit Standards beispielsweise in folgenden Bereichen:

- Überprüfen, ob Protokolle von den erwarteten Quellen erfasst werden
- Überprüfen, ob Verfahren zur Verhinderung von Datenverlusten vorhanden sind. Beispiel: Überprüfung, ob Daten häufig genug gesichert werden, so dass keine Verluste möglich sind.
- Überprüfen, ob Protokolle regelmäßig überprüft werden, um Sicherheitsverstöße zu ermitteln
- Überprüfen, ob Protokolle ordnungsgemäß in einem sicheren Archiv gespeichert wurden

- Überprüfen, ob das Alter der archivierten Daten den Standards für die Aufbewahrung von Protokollen entspricht
- Überprüfen, ob der Inhalt der Protokolle den für die Aufbewahrung obligatorischen Inhalt umfasst

Weitere Informationen

Planen von Berichtsjobs (siehe Seite 525)
Anzeigen generierter Berichte (siehe Seite 522)
Ergänzen generierter Berichte mit Anmerkungen (siehe Seite 524)
Anzeigen von Berichten (siehe Seite 298)
Beispiel: Ausführen eines Ereignis-/Alarmausgabeprozesses mit ausgewählten Abfrageergebnissen (siehe Seite 431)
Beispiel: Senden eines Alarms, der einen IT PAM-Prozess pro Abfrage ausführt (siehe Seite 442)

Aufgaben von Analysten

Systemanalysten überwachen das Protokollerfassungsnetzwerk. Anschließend erfassen und verteilen sie Berichtsdaten.

Administratoren weisen die *Analystenrolle* Benutzern zu, die für folgende Aufgaben verantwortlich sind:

- Benutzerdefinierte Berichte und Abfragen erstellen

  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.

- Planen von Aktionsalarmen

  Ein Aktionsalarm ist ein geplanter Abfragejob, mit dessen Hilfe Verletzungen von Richtlinien, Nutzungstrends, Anmeldemuster und andere Informationen, die möglicherweise ein kurzfristiges Eingreifen erfordern, ermittelt werden können. Alarmdaten können auf der Benutzeroberfläche oder über einen RSS-Feed angezeigt werden. Sie können geplante Alarme an E-Mail-Empfänger, ein SNMP-Trap-Ziel oder einen CA IT PAM-Ereignis-/Alarmausgabeprozess senden. Sie können den Prozess einmal pro Zeile oder einmal pro Abfrage ausführen.

- Kennungen erstellen

  Eine *Kennung* ist ein Begriff oder Schlüsselausdruck, mit dem Abfragen oder Berichte ermittelt werden, die zu derselben Kategorie gehören. Wenn Sie einen neuen Bericht zu einem geplanten Job hinzufügen, der zur Auswahl von Berichten mit einer spezifischen Kennung konfiguriert wurde, fügen Sie dem neuen Bericht die allgemeine Kennung hinzu. Bei einer Kennung kann es sich auch um einen Ausdruck handeln, der mit einer Abfrage verknüpft ist und so den Inhalt der Abfrage beschreibt und eine auf einem Schlüsselausdruck basierende Klassifizierung und Suche ermöglicht.

- RSS-Feeds (Rich Site Summary) anzeigen

  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.

Folgender Ansatz eignet sich für Analysten, sobald sie sich etwas mit der Arbeit mit CA Enterprise Log Manager vertraut gemacht haben:

1. Untersuchen Sie die verfügbaren vordefinierten Berichte. (Auditoren können diesen Schritt ebenfalls ausführen.)
2. Entwerfen Sie benutzerdefinierte Berichte, erstellen Sie Kennungen dafür, planen Sie die Berichte, zeigen Sie sie an, und versehen Sie sie mit Anmerkungen.
3. Planen Sie Berichte, die für eine regelmäßige Generierung in Betracht kommen. (Auditoren können diesen Schritt ebenfalls ausführen.)
4. Überprüfen Sie generierte Berichte und versehen Sie sie mit Anmerkungen. (Auditoren können diesen Schritt ebenfalls ausführen.)
5. Ermitteln Sie Kriterien für den Versand eines Alarms, das zu verwendende Format und den Empfänger. Planen Sie dann den Alarm, der generiert werden soll, wenn die Kriterien erfüllt werden.

Administratoraufgaben

Benutzern, denen die Administratorrolle zugewiesen wurde, haben unbeschränkten Zugriff auf die Funktionalität, die auf allen Registerkarten von CA Enterprise Log Manager verfügbar ist. Nur Benutzer mit Administratorrolle haben vollständigen Zugriff auf die Registerkarte "Verwaltung". Auf der Registerkarte "Verwaltung" können Administratoren alle Aspekte der Protokollerfassung, alle Dienste und den Benutzerzugriff konfigurieren und verwalten.

Weitere Informationen

Konfiguration und Anpassung der Protokollerfassung (siehe Seite 32)
Konfiguration und Überwachung von Services (siehe Seite 34)
Benutzer- und Zugriffsverwaltung (siehe Seite 37)

Konfiguration und Anpassung der Protokollerfassung

Nur Benutzer mit Administratorrolle können Funktionen für die Protokollerfassung konfigurieren und verwalten. Administratoren führen die Aufgaben der Protokollerfassung auf der Registerkarte "Verwaltung" und der Unterregisterkarte "Protokollerfassung" durch.

Für die Protokollerfassung erforderliche Connectors auf Agenten werden im Protokollerfassungs-Explorer konfiguriert. Darüber hinaus installieren Administratoren ggf. Software-Updates auf Agenten.

Die Arbeit mit der Ereignisverfeinerungs-Bibliothek ist optional. Die einsatzbereiten, regelmäßig aktualisierten Funktionen erfüllen die Anforderungen der meisten Kunden.

Zu den von Administratoren durchgeführten Aufgaben der Protokollerfassung gehören unter anderem:

- Installierte Agenten auf einem speziellen CA Enterprise Log Manager-Server für die Erfassung konfigurieren und verwalten
- Archivkatalog auf einem CA Enterprise Log Manager-Berichterstellungsserver abfragen

  Der *Archivkatalog* ist der Datensatz aller Datenbanken, die sich jemals auf dem CA Enterprise Log Manager-Server befunden haben. Zum Archivkatalog zählen kürzlich erstellte Datenbanken sowie Datenbanken, die gesichert und verschoben wurden, und gegebenenfalls auch Datenbanken, die vor der Sicherung gelöscht wurden.
- CA-Adapter konfigurieren, die von CA Audit verwendet werden
- Ereignisverfeinerungs-Bibliothek verwalten
  - Mit vordefinierten Integrationen arbeiten und völlig neue Integrationen oder Integrationen anhand einer vordefinierten Integration erstellen

    Integration ist das Mittel, mit dem nicht klassifizierte Ereignisse in verfeinerte Ereignisse verarbeitet werden, so dass sie in Abfragen und Berichten angezeigt werden.
  - Aus dem vordefinierten Listener einen Syslog-Listener erstellen
  - Völlig neue Analysedateien oder Analysedateien anhand einer ausgewählten vordefinierten Datei erstellen

    Die mit einem bestimmten Ereignisquellentyp verknüpfte Nachrichtenanalysedatei (XMP) wendet Analyseregeln an, durch die Rohereignisse in Namen-/Wertpaare unterteilt werden.

- Völlig neue Zuordnungsdateien oder Zuordnungsdateien anhand einer ausgewählten vordefinierten Datei erstellen

  Unter Datenzuordnungsdateien versteht man XML-Dateien, die die CA-ELM-Schemadefinition (CEG) verwenden, um Ereignisse vom Ursprungsformat in ein Format zu übertragen, das zur Berichterstellung und Analyse im Ereignisprotokollspeicher gespeichert werden kann.

- Völlig neue Zusammenfassungsregeln oder Zusammenfassungsregeln anhand einer ausgewählten vordefinierten Regel erstellen

  Zusammenfassungsregeln fassen bestimmte gängige, systemeigene Ereignistypen zu einem verfeinerten Ereignis zusammen.

- Völlig neue Unterdrückungsregeln oder Unterdrückungsregeln anhand einer ausgewählten vordefinierten Regel erstellen

  Unterdrückungsregeln verhindern, dass bestimmte verfeinerte Ereignisse in Berichten angezeigt werden.

- Erstellen von Regeln für die Ereignisweiterleitung

  Ereignisweiterleitungsregeln legen fest, dass ausgewählte Ereignisse an Drittanbieterprodukte weitergeleitet werden, etwa solche, durch die Ereignisse korreliert werden, nachdem sie im Ereignisprotokollspeicher abgelegt wurden.

- Profile erstellen

  In einem Profil ist eine Gruppe von Datenfiltern und Kennungen festgelegt, die zur Auswahl angezeigt werden. Durch Datenfilter werden die in Abfragen oder Berichten angezeigten Daten eingeschränkt. Durch Kennungsfilter werden die in der Abfrage- bzw. Berichtkennungsliste angezeigten Kennungen begrenzt.

Weitere Informationen

Erstellen von Agentengruppen (siehe Seite 701)
Konfigurieren der Agentenverwaltung (siehe Seite 704)
Anwenden automatischer Software-Updates (siehe Seite 711)

Konfiguration und Überwachung von Services

Nur Benutzer mit Administratorrolle können Services konfigurieren und verwalten, auf die über die Registerkarte "Verwaltung" und die Unterregisterkarte "Services" zugegriffen werden kann. Konfigurieren Sie alle Services möglichst bald nach der Installation von CA Enterprise Log Manager.

Zu den von Administratoren durchgeführten Aufgaben in Bezug auf Services gehören unter anderem:

- Konfigurieren globaler Services, wie etwa:
  - Aktualisierungsintervall
  - Sitzungszeitlimit
  - Entscheidung, ob für die Anzeige der in RSS-Feeds geposteten Alarme eine Authentifizierung erforderlich ist
  - Auszublendende Kennungen
  - Standardprofil
- Konfigurieren des Ereignisprotokollspeicherservice
  - Auf globaler Ebene Konfiguration der Services, die für alle CA Enterprise Log Manager-Server gelten
  - Auf lokaler Ebene Konfiguration der automatischen Archivierung

    Im Ereignisprotokollspeicher auf dem CA Enterprise Log Manager-Erfassungsserver sind eine heiße Datenbank und neue Protokolle gespeichert. Die heiße Datenbank wird zu einer warmen Datenbank komprimiert, wenn die konfigurierte maximale Anzahl von Zeilen erreicht wird.

    - Wenn Sie zwischen dem Erfassungs- und dem Berichterstellungsserver eine automatische Archivierung konfigurieren, wird die warme Datenbank auf den Berichterstellungsserver kopiert und anschließend vom Erfassungsserver gelöscht.

- Wenn Sie zwischen dem Erfassungsserver und einem Remote-Server, bei dem es sich nicht um einen CA Enterprise Log Manager-Server handelt, eine automatische Archivierung konfigurieren, werden warme Datenbanken abhängig von Ihren Einstellungen für die automatische Archivierung auf täglicher oder stündlicher Basis auf den Remote-Server kopiert. Standardmäßig behält der Berichtsserver die Datenbanken, bis der festgelegte Speicherplatz oder Zeitlimits erreicht sind. Sie werden nur dann automatisch aus dem Berichtsserver gelöscht, wenn Sie das Kontrollkästchen "Remote-ELM-Server" aktiviert haben.
- Wenn Sie keine automatische Archivierung vom Berichterstellungsserver auf einen Remote-Speicherserver konfigurieren, erstellen Sie manuell eine Sicherung der warmen Datenbanken und verschieben diese an den langfristigen Speicherort. Die warme Datenbank wird für die Anzahl von Tagen im Ereignisprotokollspeicher eines Berichterstellungsservers (oder eines Management-/Berichterstellungsservers in einer Bereitstellung mit zwei Servern) gespeichert, die als maximale Anzahl an Archivtagen konfiguriert wurde, sofern der verfügbare Speicherplatz nicht unter den konfigurierten Prozentsatz sinkt, der durch den Festplattenspeicher für das Archiv festgelegt ist. In diesem Fall werden warme Datenbanken beginnend mit der ältesten gelöscht.

- Konfigurieren des Berichtsserver-Service

  Der Berichtsserver-Service verarbeitet Berichte und Alarme (einschließlich der Aufbewahrungsrichtlinien), das Format für gedruckte und per E-Mail gesendete Berichte sowie die Schlüsselwerte für Berichte und Alarme. Ferner verarbeitet er die Integrationseinstellungen für CA IT PAM-Prozesse wie etwa Ereignis-/Alarmausgabeprozesse und Prozesse mit dynamischen Werten sowie die Integrationseinstellungen für die SNMP-Trap-Ziele für Alarme.

- Konfigurieren automatischer Software-Updates

  Automatische Software-Updates beziehen sich auf binäre und nicht binäre Dateien, die über den CA-Server für automatische Software-Updates für CA Enterprise Log Manager-Server, der CA EEM-Komponente des Managementservers sowie Agenten verfügbar gemacht werden.

- Verwalten der Föderation von CA Enterprise Log Manager-Servern

  Auf dem Management-Server können Sie eine Abfrage zur Erweiterung auf untergeordnete Föderationen und gleichrangige Server festlegen. CA Enterprise Log Manager-Server können zu zwei Zwecken föderiert werden:

- Der Erfassungsserver archiviert jede heiße Datenbank automatisch in einer warmen Datenbank und sendet sie an den zugehörigen Berichterstellungsserver. Erstellen Sie eine Föderation zwischen dem Quellserver und dem Berichterstellungsserver. Wenn Sie eine Abfrage des Verwaltungsservers mit aktivierter Föderation durchführen, können Sie nicht nur Ergebnisse aus den lokalen warmen Datenbanken, sondern auch aus der heißen Datenbank des Erfassungsservers abrufen.
- Es können mehrere Berichterstellungsserver erstellt werden, um die Speicherung einer warmen Datenbank auf mehrere Ereignisprotokollspeicher zu verteilen. Berichterstellungsserver können in einem Netzverbund von Quellservern föderiert werden, die untergeordnete Server des entsprechenden übergeordneten Berichterstellungsservers sind. Eine föderierte Abfrage von einem der Berichterstellungsserver im Netzverbund gibt sowohl Daten von den entsprechenden Servern im Netzverbund (den untergeordneten Servern) als auch von allen Servern zurück, die diesen untergeordnet sind.

  Hinweis: Wenn Sie einen Wiederherstellungspunkt-CA Enterprise Log Manager erstellen, um archivierte Datenbanken aus einem langfristigen Speicher wiederherzustellen, empfiehlt es sich, einen derartigen Server aus der Föderation auszunehmen.

- Überwachen und Verwalten des Systemstatus

Weitere Informationen:

Automatisierung der Sicherung und Wiederherstellung (siehe Seite 205)
Abfragen des Archivkatalogs (siehe Seite 218)
Wiederherstellen automatisch archivierter Dateien (siehe Seite 220)
Wiederherstellungs–Skript für die Wiederherstellung archivierter Datenbanken (siehe Seite 222)
Hinweise zum ODBC-Server (siehe Seite 176)
Erstellen einer Diagnosedatei für den Support (siehe Seite 195)
Neustart eines Hostservers (siehe Seite 196)
Starten Sie die ELM-Services neu. (siehe Seite 196)
Überprüfen von Service-Status und Version (siehe Seite 197)
Überprüfen von selbstüberwachenden Systemsstatus-Ereignissen (siehe Seite 197)

Benutzer- und Zugriffsverwaltung

Nur Benutzer mit Administratorrolle können Benutzerkonten, Richtlinien und andere Anwendungsobjekte konfigurieren und verwalten, die über die Registerkarte "Verwaltung", Unterregisterkarte "Benutzer- und Zugriffsverwaltung" verfügbar sind. Um sich bei CA Enterprise Log Manager anzumelden, benötigen Benutzer ein Benutzerkonto mit einer Rolle und Anmeldeinformationen. Mit vordefinierten Rollen und Richtlinien können Administratoren Benutzerzugriff ermöglichen, indem sie Benutzerkonten einrichten. Das Erstellen von benutzerdefinierten Rollen und Richtlinien ist optional.

Administratoraufgaben, die Benutzer und Zugriffe betreffen, umfassen Folgendes:

- Neue globale Benutzer definieren (im CA Enterprise Log Manager-Benutzerspeicher, wenn für den Benutzerspeicher der Standardwert eingestellt ist).

  Wenn Sie einen neuen Benutzer hinzufügen, erstellen Sie einen globalen Benutzer. Details wie der Name, der Standort und die Telefonnummer werden als global angesehen, da sie gemeinsam verwendet werden können. Bei einem *globalen Benutzer* handelt es sich um die Benutzerkontoinformationen ohne anwendungsspezifische Details.

- Referenzierte Benutzer abrufen (wenn der Benutzerspeicher ein referenzierter Benutzerspeicher ist).

  Details zu globalen Benutzern werden im konfigurierten Benutzerspeicher gespeichert. Hierbei kann es sich um ein externes Verzeichnis handeln.

- Neuen oder referenzierten Benutzern vordefinierte oder benutzerdefinierte Anwendungsgruppen (Rollen) zuweisen

  Anwendungsdetails werden im Repository des Management-Servers gespeichert. Hierbei handelt es sich um Details, die im schreibgeschützten Format geladen werden, wenn Sie einen externen Benutzerspeicher konfigurieren.

- Benutzerkonten bearbeiten, löschen und anzeigen
- Benutzerdefinierte Anwendungsgruppen (Rollen) zu zugehörige Richtlinien erstellen.

Die Erstellung von Benutzerrollen beginnt mit dem Definieren einer neuen Anwendungsbenutzergruppe und dem anschließenden Erstellen einer Richtlinie, in der die Aktionen definiert sind, die für die angegebenen Ressourcen zulässig sind. 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.

- Anwendungsgruppen und zugehörige Richtlinien bearbeiten, löschen und anzeigen.
- CALM-Anwendungszugriffsrichtlinie bearbeiten.

  Die CALM-Anwendungszugriffsrichtlinie ist eine Richtlinie vom Typ "Zugriffskontrollliste" der Richtlinie zur Bereichsdefinierung, in der festgelegt ist, wer auf CA Enterprise Log Manager zugreifen kann. Der Zugriff wird standardmäßig dem [Gruppen-]Administrator, dem [Gruppen-]Analysten und dem [Gruppen-]Auditor gewährt.
- Zugriffsrichtlinien erstellen, bearbeiten, löschen und anzeigen.

  Eine Zugriffsrichtlinie ist eine Regel, die einer Identität (Benutzer oder Benutzergruppe) Zugriffsrechte auf eine Anwendungsressource gewährt oder verweigert.
- Zugriffsfilter konfigurieren, bearbeiten, löschen und anzeigen.

  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.

Weitere Informationen

Erstellen einer globalen Gruppe (siehe Seite 41)
Erstellen eines globalen Benutzers (siehe Seite 42)
Zuweisen einer Rolle zu einem globalen Benutzer (siehe Seite 44)
Sichern aller Zugriffsrichtlinien (siehe Seite 67)
Wiederherstellen von Zugriffsrichtlinien (siehe Seite 72)
Konfigurieren von benutzerdefinierten Benutzerrollen und Zugriffsrichtlinien (siehe Seite 93)
Hinzufügen einer Identität zu einer vorhandenen Richtlinie (siehe Seite 99)
Erstellen einer CALM-Zugriffsrichtlinie (siehe Seite 100)
Erstellen einer Richtlinie für dynamische Benutzergruppen (siehe Seite 111)
Erstellen einer Richtlinie auf der Grundlage einer vorhandenen Richtlinie (siehe Seite 108)
Erstellen von Richtlinien zur Bereichsdefinierung (siehe Seite 103)
Erstellen eines Zugriffsfilters (siehe Seite 113)
Erstellen einer Anwendungsbenutzergruppe (Rolle) (siehe Seite 96)
Gewähren des Zugriffs auf CA Enterprise Log Manager für eine benutzerdefinierte Rolle (siehe Seite 98)
Testen von neuen Richtlinien (siehe Seite 110)
Erstellen von Kalendern (siehe Seite 115)

Konfigurieren von Konten mit vordefinierten Einstellungen

Wenn Sie eine temporäre Testumgebung einrichten, können Sie die Benutzer- und Zugriffsverwaltung sehr schnell einrichten, sofern Sie für Benutzerkonten vordefinierte Einstellungen verwenden und nur erforderliche Felder konfigurieren. Um eine Minimalkonfiguration mit vordefinierten Einstellungen durchzuführen, erstellen Sie für CA Enterprise Log Manager-Benutzer Benutzerkonten wie folgt:

- Wenn Sie den Standardbenutzerspeicher verwenden, erstellen Sie ein Konto mit einem Benutzernamen, weisen Sie eine vordefinierte Anwendungsgruppe (Administrator, Analyst, Auditor) und ein temporäres Kennwort zu.
- Wenn Sie auf einen externen Benutzerspeicher verweisen, suchen Sie anhand des Namens nach dem globalen Benutzer, weisen Sie eine vordefinierte Rolle (Administrator, Analyst, Auditor) und ein temporäres Kennwort zu.

Weitere Informationen:

Erstellen eines globalen Benutzers (siehe Seite 42)
Zuweisen einer Rolle zu einem globalen Benutzer (siehe Seite 44)
Verwalten eines referenzierten Benutzerkontos (siehe Seite 45)

Erstellen einer globalen Gruppe

Ob eine globale Gruppe erstellt werden kann, hängt von der Konfiguration des Benutzerspeichers ab. Bedenken Sie die folgenden Punkte:

- Wenn Sie den Standardbenutzerspeicher verwenden, ist das Erstellen von globalen Gruppen optional.
- Wenn auf einen externen Benutzerspeicher verwiesen wird, werden globale Gruppen und Benutzerkonten automatisch in den Standardbenutzerspeicher geladen. Optional können Sie benutzerdefinierte Richtlinien für diese globalen Gruppen erstellen, Sie können jedoch keine neuen globalen Gruppen erstellen.
- Wenn auf den Benutzerspeicher CA SiteMinder verwiesen wird, können Sie die in diesem CA-Produkt definierten globalen Gruppen verwenden, wie sie vorliegen, oder Sie können aus vorhandenen Gruppenmitgliedschaften neue globale Gruppen erstellen.

So erstellen Sie eine globale Gruppe:

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

   Die Fensterbereiche "Suchgruppen" und "Benutzergruppen" werden eingeblendet.
3. Klicken Sie auf die Schaltfläche "Neue globale Gruppe" neben dem Ordner "Globale Gruppen".

   Das Fenster "Neue globale Benutzergruppe" wird angezeigt.
4. Geben Sie einen Namen und, optional, eine Beschreibung ein.
5. Wenn diese globale Gruppe eine andere globale Gruppe enthalten soll, gehen Sie folgendermaßen vor:
   a. Geben Sie zum Anzeigen einer Gruppe Suchkriterien ein und klicken Sie auf "Suchen".
   b. Verschieben Sie die Gruppe, die Sie einbeziehen möchten, in die Liste "Ausgewählte globale Benutzergruppen".
   c. Wiederholen Sie diesen Schritt, bis die Liste alle gewünschten Gruppen enthält.
6. Klicken Sie auf "Speichern".

   Es wird eine Bestätigung angezeigt.

Weitere Informationen:

Planen von Benutzerrollen (siehe Seite 91)

Erstellen eines globalen Benutzers

Sie können nur neue Benutzer erstellen, wenn der Benutzerspeicher als CA Enterprise Log Manager-Benutzerspeicher (Standardbenutzerspeicher) definiert ist. Nur Administratoren können neue Benutzerkonten erstellen.

Wenn Sie auf einen externen Benutzerspeicher verweisen, werden Benutzerkonten automatisch als schreibgeschützte Datensätze in den Standardbenutzerspeicher geladen. Wenn Sie einen neuen Benutzer erstellen müssen, müssen Sie den Benutzer im externen Benutzerspeicher erstellen. Der neue Datensatz wird automatisch geladen.

Um das CA Enterprise Log Manager-Produkt zu verwenden, muss ein Benutzer ein globales Benutzerkonto haben. Das Konto muss bei der Anmeldung aktiv sein. Konten können inaktiv werden, wenn sie vom Administrator ausgesetzt, aufgrund einer Verletzung einer Kennwortrichtlinie gesperrt oder aufgrund der Tatsache, dass die Aktivierungszeit für ein Konto abgelaufen ist, deaktiviert werden.

So erstellen Sie ein neues globales Benutzerkonto:

1. Klicken Sie auf die Registerkarte "Verwaltung" und auf die Unterregisterkarte "Benutzer- und Zugriffsverwaltung".
2. Klicken Sie auf die Schaltfläche "Benutzer".
3. Stellen Sie sicher, dass das Konto, das Sie erstellen möchten, nicht bereits vorhanden ist. Wählen Sie "Globale Benutzer" aus, und klicken Sie auf "Los". Wenn der Name in den Ergebnissen nicht angezeigt wird, fahren Sie fort.
4. Klicken Sie auf die Schaltfläche "Neuer Benutzer", links neben der Struktur "Benutzer".

   Die Seite "Neuer Benutzer" wird angezeigt.
5. Geben Sie den Namen des Benutzers in das Eingabefeld "Name" ein.

6. (Optional) Weisen Sie eine Anwendungsbenutzergruppe zu.
    a. Klicken Sie auf "Anwendungsbenutzerdetails hinzufügen".
    b. Wählen Sie eine oder mehrere Benutzergruppen aus, und klicken Sie auf die Schaltfläche "Verschieben", um die Auswahl in das Feld "Ausgewählte Benutzergruppen" zu verschieben.

       Hinweis: Wenn Sie diesen Vorgang nicht jetzt durchführen, können Sie das Konto eines globalen Benutzers später bearbeiten, um eine Anwendungsbenutzergruppe hinzuzufügen.
7. Geben Sie die allgemeinen Informationen für Details zum globalen Benutzer ein.
8. (Optional) Weisen Sie eine globale Benutzergruppe zu.
9. Geben Sie Informationen für die Authentifizierung ein:
    a. Um einen Schwellenwert für die Anzahl falscher Anmeldungen festzulegen, die akzeptiert werden, bevor das Konto gesperrt wird, geben Sie für Anzahl falscher Anmeldungen eine Zahl ein. Wenn Sie 0 eingeben, bedeutet das, dass es keine Grenze gibt.
    b. Übernehmen Sie das nicht aktivierte Kontrollkästchen für das Außerkraftsetzen der Kennwortrichtlinie, es sei denn, Sie möchten, dass dieser Benutzer Kennwörter besitzt, die nicht der Kennwortrichtlinie entsprechen.
    c. Wiederholen Sie Ihren Eintrag im Feld "Kennwort bestätigen".
    d. Wählen Sie die Option zum Ändern des Kennworts bei der nächsten Anmeldung aus, damit der Benutzer das Kennwort ändern kann.
    e. Lassen Sie "Ausgesetzt" deaktiviert, wenn Sie ein neues Konto erstellen.
    f. Geben Sie unter "Neues Kennwort" und "Kennwort bestätigen" ein neues Kennwort ein.
    g. Wenn dieser Benutzer nur temporären Zugriff haben soll, geben Sie einen Datumsbereich für die Aktivierung und Deaktivierung des Benutzerkontos ein.
    h. Um die Aktivierung des Benutzerkontos auf einen späteren Termin zu verschieben, geben Sie das Datum zum Aktivieren des Kontos ein.
10. Klicken Sie auf "Speichern".
11. Klicken Sie auf "Schließen".

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".

Verwalten eines referenzierten Benutzerkontos

Sie können Informationen zu globalen Benutzerkonten verwenden, wenn Sie auf einen externen Benutzerspeicher verweisen. Sie können zwar den Benutzerdatensatz im externen Benutzerspeicher von CA Enterprise Log Manager aus nicht aktualisieren, aber Sie können auf der Anwendungsebene Details zuweisen.

Beachten Sie die folgenden Verfahrensweisen beim Verwalten des Zugriffs für Benutzer mit Konten, die in einem externen Benutzerspeicher gespeichert sind.

- Sie können eine vordefinierte Anwendungsbenutzergruppe, oder Rolle, zum Benutzerkonto hinzufügen.
- Sie können die globale Gruppe zu den vordefinierten Richtlinien hinzufügen, die dem Benutzer den Zugriff gewähren, den Sie ihm gestatten möchten.
- Sie können benutzerdefinierte Rollen und zugehörige Richtlinien erstellen und die benutzerdefinierte Rolle dem Benutzerkonto hinzufügen.

Benutzer-Aktivierungsrichtlinien

Halten Sie sich an die folgenden Anleitungen, wenn Sie die Kontoaktivierungsfunktionen verwenden:

- Wenn Sie mehrere Benutzerkonten gleichzeitig erstellen, können Sie "Aktivierungsdatum" verwenden, um ein Datum in der Zukunft festzulegen, an dem alle oder ausgewählte Konten aktiviert werden sollen. Dies ermöglicht es Ihnen, die Gewährung der Zugriffsrechte mit Schulungsmaßnahmen koordinieren, die Sie für die neuen Benutzer planen.
- Wenn Sie temporäre Konten für externe Auditoren erstellen, können Sie die Einstellungen für das Aktivierungsdatum und das Inaktivierungsdatum verwenden, um einen bestimmten Zeitraum festzulegen.
- Wenn Ihnen verdächtiges Verhalten seitens eines Benutzers auffällt, können Sie das entsprechende Konto sofort als gesperrt markieren und so verhindern, dass sich der Benutzer an irgendeinem CA Enterprise Log Manager-Server erfolgreich anmelden kann.
- Wenn ein Benutzer das Unternehmen verlässt, können Sie den Datensatz des Benutzers entweder ganz löschen oder als gesperrt markieren oder ein Ablaufdatum eingeben, an dem es inaktiviert wird.

Weitere Informationen:

Erstellen eines globalen Benutzers (siehe Seite 42)
Bearbeiten eines Benutzerkontos (siehe Seite 47)
Löschen einer Benutzergruppe (siehe Seite 51)

Bearbeiten eines Benutzerkontos

Nur Administratoren können Benutzerkonten erstellen und bearbeiten. Sie können aus jedem beliebigen der folgenden Gründe nach einem Benutzer suchen und die Informationen zu dem ausgewählten Benutzerkonto anzeigen:

- um einem globalen Benutzer eine CA Enterprise Log Manager-Rolle zuzuweisen, also die Mitgliedschaft in einer Anwendungsgruppe, wenn dessen Kontoinformationen aus einem referenzierten Benutzerspeicher geladen wurden;
- um Details für das Konto eines globalen Benutzers im lokalen Benutzerspeicher zu aktualisieren;
- um ein Benutzerkonto zu sperren;
- um das Kennwort für ein Benutzerkonto zurückzusetzen, entweder, weil das Kennwort vergessen oder das Konto gesperrt wurde und die Kennwort-Richtlinien nicht erlauben, dass Benutzer ihre Konten selbst entsperren dürfen.
- So können Sie ein Benutzerkonto inaktivieren oder die Aktivierungsdauer eines Kontos zurücksetzen:

Wichtig! Machen Sie keine Eingabe in das Feld "Zählung inkorrekter Anmeldungen" im Bereich "Authentifizierung". Der in diesem Feld angezeigte Wert wird vom System aktualisiert.

So bearbeiten Sie ein Benutzerkonto:

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

   Der Fensterbereich "Benutzer suchen" wird angezeigt.

3. Geben Sie auf eine der folgenden Weisen Suchkriterien im Fensterbereich "Benutzer suchen" an:

   - Um Anwendungsdetails für den globalen Benutzer hinzuzufügen, wählen Sie "Globale Benutzer" aus, geben Sie Suchkriterien ein, und klicken Sie auf "Los".
   - Um das Konto eines Benutzers mit einer existierenden CA Enterprise Log Manager-Rolle zu bearbeiten, wählen Sie "Details für Anwendungsbenutzer", geben Sie Suchkriterien ein, und klicken Sie auf "Los".

   Hinweis: Verwenden Sie bei der Eingabe von Suchkriterien den Operator WIE, wenn Sie einen Platzhalter eingeben, und den Operator GLEICH, wenn Sie die komplette Zeichenkette eingeben. Es folgen einige Beispiele:

   - Gruppenmitgliedschaft WIE Aud*
   - Gruppenmitgliedschaft GLEICH Auditor

   Die Namen der Benutzer, die den Suchkriterien entsprechen, werden im Fensterbereich "Benutzer" eingeblendet.

4. Klicken Sie auf den Benutzernamen des zu bearbeitenden Kontos.

   Das ausgewählte Konto wird im rechten Fensterbereich angezeigt.

5. Um eine Rolle hinzuzufügen, klicken Sie auf "Benutzerdetails", wählen Sie den entsprechenden Benutzer unter "Verfügbare Benutzergruppen" aus, und verschieben Sie ihn nach "Ausgewählte Benutzergruppen".

6. Um Details eines globalen Benutzers zu aktualisieren, ersetzen Sie die vorhandenen Details mit den neuen Details im Abschnitt "Details globaler Benutzer".

   Hinweis: Sie können Details nur dann aktualisieren, wenn der Standardbenutzerspeicher verwendet wird.

7. Zum Aktualisieren der Authentifizierungskonfiguration verwenden Sie eine der folgenden Möglichkeiten:

   - Wählen Sie "Kennwortrichtlinien außer Kraft setzen", um diesen Benutzer von sämtlichen Überprüfungen, die auf Grund von Kennwortrichtlinien durchgeführt werden, auszunehmen.
   - Wählen Sie "Gesperrt", um diesen Benutzer am Zugriff auf sämtliche CA Enterprise Log Manager-Server zu hindern.
   - Löschen Sie "Gesperrt", um dieses Konto zu aktivieren, so dass der Benutzer sich anmelden kann.
   - Wenn Ihre Kennwortrichtlinie so eingestellt ist, dass Benutzern das Entsperren von Kennwörtern nicht erlaubt ist und das Kennwort eines Benutzers gesperrt ist, wählen Sie "Kennwort zurücksetzen", geben Sie das neue Kennwort zweimal ein, und wählen Sie "Kennwort bei der nächsten Anmeldung ändern".

     Hinweis: Im Feld "Zählung inkorrekter Anmeldungen" wird bei einem fehlgeschlagenen Anmeldeversuch automatisch um eins hochgezählt; bei einer erfolgreichen Anmeldung wird die Zählung auf 0 zurückgesetzt. Ein Benutzerkonto wird gesperrt, wenn der gezählte Wert denjenigen Wert erreicht oder überschreitet, der in der Kennwortrichtlinie für das Sperren von Benutzerkonten nach fehlgeschlagenen Anmeldungen festgelegt ist.
   - Legen Sie einen Zeitraum fest, in dem dieses Konto aktiviert werden soll, indem Sie auf "Aktivierungsdatum" klicken und ein Startdatum eingeben und dann auf "Inaktivierungsdatum" klicken und ein Enddatum eingeben. Benutzer haben Zugriff von 0 Uhr am Tag des Startdatums bis 24 Uhr am Tag des Enddatums. Um den Zugriff für einen Tag zu gestatten, geben Sie als Start- und Enddatum dasselbe Datum ein.

8. Klicken Sie auf "Speichern".

   Die Aktualisierung des Benutzerkontos ist nun gespeichert und in Kraft.

Zurücksetzen von Benutzerkennwörtern

Sie können das Kennwort für Benutzer zurücksetzen, die ihr Kennwort vergessen haben. Wenn ein Benutzer gesperrt wird, weil er die konfigurierte Anzahl von fehlgeschlagenen Anmeldeversuchen wegen eines vergessenen Kennworts überschritten hat, können Sie das Kennwort zurücksetzen. Anschließend kann der Benutzer das Konto entsperren, sofern die entsprechende Kennwortrichtlinie dies zulässt.

So setzen Sie ein Benutzerkennwort zurück:

1. Klicken Sie auf die Registerkarte "Verwaltung" und auf die Unterregisterkarte "Benutzer- und Zugriffsverwaltung".
2. Klicken Sie auf die Schaltfläche "Benutzer".
3. Suchen Sie nach dem zu bearbeitenden Benutzerkonto.
   a. Wählen Sie Anwendungsbenutzerdetails aus.
   b. Geben Sie den Benutzernamen in das Feld "Wert" ein. Achten Sie darauf, dass "Attribut" auf "Benutzername" und "Operator" auf LIKE eingestellt ist.
   c. Klicken Sie auf "Los".
4. Klicken Sie in der Baumstruktur "Benutzer" auf den Benutzernamen.

   Die Details zum ausgewählten Benutzerkonto werden angezeigt.
5. Wählen Sie im Fensterbereich "Authentifizierung" die Option "Kennwort zurücksetzen" aus.

   Die Felder "Neues Kennwort:" und "Kennwort bestätigen" werden angezeigt.
6. Geben Sie das neue Kennwort in die Felder "Neues Kennwort" und "Kennwort bestätigen" ein.
7. Klicken Sie auf "Speichern" und anschließend auf "Schließen".

Löschen einer Benutzergruppe

Sie können alle globalen Benutzerkonten, die in CA Enterprise Log Manager erstellt wurden, löschen.

Sie können ein Benutzerkonto auch inaktivieren, ohne es zu löschen. Verwenden Sie dabei eine der folgenden Methoden:

- Sie können ein bestimmtes Datum festlegen, an dem ein Konto inaktiviert werden soll.
- Sie können ein Konto sperren, so dass der entsprechende Benutzer keinen Zugang zur CA Enterprise Log Manager-Benutzeroberfläche mehr hat.

So löschen Sie ein globales Benutzerkonto:

1. Klicken Sie auf die Registerkarte "Verwaltung", die Unter-Registerkarte "Benutzer- und Zugriffsverwaltung" und die Schaltfläche "Benutzer".

   Die Fensterbereiche "Benutzer suchen" und "Benutzer" werden eingeblendet.

2. Wählen Sie entweder "Globale Benutzer" oder "Details zu Anwendungsbenutzern", geben Sie Suchkriterien an, und klicken Sie auf "Los".

3. Wählen Sie den zu löschenden Benutzer aus der Liste der vorhandenen Benutzer aus.

   Der Datensatz zu dem ausgewählten Benutzer wird im rechten Fensterbereich angezeigt.

4. Klicken Sie auf "Löschen".

   Sie werden aufgefordert, zu bestätigen, dass dieser Benutzer gelöscht werden soll.

5. Klicken Sie auf "OK".

   Die Bestätigungsmeldung "Globaler Benutzer erfolgreich gelöscht" wird eingeblendet.

   Hinweis: Wenn Sie "Los" im Fensterbereich "Benutzer suchen" erneut klicken, enthält die angezeigte Liste den Namen des gelöschten Benutzers nicht mehr.

Kapitel 3: Richtlinien

Das Erstellen benutzerdefinierter Rollen setzt voraus, dass vordefinierte Richtlinien bearbeitet und benutzerdefinierte Richtlinien festgelegt werden. Bevor Sie damit beginnen, ist es nützlich, sich mit den vordefinierten Richtlinien für die einzelnen vordefinierten Rollen vertraut zu machen. Es ist gute Praxis, vordefinierte Zugriffsrichtlinien vor dem Bearbeiten zu sichern.

Dieses Kapitel enthält folgende Themen:

Einführung in Richtlinien

Eine *Zugriffsrichtlinie* ist eine Regel, die einer Identität (Benutzer oder Benutzergruppe) Zugriffsrechte auf eine Anwendungsressource oder eine globale Ressource 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. Das bedeutet, dass eine Richtlinie die Aktionen angibt, die bestimmten Identitäten auf bestimmten Ressourcen gewährt oder verweigert werden. Richtlinien, die den Zugriff auf eine bestimmte Ressource verweigern, haben Vorrang vor Richtlinien, die den Zugriff auf dieselbe Ressource gewähren.

CA Enterprise Log Manager unterstützt die folgenden Arten von Zugriffsrichtlinien:

- CALM-Zugriffsrichtlinien
- Delegierungsrichtlinien
- Richtlinien für dynamische Benutzergruppen (eine Alternative zu benutzerdefinierten Anwendungsgruppen)
- Verpflichtungsrichtlinien (werden beim Erstellen eines Zugriffsfilters automatisch erstellt)
- Bereichsrichtlinien

CA Enterprise Log Manager wird mit vordefinierten CALM-Zugriffsrichtlinien und Bereichsrichtlinien für die drei CA Enterprise Log Manager-Anwendungsbenutzergruppen "Administrator", "Analyst" und "Auditor" installiert. Diese Richtlinien reichen aus, wenn Sie Benutzern mit unterschiedlichen Rollen nur die vordefinierten Anwendungsbenutzergruppen zuweisen möchten.

Wichtig! Wir empfehlen, eine Sicherung der vordefinierten Richtlinien zu erstellen, die mit CA Enterprise Log Manager bereitgestellt werden. Wenn eine CALM-Zugriffsrichtlinie versehentlich gelöscht wird, können Benutzer erst wieder auf CA Enterprise Log Manager zugreifen, wenn diese Richtlinie von einer Sicherung wiederhergestellt wurde.

Vordefinierte Zugriffsrichtlinien

Wenn Sie einsatzfertige Standardfunktionen verwenden, bei denen Sie eine vordefinierte Anwendungsgruppe (Administrator, Analyst oder Auditor) den einzelnen Benutzern als Rolle zuweisen, brauchen Sie keine Zugriffsrichtlinien zu erstellen. Alle erforderlichen Richtlinien sind bereits definiert und verwendungsbereit.

Weitere Informationen

Überprüfen von Richtlinien für alle Benutzer (siehe Seite 55)
Überprüfen von Richtlinien für Auditoren (siehe Seite 59)
Überprüfen von Richtlinien für Analysten (siehe Seite 61)
Überprüfen von Richtlinien für Administratoren (siehe Seite 64)
Ressourcen und Aktionen (siehe Seite 84)

Überprüfen von Richtlinien für alle Benutzer

Sie können Richtlinien für alle Benutzer überprüfen. Bearbeiten Sie die Richtlinie für den CALM-Anwendungszugriff, um benutzerdefinierte Rollen festzulegen. Alle Standardrollen müssen als Identitäten zu dieser Richtlinie hinzugefügt werden.

So überprüfen Sie Richtlinien für alle Benutzer:

1. Klicken Sie auf die Registerkarte "Verwaltung" und anschließend auf die Unterregisterkarte "Benutzer- und Zugriffsverwaltung".
2. Klicken Sie im linken Fensterbereich auf "Zugriffsrichtlinien".
3. Zeigen Sie die CALM-Anwendungszugriffsrichtlinie wie folgt an:
   a. Wählen Sie die Option Richtlinien mit zutreffendem Namen anzeigen.
   b. Geben Sie CALM* ein.
   c. Klicken Sie auf "Los".

4. Überprüfen Sie die CALM-Anwendungszugriffsrichtlinie.

   Diese Richtlinie gewährt allen Mitgliedern der Standard-Anwendungsbenutzergruppen (Administrator, Analyst und Auditor) sowie allen, die die CA Enterprise Log Manager-API verwenden, Lese- und Schreibzugriff auf die aufgeführten Ressourcen:

Zugriffsrichtlinien

Name/Beschreibung	RessourceKlassenName	Optionen	Identitäten	Aktionen	Ressourcen
CALM Application Access This policy defines who all can access the CALM Application	SafeObject	Explizite Genehmigung	ug:Administrator ug:Analyst ug:Auditor CALM_API_UT	read write	ApplicationInstance AppObject Policy User GlobalUser

Folgende Ressourcen werden aufgeführt:

- Die Ressource "Anwendungsinstanz" (ApplicationInstance) ist CAELM und bezieht sich auf das Produkt CA Enterprise Log Manager.
- "Richtlinie" bezieht sich auf Zugriffsrichtlinien.
- "Benutzer" ist jeder Benutzer, der zu einer CA Enterprise Log Manager-Anwendungsbenutzergruppe hinzugefügt wurde.
- "Globaler Benutzer" ist jeder Benutzer, der im Benutzerspeicher innerhalb von CA Enterprise Log Manager definiert ist oder auf den von CA Enterprise Log Manager aus verwiesen wird.
- "AppObject" mit dem Wert "pozFolder" für den Ordner "Profile" bezieht sich auf Profile.
- "AppObject" mit dem Wert "pozFolder" für den Flex-Ordner bezieht sich auf die dynamische Zeitraum-XML, mit der die Dropdown-Liste für Zeiträume im Schritt "Ergebnisbedingungen" der abfragebasierten Assistenten gefüllt wird.

Der Filter für den CALM-Anwendungszugriff gibt die Aktionsbeschränkungen für jede Ressource an.

Filter

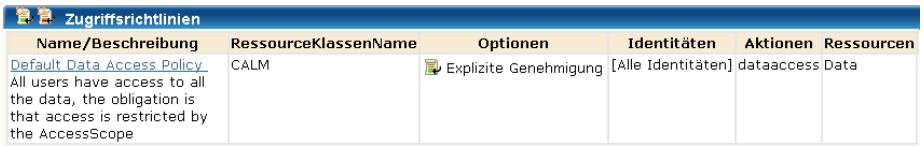
```
WHERE  ( req:resource      ==  val:ApplicationInstance
  AND    req:action        {}  val:read                          )
   OR  ( req:resource      ==  val:Policy
  AND    req:action        {}  val:read                          )
   OR  ( req:resource      ==  val:User
  AND    req:action        {}  val:read,write
  AND    name:cn           ==  req:identity                      )
   OR  ( req:resource      ==  val:GlobalUser
  AND    req:action        {}  val:read
  AND    name:cn           ==  req:identity                      )
   OR  ( req:resource      ==  val:AppObject
  AND    req:action        ==  val:read
  AND    name:pozFolder *--* val:/CALM_Configuration/Content/Profiles )
   OR  ( req:action        ==  val:read
  AND    req:resource      ==  val:AppObject
  AND    name:pozFolder *--* val:/CALM_Configuration/flex       )
```

5. Suchen Sie wie folgt nach Richtlinien für alle Benutzer:
   a. Klicken Sie im linken Fensterbereich auf "Zugriffsrichtlinien".
   b. Wählen Sie "Richtlinien mit zutreffender Identität anzeigen". Deaktivieren Sie andere ausgewählte Optionen.
   c. Geben Sie in das Feld "Identität hinzufügen" [Alle Identitäten] ein.
   d. Klicken Sie auf "Hinzufügen".
   e. Klicken Sie auf "Los".

   Vier Richtlinien werden angezeigt, einschließlich der CEG-Richtlinie und der Standard-Datenzugriffsrichtlinie. (Wenn Sie nicht ausdrücklich [Alle Identitäten] eingeben, werden viele zusätzliche Richtlinien angezeigt.)

6. Überprüfen Sie die Standard-Datenzugriffsrichtlinie.

   Die vordefinierte Standard-Datenzugriffsrichtlinie der CALM-Ressourcenklasse gewährt nach Maßgabe eines Zugriffsfilters allen Benutzern Zugriff auf CA Enterprise Log Manager-Daten. Ein Zugriffsfilter wird in eine Pflichtrichtlinie mit dem Pfad "FulfillOnGrant Action to dataaccess/CALM/Data" umgewandelt.

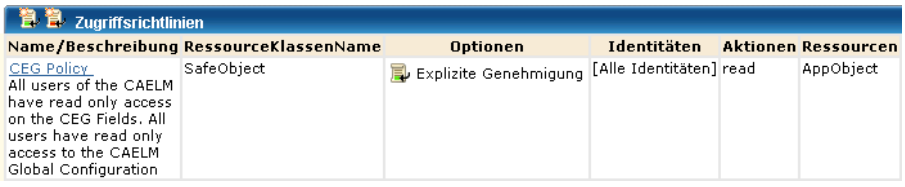


Zugriffsrichtlinien

Name/Beschreibung	RessourceKlassenName	Optionen	Identitäten	Aktionen	Ressourcen
Default Data Access Policy All users have access to all the data, the obligation is that access is restricted by the AccessScope	CALM	Explizite Genehmigung	[Alle Identitäten]	dataaccess	Data

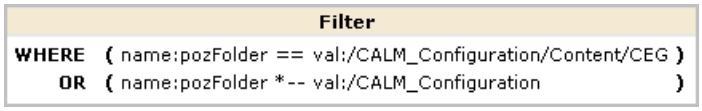
7. Überprüfen Sie die Richtlinie zur Bereichsdefinierung "CEG-Richtlinie".

   Die vordefinierte CEG-Richtlinie befähigt alle Benutzer mit CALM-Anwendungszugriff dazu, Felder für die ELM-Schemadefinition anzuzeigen. Daher werden bei einfachen und erweiterten Filtern für alle Benutzer die CEG-Felder in Dropdown-Listen angezeigt, da alle Benutzer für ihre Abfragen globale und lokale Filter festlegen können. Benutzer mit Rechten zum Erstellen und Bearbeiten von Abfragen können Filter für die Abfragen festlegen, die sie erstellen und bearbeiten. Diese Richtlinie stellt außerdem sicher, dass alle Benutzer die Einstellungen der globalen Konfiguration sehen können.



Zugriffsrichtlinien

Name/Beschreibung	RessourceKlassenName	Optionen	Identitäten	Aktionen	Ressourcen
CEG Policy All users of the CAELM have read only access on the CEG Fields. All users have read only access to the CAELM Global Configuration	SafeObject	Explizite Genehmigung	[Alle Identitäten]	read	AppObject



Filter

```
WHERE  ( name:pozFolder == val:/CALM_Configuration/Content/CEG )
  OR   ( name:pozFolder *-- val:/CALM_Configuration             )
```

Überprüfen von Richtlinien für Auditoren

Sie können die vordefinierten Richtlinien für Auditoren überprüfen, um herauszufinden, wie durch diese der Anwendungszugriff auf Ressourcen beschränkt wird, die für die Durchführung nachstehender Aufgaben benötigt werden:

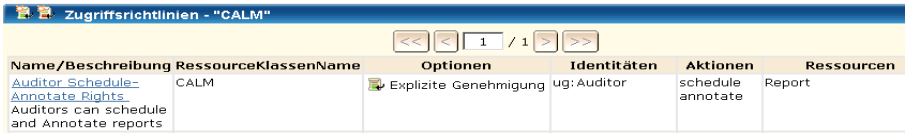
- Planen und Anmerken von Berichten
- Anzeigen von Berichten

So überprüfen Sie vordefinierte Richtlinien für Auditoren:

1. Klicken Sie auf die Registerkarte "Verwaltung" und auf die Unterregisterkarte "Benutzer- und Zugriffsverwaltung".
2. Klicken Sie im linken Fensterbereich auf "Zugriffsrichtlinien".
3. Suchen Sie wie folgt nach Richtlinien für Auditoren:
   a. Wählen Sie "Richtlinien mit zutreffender Identität anzeigen".
   b. Geben Sie in das Feld "Identität hinzufügen" "ug:Auditor" ein.
   c. Klicken Sie auf "Hinzufügen".
   d. Klicken Sie auf "Los".

   Alle Richtlinien für [Alle Identitäten] und diejenigen mit "ug:Auditor" werden angezeigt.
4. Überprüfen Sie die Richtlinie zur Gewährung von Auditorenrechten zum Planen und Anmerken.

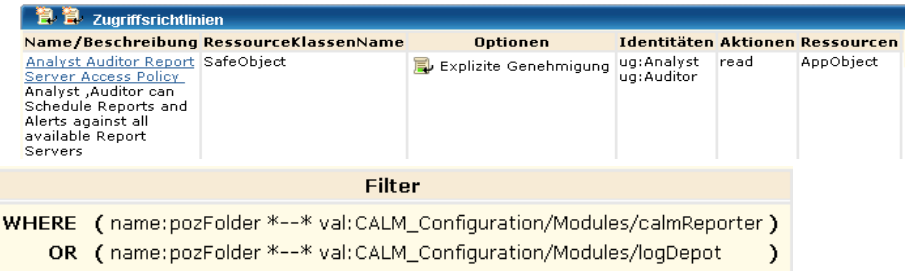
   Alle CALM-Zugriffsrichtlinien definieren die Aktionen, die im Hinblick auf anwendungsspezifische Ressourcen durchgeführt werden können. Diese Richtlinie befähigt Benutzer mit der zugewiesenen Anwendungsbenutzergruppe "Auditor" zum Planen und Anmerken von Berichten.



   Vergleichen Sie diese Richtlinie mit der Richtlinie zum Erstellen, Planen und Anmerken durch Analysten und der Richtlinie zum Erstellen durch Administratoren.

5. Überprüfen Sie die Zugriffsrichtlinie für den Zugriff auf den Berichtsserver durch Analysten und Auditoren.

   Diese Richtlinie zur Bereichsdefinierung ermöglicht es Auditoren, für das Berichtsziel beliebige Berichtsserver festzulegen und einen föderierten Bericht zu erstellen. Dies erfordert den Zugriff auf sämtliche Ereignisprotokollspeicher. Diese Richtlinie enthält die Ressource "AppObject". Anwendungsobjekte sind die Berichtsserver und Ereignisprotokollspeicher.



Zugriffsrichtlinien

Name/Beschreibung	RessourceKlassenName	Optionen	Identitäten	Aktionen	Ressourcen
Analyst Auditor Report Server Access Policy Analyst ,Auditor can Schedule Reports and Alerts against all available Report Servers	SafeObject	Explizite Genehmigung	ug:Analyst ug:Auditor	read	AppObject

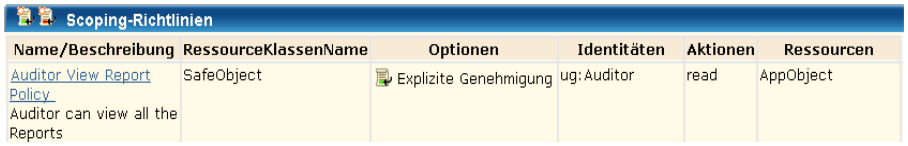
Filter

```
WHERE  ( name:pozFolder *--* val:CALM_Configuration/Modules/calmReporter )
   OR  ( name:pozFolder *--* val:CALM_Configuration/Modules/logDepot      )
```

   Hinweis: Zu einer bestimmten CALM-Zugriffsrichtlinie, d. h. eine Richtlinie für die CALM-Ressourcenklasse gibt es normalerweise eine zugehörige Richtlinie zur Bereichsdefinierung für die SafeObject-Ressourcenklasse.

6. Überprüfen Sie die Richtlinie zum Anzeigen von Berichten durch Auditoren.

   Diese Richtlinie zur Bereichsdefinierung gewährt Benutzern Lesezugriff auf Berichte. In dieser Richtlinie ist die Ressource "AppObject" (Anwendungsobjekt) aufgelistet.



Scoping-Richtlinien

Name/Beschreibung	RessourceKlassenName	Optionen	Identitäten	Aktionen	Ressourcen
Auditor View Report Policy Auditor can view all the Reports	SafeObject	Explizite Genehmigung	ug:Auditor	read	AppObject

   "AppObject" ist mit Hilfe eines Filters auf eine bestimmte Anwendungsressource beschränkt. Dieser gewährt das Recht, Berichte anzuzeigen. Der zugehörige Pfad ist ein EEM-Ordnerpfad, in dem die Inhalte aller Berichte gespeichert sind.

Filter

```
WHERE  ( name:pozFolder *--* val:/CALM_Configuration/Content/Reports )
```

Überprüfen von Richtlinien für Analysten

Sie können die vordefinierten Richtlinien für Analysten überprüfen, um herauszufinden, wie durch diese der Anwendungszugriff auf Ressourcen beschränkt wird, die für die Durchführung nachstehender Aufgaben benötigt werden:

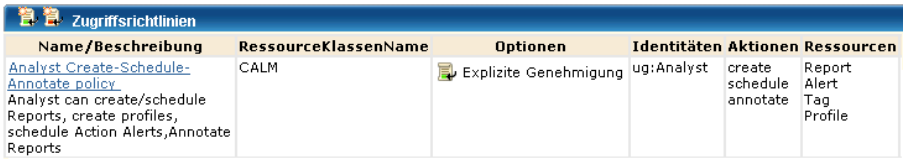
- Planen und Anmerken von Berichten (Aufgaben des Auditors)
- Anzeigen von Berichten (Aufgabe des Auditors)
- Erstellen von Berichten und Kennungen
- Erstellen und Planen von Alarmen (Abfragen)
- Bearbeiten von Berichten, Alarmen und Kennungen

So überprüfen Sie vordefinierte Richtlinien für Analysten:

1. Klicken Sie auf die Registerkarte "Verwaltung" und auf die Unterregisterkarte "Benutzer- und Zugriffsverwaltung".
2. Klicken Sie im linken Fensterbereich auf "Zugriffsrichtlinien".
3. Suchen Sie wie folgt nach Richtlinien für Analysten:
   a. Entfernen Sie das Häkchen vor "Richtlinien mit zutreffendem Namen anzeigen".
   b. Wählen Sie "Richtlinien mit zutreffender Identität anzeigen".
   c. Geben Sie in das Feld "Identität hinzufügen" "ug:Analyst" ein.
   d. Klicken Sie auf "Hinzufügen".
   e. Klicken Sie auf "Los".
4. Alle Richtlinien für "ug:Analyst" werden angezeigt, einschließlich [Alle Identitäten], die diese Benutzergruppe beinhalten.

5. Überprüfen Sie die Richtlinie zum Erstellen, Planen und Anmerken durch Analysten.

   Diese CALM-Zugriffsrichtlinie definiert die Aktionen, die im Hinblick auf anwendungsspezifische Ressourcen durchgeführt werden können. Die Richtlinie befähigt Benutzer mit der zugewiesenen CA Enterprise Log Manager-Anwendungsbenutzergruppe "Analyst" zum Erstellen, Planen und Anmerken von Berichten, zum Erstellen und Planen von Aktionsalarmen sowie zum Erstellen von Kennungen. (Auditoren können Berichte lediglich planen und Anmerkungen hinzufügen.)

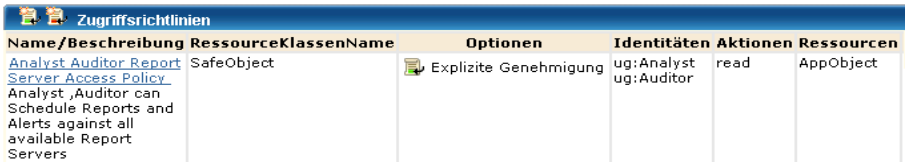


Zugriffsrichtlinien

Name/Beschreibung	RessourceKlassenName	Optionen	Identitäten	Aktionen	Ressourcen
Analyst Create-Schedule-Annotate policy Analyst can create/schedule Reports, create profiles, schedule Action Alerts,Annotate Reports	CALM	Explizite Genehmigung	ug:Analyst	create schedule annotate	Report Alert Tag Profile

6. Überprüfen Sie die Zugriffsrichtlinie für den Zugriff auf den Berichtsserver durch Analysten und Auditoren.

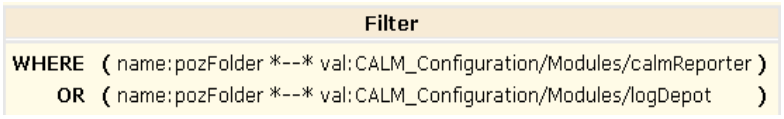
   Diese Bereichsrichtlinie gewährt Analysten Planungsrechte für alle Berichtsserver. In dieser Richtlinie ist die Ressource "AppObject" (Anwendungsobjekt) aufgelistet.



Zugriffsrichtlinien

Name/Beschreibung	RessourceKlassenName	Optionen	Identitäten	Aktionen	Ressourcen
Analyst Auditor Report Server Access Policy Analyst ,Auditor can Schedule Reports and Alerts against all available Report Servers	SafeObject	Explizite Genehmigung	ug:Analyst ug:Auditor	read	AppObject

   "AppObject" ist mit Hilfe von Filtern auf bestimmte Ressourcen beschränkt.



Filter	
WHERE	(name:pozFolder *--* val:CALM_Configuration/Modules/calmReporter)
OR	(name:pozFolder *--* val:CALM_Configuration/Modules/logDepot)

   - Der Filter mit der Endung "calmReporter" gewährt Lesezugriff auf alle Berichtsserver. Während der Planung eines Berichts werden die Zielberichtsserver angegeben, von denen aus der generierte Bericht angezeigt werden kann.
   - Der Filter mit der Endung "logDepot" gewährt Zugriff auf alle Ereignisprotokollspeicher. Wenn ein Bericht als föderiert definiert wird, werden Abfragen für die Daten in allen zutreffenden Ereignisprotokollspeichern durchgeführt. Ob ein Ereignisprotokollspeicher in Frage kommt, ist bei hierarchischen Föderationen abhängig von der hierarchischen Position des Servers, auf dem der Bericht initiiert wird.

7. Überprüfen Sie die Richtlinie zum Anzeigen und Bearbeiten von Berichten durch Analysten.

   Diese Richtlinie zur Bereichsdefinierung befähigt Benutzer mit der zugewiesenen Rolle "Analyst" zum Anzeigen, Bearbeiten oder Löschen sämtlicher Berichte. In dieser Richtlinie ist die Ressource "AppObject" (Anwendungsobjekt) angegeben.

Scoping-Richtlinien

Name/Beschreibung	RessourceKlassenName	Optionen	Identitäten	Aktionen	Ressourcen
Analyst Report View-Edit Policy Analyst can View/Edit any Report	SafeObject	Explizite Genehmigung	ug:Analyst	read write	AppObject

   "AppObject" ist durch den folgenden Filter auf Berichte beschränkt. Er gewährt das Recht zum Anzeigen generierter Berichte, die im EEM-Verzeichnis "/CALM_Configuration/Content/Reports" gespeichert sind.

Filter
WHERE (name:pozFolder *--* val:/CALM_Configuration/Content/Reports)

   Hinweis: Die durch diese Richtlinie gewährte Fähigkeit zum Bearbeiten von Berichten wird durch die CEG-Richtlinie erweitert, welche dazu berechtigt, mittels CEG-Spalten Filter zu Berichten hinzuzufügen.

Überprüfen von Richtlinien für Administratoren

Administratoren weisen die Rolle "Administrator" Benutzern zu, die vollständigen Zugriff auf die Anwendung CA Enterprise Log Manager und ihre gesamten Funktionen haben müssen. Sie können die vordefinierten Richtlinien für Administratoren überprüfen, um herauszufinden, wie der Zugriff Benutzern gewährt wird, die nachstehende Aufgaben ausführen müssen:

- Erstellen einer Ereignisgruppierung, d. h. Erstellen von Unterdrückungs- und Zusammenfassungsregeln mittels ELM-Schemadefinition
- Erstellen einer Integration, d. h. Erstellen von Datenzuordnungs- und Nachrichtenanalysedateien mittels ELM-Schemadefinition
- Erstellen einer Ereignisweiterleitung, d. h. Erstellen von Regeln für die Ereignisweiterleitung an Drittanbietersysteme
- Ausführen einer Datenbank-Abfrage, d. h. mittels Archivkatalogabfrage nach den Namen von Datenbanken suchen, die gesichert und extern archiviert wurden
- Anzeigen oder Bearbeiten von Richtlinien
- Anzeigen oder Bearbeiten von benutzerdefinierten Kalendern
- Anzeigen und Bearbeiten von Anwendungsobjekten Anwendungsobjekte sind Berichtsvorlagen, Abfragevorlagen, geplante Berichtsjobs, Alarmjobs, Profile, Servicekonfigurationen, Datenzuordnungsdateien, Nachrichtenanalysedateien (XMP), Unterdrückungs- und Zusammenfassungsregeln und Regeln für die Ereignisweiterleitung.
- Erstellen von Filtern mit Hilfe des iPoz-Attributs von "AppObject"
- Anzeigen der Ordner unter "Verwaltung", "Benutzer- und Zugriffsverwaltung", "EEM-Ordner" und Bearbeiten sämtlicher benutzerdefinierter Daten in diesen Ordnern
- Anzeigen oder Bearbeiten von Details in Bezug auf alle Anwendungsbenutzer, Anwendungsbenutzergruppen oder globale Benutzer
- Alle Analysten- und Auditoraufgaben

So überprüfen Sie vordefinierte Richtlinien für Administratoren:

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

3. Suchen Sie wie folgt nach Richtlinien für Administratoren:

   a. Wählen Sie "Richtlinien mit zutreffender Identität anzeigen".

   b. Geben Sie in das Feld "Identität hinzufügen" "ug:Administrator" ein.

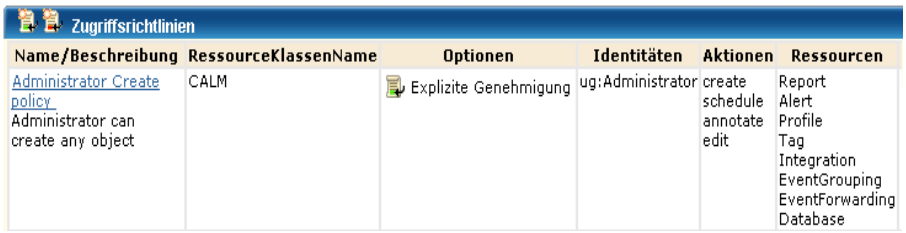
   c. Klicken Sie auf "Hinzufügen".

   d. Klicken Sie auf "Los".

   Alle Richtlinien für [Alle Identitäten] und diejenigen mit "ug:Administrator" werden angezeigt.

4. Überprüfen Sie die CALM-Zugriffsrichtlinie "Richtlinie zum Erstellen durch Administratoren".

   Diese Richtlinie definiert die Aktionen, die im Hinblick auf anwendungsspezifische Ressourcen durchgeführt werden können. Die Richtlinie befähigt Benutzer mit der zugewiesenen Anwendungsbenutzergruppe "Administrator" zur Durchführung der angegebenen Aktionen, welche jeweils auf die aufgelisteten Ressourcen zutreffen.



Zugriffsrichtlinien

Name/Beschreibung	RessourceKlassenName	Optionen	Identitäten	Aktionen	Ressourcen
Administrator Create policy Administrator can create any object	CALM	Explizite Genehmigung	ug:Administrator	create schedule annotate edit	Report Alert Profile Tag Integration EventGrouping EventForwarding Database

5. Überprüfen Sie die CALM-Zugriffsrichtlinie "Richtlinie zur Agentenverwaltung durch Administratoren".

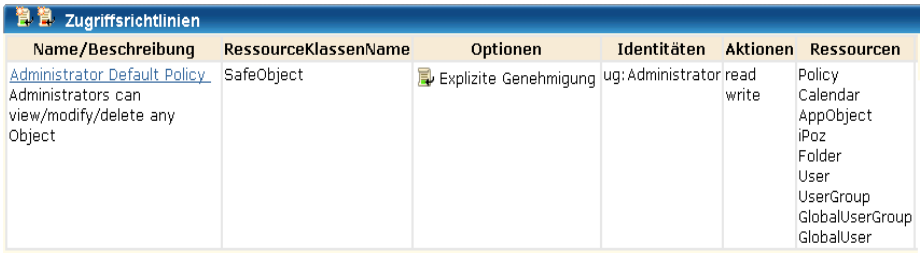
   Die Richtlinie berechtigt Administratoren zum Erstellen von Agentengruppen, zum Bearbeiten aller Agentengruppen, zum Konfigurieren von Connectors und zum Erstellen von Integrationen. Sie ermöglicht Administratoren die Bearbeitung des Authentifizierungsschlüssels des Agenten für die Anwendungsinstanz des CA Enterprise Log Manager-Servers, auf die der Agent erfasste Ereignisse überträgt. Standardmäßig gilt der konfigurierte Authentifizierungsschlüssel des Agenten für alle CA Enterprise Log Manager-Server über Anwendungsinstanzen hinweg. Er kann jedoch auf eine spezifische Anwendungsinstanz festgelegt werden.

Zugriffsrichtlinien

Name/Beschreibung	RessourceKlassenName	Optionen	Identitäten	Aktionen	Ressourcen
Admin Agent Manager Policy Access Rights for Admnistrator for Agent Management	CALM	Explizite Genehmigung	ug:Administrator	edit	AgentConfiguration AgentAuthenticationKey Connector ALL_GROUPS Integration

6. Überprüfen Sie die Richtlinie zur Bereichsdefinierung "Administratorstandardrichtlinie".

   Diese Richtlinie gewährt Administratoren das Recht, die aufgeführten Ressourcen anzuzeigen, zu bearbeiten oder zu löschen. Die aufgeführten Ressourcen sind nicht spezifisch für CA Enterprise Log Manager und AppObject. AppObject bezieht sich auf anwendungsspezifische Objekte, d. h. auf Ressourcen, die in der Richtlinie für die CALM-Administratorerstellung und in der Richtlinie für den CALM-Admin-Agentenmanager aufgeführt sind.



Zugriffsrichtlinien

Name/Beschreibung	RessourceKlassenName	Optionen	Identitäten	Aktionen	Ressourcen
Administrator Default Policy Administrators can view/modify/delete any Object	SafeObject	Explizite Genehmigung	ug:Administrator	read write	Policy Calendar AppObject iPoz Folder User UserGroup GlobalUserGroup GlobalUser

Zugriffsrichtlinien für registrierte Produkte

Wenn ein Produkt für CA Enterprise Log Manager registriert wird, wird ein neues Zertifikat generiert und bestimmte Zugriffsrichtlinien werden aktualisiert, um Lesezugriff für alle Kennungen, Abfragen und Berichte zu gewähren. Im Besonderen wird der Name des Zertifikats, mit dem das registrierte Produkt authentifiziert wird, als Zertifikatsname "Identität" zu folgenden Richtlinien hinzugefügt:

- CALM-Anwendungszugriff
- Zugriffsrichtlinie für den Zugriff auf den Berichtsserver durch Analysten und Auditoren
- Richtlinie zum Anzeigen und Bearbeiten von Berichten durch Analysten

Durch das Hinzufügen des Zertifikatnamens zu den Richtlinien können die Benutzer eines jeden CA-Produkts, eines Fremdanbieterprodukts oder CA-Kunden eine Liste der Abfragen und Berichte nach Kennung erhalten. Diese Benutzer können die Listen in ihrer eigenen Benutzeroberfläche anzeigen und die feiner gefilterten Ereignisdaten abrufen, die sie benötigen.

Sichern aller Zugriffsrichtlinien

Der Export vordefinierter Zugriffsrichtlinien ist empfehlenswert, um für den Fall, dass eine Zugriffsrichtlinie unabsichtlich gelöscht oder beschädigt wird, eine Sicherungskopie zurückzubehalten.

Wichtig! Da Richtlinien während eines Neustarts des Systems oder des CA EEM-Service beschädigt werden können, ist es wichtig, für die Wiederherstellung eine aktuelle Version zu sichern. Außerdem sollten Sie CA EEM regelmäßig sichern, z. B. nach der Installation eines neuen CA Enterprise Log Manager und nach dem Erstellen benutzerdefinierter Richtlinien.

Sie können alle Richtlinien aller Typen von Zugriffsrichtlinien exportieren. Wenn Sie Richtlinien exportieren, wird für jede Richtlinie des ausgewählten Typs eine XML-Datei angelegt. Die XML-Dateien werden in eine Zip-Datei gepackt, deren Bezeichnung "CAELM[1].xml.gz" lautet und die das "CAELM[1].xml"-Dokument enthält. Die exportierte Zip-Datei können Sie in einem Verzeichnis Ihrer Wahl speichern.

Bevor Sie Ihre gespeicherte Sicherungsdatei wiederherstellen können, müssen Sie sie in das folgende Verzeichnis des CA Enterprise Log Manager mit dem internen Benutzerspeicher kopieren: /opt/CA/LogManager/EEM. Sie können diesen Kopiervorgang gleich nach dem Speichern in Ihr lokales Verzeichnis vornehmen, oder Sie können damit warten, bis eine Wiederherstellung erforderlich ist.

Das Format, in dem Richtlinien exportiert werden, hängt ab von der Anzahl der exportierten Objekte.

- *Dateiname*.tar.gz wird für eine sehr große Anzahl exportierter Objekte verwendet
- *Dateiname*.xml.gz wird für eine kleine bis mittlere Anzahl exportierter Objekte verwendet

Es ist gute Praxis, *Dateiname* (CAELM[n]) beim Export in sinnvoller Weise umzubenennen. Exportieren Sie z. B. die Dateien aus drei Ordnern mit vordefinierten Richtlinien als CAELM_CalmZugriffsRichtlinien, CAELM_EreignisRichtlinien und CAELM_BereichsRichtlinien.

Hinweis: Es müssen dieselben Erweiterungen, "xml.gz" oder "tar.gz", beibehalten werden.

Sie können die XML-Datei mit der Definition der Zugriffsrichtlinie aus der Zip-Datei extrahieren und als Eingabe für das Hilfsprogramm "safex" verwenden, das zum Wiederherstellen der Zugriffsrichtlinie verwendet wird.

So sichern Sie alle Zugriffsrichtlinien:

1. Klicken Sie auf die Registerkarte "Verwaltung" und anschließend auf die Unterregisterkarte "Benutzer- und Zugriffsverwaltung".
2. Sichern Sie die vordefinierten CALM-Zugriffsrichtlinien folgendermaßen:
   a. Klicken Sie auf die Schaltfläche "Zugriffsrichtlinien".
   b. Klicken Sie auf "CALM".

      Die Richtlinientabelle "Zugriffsrichtlinien - CALM" wird angezeigt
   c. Klicken Sie auf die Schaltfläche "Exportieren".
   d. Das Dialogfeld "Datei herunterladen" mit Optionen zum Öffnen oder Speichern wird eingeblendet.
   e. (Optional) Klicken Sie auf "Öffnen", um die Zip-Datei "CAELM[1].xml.gz" zu öffnen. Doppelklicken Sie auf "CAELM[1].xml", um die Datei im XML-Format einzusehen.
   f. Klicken Sie zum Speichern der Datei auf "Speichern".

      Das Dialogfeld "Speichern unter" wird angezeigt.
   g. Wählen Sie den Zielordner, in dem die Datei gespeichert werden soll, ändern Sie ggf. den Dateinamen, und klicken Sie auf "Speichern".

      Wenn Sie den Dateinamen nicht ändern, wird die Zip-Datei unter "CAELM[1].xml.gz" gespeichert.
   h. Klicken Sie auf "Schließen".

      Das Dialogfeld "Herunterladen abgeschlossen" wird geschlossen. Die Richtlinienliste wird im linken Fensterbereich angezeigt.

3. Sichern Sie die vordefinierten CALM-Ereignisrichtlinien folgendermaßen:
   a. Klicken Sie auf "Ereignisrichtlinien".

      Die Richtlinientabelle "Ereignisrichtlinien" wird angezeigt

   b. Klicken Sie auf die Schaltfläche "Exportieren".

   c. Das Dialogfeld "Datei herunterladen" mit Optionen zum Öffnen oder Speichern wird eingeblendet.

   d. Klicken Sie zum Speichern der Datei auf "Speichern".

      Eine Meldung wird angezeigt, in der Sie gefragt werden, ob Sie die vorhandene" CAELM[1].xml.gz"-Datei ersetzen möchten.

   e. Klicken Sie auf "Nein".

   f. Geben Sie einen eindeutigen Namen in das Feld "Dateiname" ein, und klicken Sie auf "Speichern". Ändern Sie z. B. den Namen nach "CAELM[2].xml.gz" oder geben Sie eine Bezeichnung für den Richtlinientyp ein wie etwa "CAELM_Ereignisrichtlinien".

   g. Klicken Sie auf "Schließen".

      Das Dialogfeld "Herunterladen abgeschlossen" wird geschlossen. Die Richtlinienliste wird im linken Fensterbereich angezeigt.

4. Sichern Sie die vordefinierten CALM-Bereichsrichtlinien folgendermaßen:
   a. Klicken Sie auf "Bereichsrichtlinien".

      Die Richtlinientabelle "Bereichsrichtlinien" wird angezeigt

   b. Klicken Sie auf die Schaltfläche "Exportieren". Möglicherweise müssen Sie horizontal scrollen, um die Schaltfläche in der oberen rechten Ecke des Bildschirms anzuzeigen.

   c. Das Dialogfeld "Datei herunterladen" mit Optionen zum Öffnen oder Speichern wird eingeblendet.

   d. Klicken Sie zum Speichern der Datei auf "Speichern".

      Eine Meldung wird angezeigt, in der Sie gefragt werden, ob Sie die vorhandene" CAELM[1].xml.gz"-Datei ersetzen möchten.

   e. Klicken Sie auf "Nein".

   f. Geben Sie einen eindeutigen Namen in das Feld "Dateiname" ein, und klicken Sie auf "Speichern". Ändern Sie z. B. den Namen nach "CAELM[3].xml.gz" oder geben Sie eine Bezeichnung für den Richtlinientyp ein wie etwa "CAELM_Bereichsrichtlinien".

   g. Klicken Sie auf "Schließen".

      Das Dialogfeld "Herunterladen abgeschlossen" wird geschlossen. Die Richtlinienliste wird im linken Fensterbereich angezeigt.

5. Klicken Sie auf "Schließen".

   Die Liste "Zugriffsrichtlinien" wird geschlossen.

Beispiel: "CAELM[1].xml" für CALM-Zugriffsrichtlinien

Im Folgenden wird ein Eintrag für eine Richtlinie in der "CAELM[1].xml"-Datei gezeigt.

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
- <Safex>
    <Attach label="CAELM" />
    <Add />
  - <AddOrModify>
    - <Policy folder="/" name="Auditor Schedule-Annotate Rights">
        <Description>Auditors can schedule and Annotate reports</Description>
        <ResourceClassName>CALM</ResourceClassName>
        <PolicyType>policy</PolicyType>
        <Disabled>False</Disabled>
        <ExplicitDeny>False</ExplicitDeny>
        <PreDeployment>False</PreDeployment>
        <RegexCompare>False</RegexCompare>
        <Resource>Report</Resource>
        <Action>schedule</Action>
        <Action>annotate</Action>
        <Identity>ug:Auditor</Identity>
        <Attribute name="CreateTimestamp">20080926053329</Attribute>
      </Policy>
```

Wiederherstellen von Zugriffsrichtlinien

Sie können eine Zugriffsrichtlinie, die gelöscht oder so geändert wurde, dass sie Probleme verursacht, wiederherstellen. Wird eine Zugriffsrichtlinie versehentlich gelöscht oder beschädigt, sind die in dieser Richtlinie als "Identitäten" ausgewiesenen Benutzer nicht mehr in der Lage, auf CA Enterprise Log Manager zuzugreifen, bis die Richtlinie neu definiert oder wiederhergestellt wird.

Zur Wiederherstellung von Zugriffsrichtlinien muss das Hilfsprogramm "safex" für Richtlinien ausgeführt werden.

Verwenden Sie – abhängig davon, ob beim Export eine Sicherungsdatei mit der Erweiterung "xml.gz" oder "tar.gz" erstellt wurde – eines der beiden folgenden Verfahren.

So stellen Sie Zugriffsrichtlinien mittels einer Sicherungsdatei namens "filename.xml.gz" wieder her:

1. Kopieren Sie Ihre gespeicherten Sicherungsdateien in das folgende Verzeichnis des CA Enterprise Log Manager der Verwaltung, normalerweise der erste installierte Server.

   ```
   /opt/CA/LogManager/EEM
   ```

2. Führen Sie folgenden Befehl aus, um die XML-Datei abzurufen:

   ```
   gunzip filename.xml.gz
   ```

   Auf diese Weise wird die Datei "*filename*.xml" erzeugt.

3. Optional: Wenn Sie nur eine der Richtlinien in der Gruppe, die Sie gesichert haben, wiederherstellen möchten, gehen Sie wie folgt vor:

   a. Öffnen Sie die XML-Datei.

   b. Löschen Sie bei den Richtlinien, die Sie nicht wiederherstellen möchten, die XML-Zeilen, welche mit den folgenden Tags beginnen bzw. enden: <Policy folder="/ name=*policyname*> und </Policy>

   c. Speichern Sie die Datei.

4. Führen Sie den folgenden Befehl aus (*eemserverhostname* bezieht sich auf den Hostnamen des CA Enterprise Log Manager der Verwaltung):

   ```
   ./safex –h eemserverhostname –u EiamAdmin –p password –f filename.xml
   ```

   Wenn der CA Enterprise Log Manager-Server im FIPS-Modus vorliegt, stellen Sie sicher, dass Sie die -Fips-Option einschließen.

Die in der Datei "filename.xml" definierten, in der Wiederherstellung befindlichen Richtlinien werden zum entsprechenden Richtlinientyp hinzugefügt und in Kraft gesetzt.

So stellen Sie Zugriffsrichtlinien mittels einer Sicherungsdatei namens "filename.tar.gz" wieder her:

1. Kopieren Sie Ihre gespeicherten Sicherungsdateien in das folgende Verzeichnis des CA Enterprise Log Manager der Verwaltung, normalerweise der erste installierte Server.

   ```
   /opt/CA/LogManager/EEM
   ```

2. Führen Sie folgenden Befehl aus, um die XML-Datei abzurufen:

   ```
   gunzip filename.tar.gz
   ```

   Auf diese Weise wird die Datei "*filename*.tar" erzeugt.

3. Führen Sie den folgenden Befehl aus:

   ```
   tar –xvf filename.tar
   ```

   Auf diese Weise wird die Datei "*filename*.xml" erzeugt.

4. Optional: Wenn Sie nur eine der Richtlinien in der Gruppe, die Sie gesichert haben, wiederherstellen möchten, gehen Sie wie folgt vor:

   a. Öffnen Sie die XML-Datei.

   b. Löschen Sie bei den Richtlinien, die Sie nicht wiederherstellen möchten, die XML-Zeilen, welche mit den folgenden Tags beginnen bzw. enden: <Policy folder="/ name=*policyname*> und </Policy>

   c. Speichern Sie die Datei.

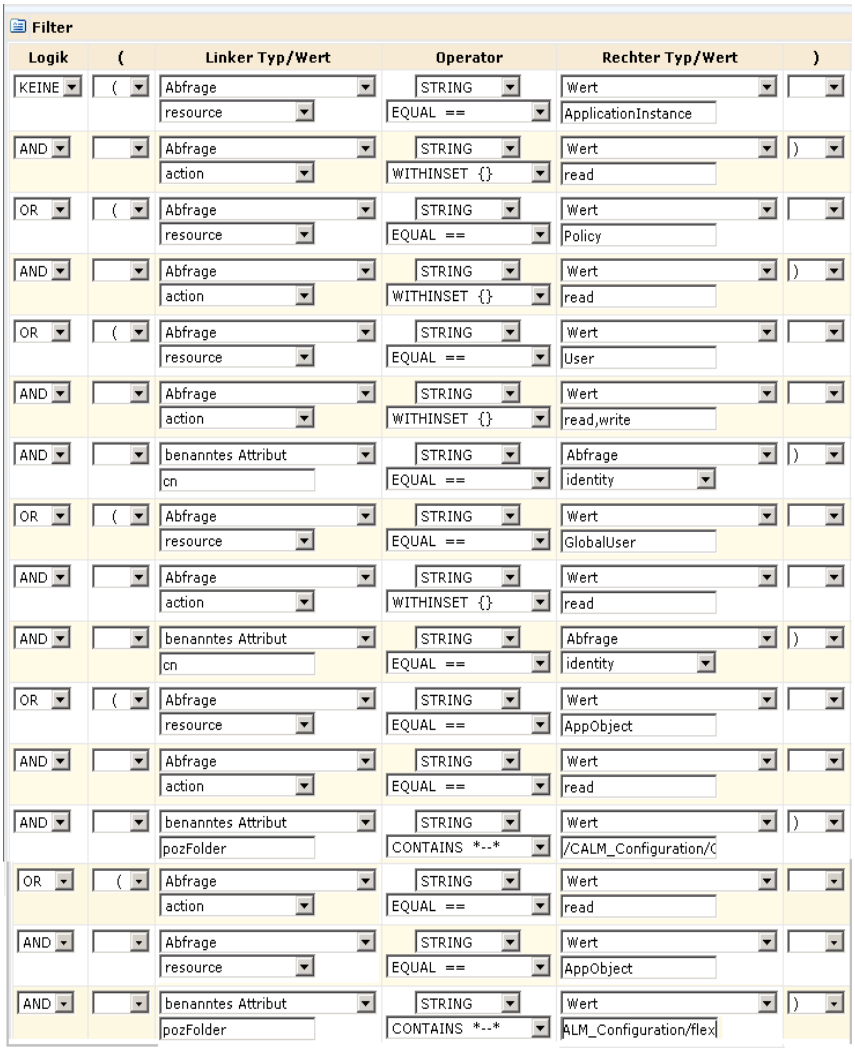
5. Führen Sie den folgenden Befehl aus (*eemserverhostname* bezieht sich auf den Hostnamen des CA Enterprise Log Manager der Verwaltung):

   ```
   ./safex –h eemserverhostname –u EiamAdmin –p password –f filename.xml
   ```

So erstellen Sie im Falle einer nicht vorhandenen Sicherungsdatei eine neue CALM-Zugriffsrichtlinie:

Wenn Sie keine Sicherungsdatei haben, können Sie die CALM-Anwendungszugriffsrichtlinie neu erstellen.

1. Neuerstellen der CALM-Anwendungszugriffsrichtlinie, siehe "vordefinierte Richtlinien".
2. Definieren Sie die Filter anhand folgender Abbildung: Die Teilpfade lauten:
   - /CALM_Configuration/Content/Profiles
   - /CALM_Configuration/flex



Durch das Vorhandensein dieser Richtlinie kann sich jeder Administrator anmelden und die anderen Richtlinien erstellen.

Kapitel 4: Benutzerdefinierte Rollen und Richtlinien

Dieses Kapitel enthält folgende Themen:

Hinweise zur Erstellung von Richtlinien

Alle CALM-Zugriffsrichtlinien und Richtlinien zur Bereichsdefinierung enthalten die Aktionen, die bestimmten Identitäten zur Ausführung auf bestimmten Ressourcen gewährt oder verweigert werden. Richtlinien für die CALM-Ressourcenklasse gewähren oder verweigern den angegebenen Identitäten die Möglichkeit, Aktionen auf Applikationsressourcen (CALM-Ressourcen) durchzuführen. Richtlinien für die SafeObject-Ressource "AppObject" gewähren oder verweigern den angegebenen Identitäten das Ausführen von Schreib- und Leseaktionen auf einer Ressource auf Applikationsebene, wobei die einzelnen Filter maßgeblich sind. Andere Richtlinien für die SafeObject-Ressourcenklasse gewähren oder verweigern den angegebenen Identitäten Schreib- und Leseaktionen in globalen Ressourcen.

Der zu erstellende Richtlinientyp hängt von der Ressource ab, auf die Sie den Zugriff beschränken möchten. Nachfolgend finden Sie eine Zusammenfassung der einzelnen Ressourcen und der jeweils erforderlichen Richtlinien:

- Ressourcen, die eine CALM-Richtlinie und Richtlinien zur Bereichsdefinierung für "AppObject" benötigen:
  - Ereignisweiterleitung
  - Ereignisgruppierung
  - Integration (nicht agentenbezogen)
  - Profil
  - Bericht
- Ressourcen, die nur eine CALM-Richtlinie erfordern:
  - Authentifizierungsschlüssel des Agenten
  - Agentenkonfiguration
  - Alert
  - ALLE_GRUPPEN
  - Connector
  - Database
  - Integration (agentenbezogen)
  - Kennung

- Ressourcen, die nur Richtlinien zur Bereichsdefinierung für die globale Ressource benötigen:
  - Kalender
  - Ordner
  - Globaler Benutzer
  - Globale Benutzergruppe
  - iPoz
  - Richtlinie
  - Benutzer
  - Benutzergruppe

Im Folgenden werden basierend auf den unterschiedlichen Ressourcen, für die Sie den Zugriff steuern möchten, verschiedene Herangehensweisen zur Erstellung von Richtlinien verdeutlicht.

So steuern Sie den Zugriff auf die Ressourcen "Ereignisweiterleitung", "Ereignisgruppierung", "Integration", "Profil" und "Bericht":

Die folgende Herangehensweise gilt nur für Richtlinien auf den CALM-Ressourcen "Ereignisgruppierung", "Integration", "Profil" und "Bericht". Diese Anwendungsressourcen erfordern eine CALM-Richtlinie und zwei Richtlinien zur Bereichsdefinierung.

1. Erstellen Sie eine CALM-Richtlinie für eine oder mehrere Anwendungsressourcen wie "Bericht" oder "Integration". Legen Sie eine oder mehrere anwendungsspezifische Aktionen fest, die für die angegebenen Ressourcen zulässig sind, zum Beispiel: Erstellen, Planen oder Anmerken Fügen Sie die Identitäten hinzu, denen die Ausführung der Aktionen gewährt oder verweigert wird.
2. Erstellen Sie eine begleitende Richtlinie zur Bereichsdefinierung für die AppObject-Ressource, die sowohl Lese- als auch Schreibaktionen autorisiert. Legen Sie die Schreibaktion so fest, dass die Identität die Ressource zwar bearbeiten oder löschen, jedoch nicht erstellen kann. Legen Sie die Leseaktion so fest, dass die Identität die Ressource anzeigen kann. Erstellen Sie einen Filter, der die AppObject-Ressource mit der zugehörigen Anwendungsressource verknüpft. Geben Sie im Filter den EEM-Verzeichnispfad an, in dem die Inhalte der angegebenen Ressource gespeichert sind oder das Modul, für das ein Zugriff auf die zugehörige Anwendungsressource erforderlich ist. Fügen Sie zu dieser Richtlinie dieselben Identitäten hinzu wie bei der zugehörigen CALM-Richtlinie.
3. Erstellen Sie eine zweite begleitende Richtlinie zur Bereichsdefinierung für die AppObject-Ressource, in der die Leseaktion autorisiert wird. Legen Sie die Leseaktion so fest, dass die Identität die Ressource anzeigen kann. Erstellen Sie einen Filter, der die AppObject-Ressource mit der zugehörigen Anwendungsressource verknüpft. Geben Sie im Filter den EEM-Verzeichnispfad an, in dem die Inhalte der angegebenen Ressource gespeichert sind oder das Modul, für das ein Zugriff auf die zugehörige Anwendungsressource erforderlich ist. Fügen Sie als Identitäten dieser Richtlinie Benutzer oder Benutzergruppen mit weniger Berechtigungen hinzu.

So steuern Sie den Zugriff auf Alarm, Datenbank, Kennung und agentenbezogene Ressourcen

Die folgende Herangehensweise gilt für Anwendungsressourcen, die nur eine CALM-Richtlinie zur Zugriffsgewährung und -Beschränkung benötigen.

- Erstellen Sie eine CALM-Zugriffsrichtlinie für eine Ressource wie etwa "Connector" oder "Kennung". Legen Sie die Aktion zum Bearbeiten so fest, dass die Identität die Ressource erstellen, bearbeiten und löschen sowie alle anderen zulässigen Aktionen durchführen kann. Fügen Sie die Identitäten hinzu, denen die Ausführung dieser Aktion gewährt oder verweigert wird.

  Hinweis: Mit dem Zugriff auf agentenbezogene Ressourcen sind die Schaltflächen für den Ordner "Agenten-Explorer" oder dessen Unterordner auf der Unterregisterkarte "Protokollerfassung" der Registerkarte "Verwaltung" verfügbar. Mit dem Zugriff auf die Ressource "Alarm" erhält die Identität Zugriff auf die Registerkarte "Alarme". Mit dem Zugriff auf die Ressource "Kennung" kann die Identität eine Kennung für benutzerdefinierte Abfragen oder Berichte erstellen. Mit dem Zugriff auf die Ressource "Datenbank" kann die Identität eine Archivabfrage durchführen.

Steuerung des Zugriffs auf globale Ressourcen, die in der CAELM-Anwendung verwendet werden

Die folgende Herangehensweise gilt für globale Ressourcen, die nur eine Richtlinie zur Bereichsdefinierung zur Zugriffsbeschränkung benötigen.

1. Erstellen Sie eine Richtlinie zur Bereichsdefinierung für eine oder mehrere globale Ressourcen wie Benutzer oder Richtlinie. Legen Sie die Schreibaktion so fest, dass die Identität die Ressource erstellen, bearbeiten oder löschen kann. Fügen Sie die Identitäten hinzu, denen die Ausführung dieser Aktion gewährt oder verweigert wird.
2. Erstellen Sie eine Richtlinie zur Bereichsdefinierung für eine oder mehrere globale Ressourcen wie Benutzer oder Richtlinie. Legen Sie die Leseaktion so fest, dass die Identität die globale Ressource anzeigen kann. Fügen Sie die Identitäten hinzu, denen die Ausführung dieser Aktion gewährt oder verweigert wird.

   Hinweis: Für globale Ressourcen stehen entsprechende Schaltflächen auf der Unterregisterkarte "Benutzer- und Zugriffsverwaltung" der Registerkarte "Verwaltung" zur Verfügung.

Weitere Informationen

CALM-Zugriffsrichtlinientypen (siehe Seite 80)
Ressourcen und Aktionen (siehe Seite 84)
CALM-Ressourcen und EEM-Ordner (siehe Seite 87)
Globale Ressourcen und CA EEM-Funktionalität (siehe Seite 90)
Erstellen einer CALM-Zugriffsrichtlinie (siehe Seite 100)

CALM-Zugriffsrichtlinientypen

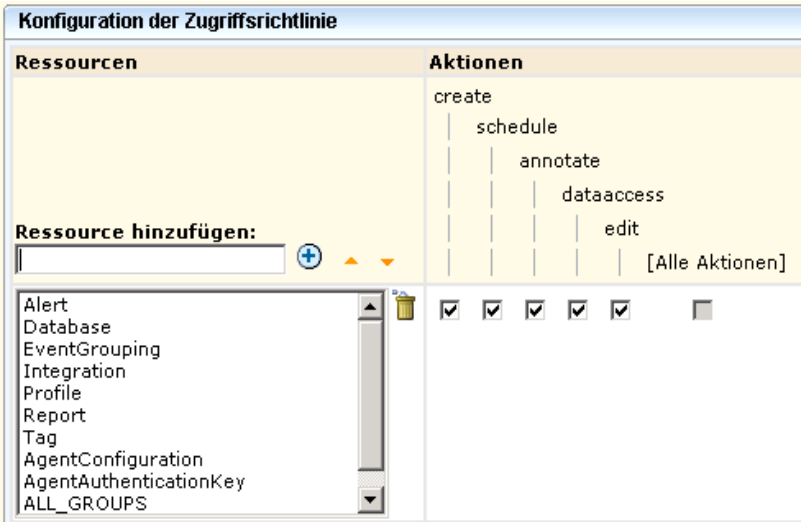
Wenn Sie eine Zugriffsrichtlinie für CALM oder eine Richtlinie zur Bereichsdefinierung erstellen, wählen Sie einen der folgenden drei Typen aus:

- Zugriffsrichtlinie
- Zugriffssteuerungsliste
- Zugriffssteuerungsliste für Identitäten

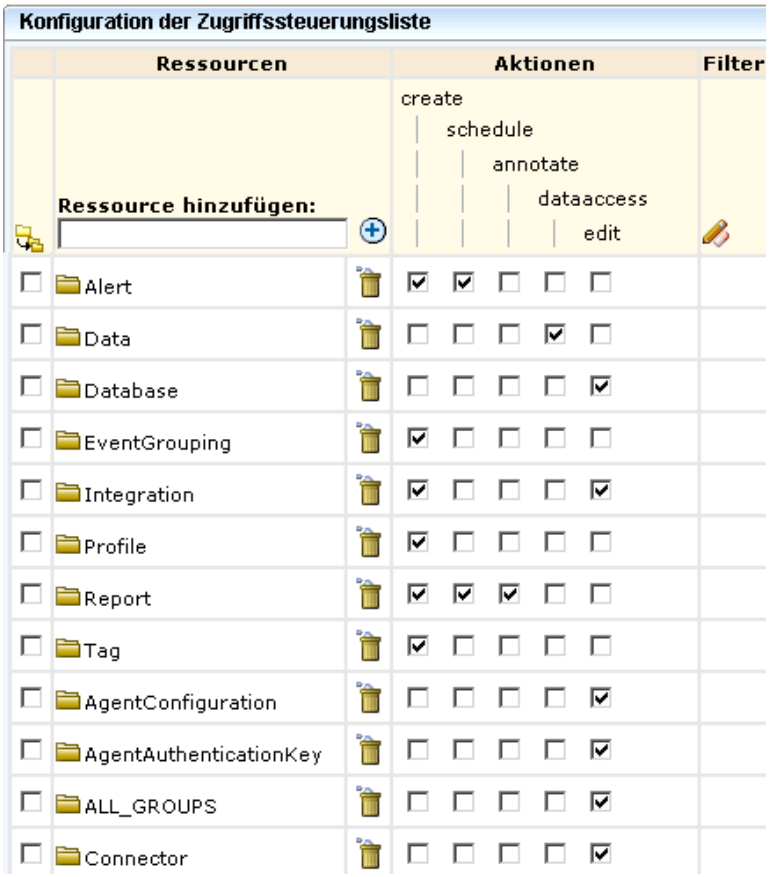
Die jeweilige Auswahl wirkt sich auf den Detailgrad der Zugriffsrichtlinienkonfiguration aus, wobei die Zugriffsrichtlinie am umfassendsten definiert ist.

Hinweis: Die hier gezeigten Beispiele stellen Zugriffsrichtlinien für die CALM-Ressourcenklasse dar und enthalten daher Aktionen und Ressourcen, die für CA Enterprise Log Manager gelten.

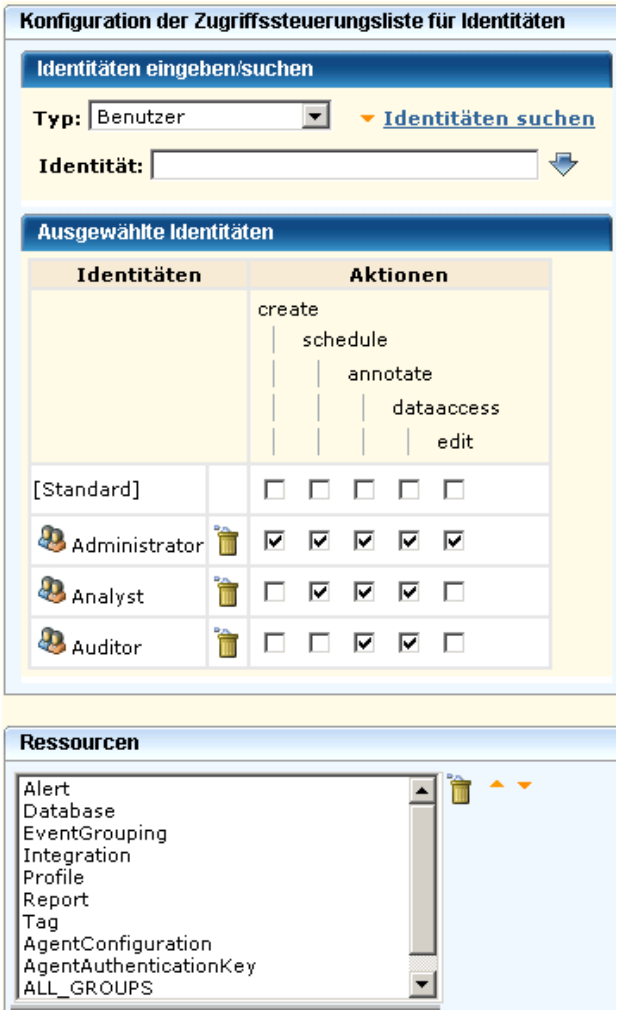
Eine Zugriffsrichtlinie gibt Aktionen an, die für alle ausgewählten Ressourcen gelten, die allen ausgewählten Identitäten gewährt werden. Wenn Sie eine generische Richtlinie für CA Enterprise Log Manager erstellen, fügen Sie zunächst Ressourcen der CALM-Ressourcenklasse hinzu und wählen anschließend Aktionen aus der angezeigten Liste aus. Die von Ihnen ausgewählten Aktionen gelten für alle ausgewählten Ressourcen, für die sie zulässig sind. Im vorliegenden Beispiel erlaubt die Richtlinie, dass jede ausgewählte Aktion für alle ausgewählten Ressourcen gilt, für die die Aktion "Erstellen" zulässig ist.



Bei einer Zugriffssteuerungsliste werden die für die einzelnen Ressourcen zulässigen Aktionen separat für die ausgewählten Identitäten angegeben. Wenn Sie eine ressourcenorientierte Richtlinie erstellen, geben Sie an, welche Aktionen für die jeweilige Ressource zulässig sind. Sie brauchen Aktionen für eine bestimmte Ressource nicht auswählen, nur weil sie gültig sind. So können Sie beispielsweise bei der Ressource "Bericht" die Aktion "Erstellen" markieren, jedoch bei der Ressource "Alarm" dieselbe Aktion ausschließen, obwohl sie für Alarme zulässig ist. Über die Zugriffsststeuerungsliste wird die Richtlinie am genauesten präzisiert, wenn sie jeweils für eine Identität implementiert wird.



Eine Zugriffssteuerungsliste für Identitäten gibt die Aktionen an, die ausgewählten Identitäten gewährt werden, und zwar in Bezug auf alle ausgewählten zutreffenden Ressourcen. Wenn Sie eine identitätsorientierte Richtlinie erstellen, bestimmen Sie, welche Identitäten welche Aktionen durchführen können (Erstellen, Planen, Anmerken, Bearbeiten). Dies erfolgt bei allen aufgelisteten Ressourcen, für die die einzelnen Aktionen jeweils gelten. Wenn Sie die Rechte eines Auditors zur Planung von Alarmen einschränken möchten, lassen Sie das Kästchen unter "Planen" leer. Wenn Sie Sie das Kästchen unter "Planen" leer lassen, würde dies auch die Rechte eines Auditors zur Planung von Berichten einschränken.



Ressourcen und Aktionen

Beim Erstellen von Richtlinien konfigurieren Sie eine Zugriffsrichtlinie, für die ein Zugriffsfilter erforderlich ist. 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, die von den angegebenen Benutzern oder Gruppen eingesehen werden. Zugriffsfilter werden automatisch in EEM-Pflichtrichtlinien konvertiert. Zugriffsfilter werden häufig in Form von relativen Pfaden für die Objekte angegeben, auf die der Benutzerzugriff beschränkt werden soll. Sie können diese relativen Pfade im EEM-Verzeichnisbereich der Oberfläche anzeigen.

Normalerweise werden Richtlinien, die Aktionen wie Erstellen und Planen autorisieren, mit Hilfe der CALM-Ressourcenklasse und CALM-Ressourcen definiert, z. B. Berichte, Kennungen, Datenzuordnungs- und Nachrichtenanalysedateien, Unterdrückungs- und Zusammenfassungsregeln. Richtlinien, die Lese- und Schreibaktionen autorisieren, werden mit Hilfe der SafeObject-Ressourcenklasse und der AppObject-Ressource definiert. Die Aktion "Bearbeiten" ist die einzig gültige Aktion für agentenbezogene Ressourcen in der CALM-Ressourcenklasse.

Im Folgenden sind insbesondere Aktionen aufgeführt, die für Objekte autorisiert werden können, welche zur CALM-Ressourcenklasse gehören:

Aktion	Ressource	Beschreibung
Anmerken	Bericht	Erfassen von Kommentaren in Berichten
Erstellen	Ereignisweiterleitung	Erstellen Sie Regeln zur Weiterleitung bestimmter Ereignisse an Drittanbieteranwendungen.
Erstellen	Ereignisgruppierung	Erstellen von Unterdrückungs- und Zusammenfassungsregeln mittels ELM-Schemadefinition
Erstellen	Integration	Erstellen von Datenzuordnungs- und Nachrichtenanalysedateien mittels ELM-Schemadefinition
Erstellen	Profil	Profile erstellen
Erstellen	Bericht	Erstellen von Berichten und Abfragen
Erstellen	Kennung	Erstellen von Kennungen für Berichte und Abfragen
Datenzugriff	Daten	Zugriff auf CALM-Ereignisdaten, Beschränkung möglich durch Datenzugriffsfilter

Aktion	Ressource	Beschreibung
Bearbeiten	Agentenkonfiguration	Erstellen von Agentengruppen Konfigurieren von installierten Agenten mit Quellen zur Erfassung und Ziel zur Verarbeitung
Bearbeiten	Authentifizierungsschlüssel des Agenten	Erstellen und Bearbeiten des während der Agenteninstallation angegebenen Authentifizierungsschlüssels des Agenten
Bearbeiten	ALLE_GRUPPEN	Bearbeiten aller verfügbaren Agentengruppen **Hinweis:** Der Zugriff kann auf eine bestimmte Agentengruppe beschränkt werden, indem der Name der Agentengruppe als Ressource angegeben wird.
Bearbeiten	Connector	Konfigurieren von Connectors
Bearbeiten	Database	Bestimmen der vorhandenen Protokolle, die den Kriterien der Archivkatalogabfrage entsprechen und Neukatalogisieren der Datenbank
Bearbeiten	Integration	Bearbeiten von Integrationsdetails
Planen	Alert	Planen von Aktionsalarmen
Planen	Bericht	Planen von Berichten und Abfragen

Mit folgenden Aktionen können Benutzer ein Objekt, das zur SafeObject-Ressourcenklasse gehört, anzeigen oder bearbeiten:

Aktion	Ressource	Beschreibung
Lesen	AppObject	Anzeigen von Berichtsvorlagen, Abfragevorlagen, Kennungen, geplanten Berichtsjobs, Alarmjobs, Service-Konfigurationen, Datenzuordnungsdateien, Nachrichtenanalysedateien (XMP-Dateien), Unterdrückungs- und Zusammenfassungsregeln sowie Ereignisweiterleitungsregeln
Lesen	Kalender	Anzeigen von Kalendern unter Verwaltung, Benutzer- und Zugriffsverwaltung, Kalender
Lesen	Ordner	Anzeigen von Ordnern unter Verwaltung, Benutzer- und Zugriffsverwaltung, EEM-Ordner

Aktion	Ressource	Beschreibung
Lesen	Globaler Benutzer	Anzeigen von Informationen zu Benutzern, die aufgelistet werden bei Abfrage nach Globale Benutzer unter Verwaltung, Benutzer- und Zugriffsverwaltung, Benutzer
Lesen	iPoz	Anzeigen von Einstellungen zum Benutzerspeicher unter Verwaltung, Benutzer- und Zugriffsverwaltung, Benutzerspeicher Anzeigen von Einstellungen zur Kennwortrichtlinie unter Verwaltung, Benutzer- und Zugriffsverwaltung, Kennwortrichtlinien
Lesen	Richtlinie	Anzeigen von Richtlinien unter Verwaltung, Benutzer- und Zugriffsverwaltung, Zugriffsrichtlinien
Lesen	Benutzer	Anzeigen von Benutzerdetails bei Abfrage nach Anwendungsbenutzerdetails unter Verwaltung, Benutzer- und Zugriffsverwaltung, Benutzer
Lesen	Benutzergruppe	Anzeigen der Anwendungsgruppenmitgliedschaft von Benutzern, die aufgelistet werden bei Abfrage nach Anwendungsbenutzerdetails unter Verwaltung, Benutzer- und Zugriffsverwaltung, Benutzer
Schreiben	AppObject	Bearbeiten oder Löschen von Berichtsvorlagen, Abfragevorlagen, Kennungen, geplanten Berichtsjobs, Alarmjobs, Service-Konfigurationen, Datenzuordnungsdateien, Nachrichtenanalysedateien (XMP-Dateien), Unterdrückungs- und Zusammenfassungsregeln und Ereignisweiterleitungsregeln
Schreiben	Kalender	Bearbeiten von benutzerdefinierten Kalendern
Schreiben	Ordner	Bearbeiten von benutzerdefinierten, zur EEM-Ordnerstruktur hinzugefügten Daten
Schreiben	Globaler Benutzer	Bearbeiten von globalen Benutzerdetails
Schreiben	iPoz	Konfigurieren von Benutzerspeichern und Kennwortrichtlinien
Schreiben	Richtlinie	Bearbeiten von benutzerdefinierten und vordefinierten Richtlinien
Schreiben	Benutzer	Bearbeiten von Anwendungsbenutzerdetails
Schreiben	Benutzergruppe	Erstellen, Bearbeiten oder Löschen einer Anwendungsbenutzergruppe

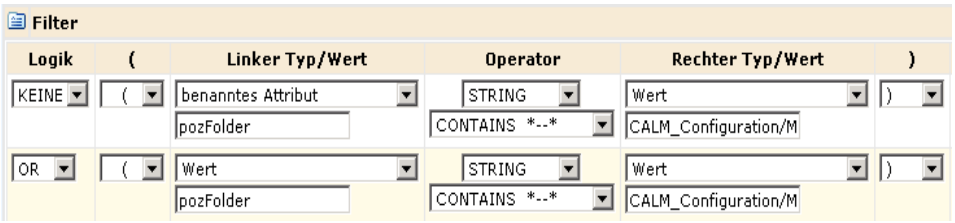
CALM-Ressourcen und EEM-Ordner

Bei jeder benutzerdefinierten CALM-Richtlinie unter Beteiligung von Ereignisweiterleitung, Ereignisgruppierung, Integration, Profil oder Bericht, die Sie von Grund auf erstellen, erstellen Sie eine Bereichsrichtlinie in "AppObject". Die Bereichsrichtlinie hat Lese- bzw. Schreibzugriff, mit dem die EEM-Pfade nach allen CALM-Ressourcen gefiltert werden, die in der entsprechenden CALM-Richtlinie aufgelistet sind. Als Identitäten für diese Richtlinie werden dieselben Benutzergruppen bzw. Identitäten wie bei der CALM-Richtlinie zugewiesen. Um das Richtlinienset zu vervollständigen, erstellen Sie eine weitere, schreibgeschützte Bereichsrichtlinie, ordnen ihr eine Identität zu, die die Ressource nur anzeigen kann, und geben einen Filter mit EEM-Ordnerpfad ein.

Hinweis: Ob eine CALM-Richtlinie eine sie unterstützende Bereichsrichtlinie erfordert, hängt von der Ressource ab, die die CALM-Richtlinie verwendet. Beispielsweise sind die Ressourcen Datenbank, Kennung und Alarm reine CALM-Ressourcen, für die keine Richtlinien zur Bereichsdefinierung erforderlich sind. Für agentenbezogene Ressourcen sind ebenfalls keine Richtlinien zur Bereichsdefinierung erforderlich.

Sie können EEM-Ordner anzeigen, indem Sie auf der Registerkarte "Verwaltung" auf die Unterregisterkarte "Benutzer- und Zugriffsverwaltung" klicken. Wenn Sie einen Ordner wie etwa "Unterdrückung" auswählen, wird der zugehörige Pfad angezeigt. Dies wird mit folgendem Beispiel verdeutlicht:

Sie geben den EEM-Verzeichnispfad als Wert in einem Ausdruck an, der mit "pozFolder CONTAINS" beginnt, siehe Bereich "Filter" in einer Richtliniendefinition. Beispiel:



In den folgenden Tabellen erhalten Sie Hinweise zum Filterwert einer Richtlinie zur Bereichsdefinierung, die sich auf eine CALM-Richtlinie bezieht, welche den Zugriff auf bestimmte CALM-Ressourcen gewährt oder verweigert.

Hinweis: Es gibt keine Eins-zu-Eins-Entsprechung zwischen CALM-Ressourcen und Ordnern.

Erstellen einer Richtlinie zur Bereichsdefinierung, die Zugriff auf den Inhalt nachstehender CALM-Ressource gewährt	**Fügen Sie einen Filter mit folgendem EEM-Verzeichnispfad hinzu**
Ereignisweiterleitung	pozFolder CONTAINS /CALM_Configuration/Content/Rules/Forwarding
Ereignisgruppierung	pozFolder CONTAINS /CALM_Configuration/Content/Rules/Summarization pozFolder CONTAINS /CALM_Configuration/Content/Rules/Suppression
Integration (Server)	pozFolder CONTAINS /CALM_Configuration/Content/Mapping pozFolder CONTAINS /CALM_Configuration/Content/Parsing
Profil	pozFolder CONTAINS /CALM_Configuration/Content/Profiles
Bericht	pozFolder CONTAINS /CALM_Configuration/Content/CEG pozFolder CONTAINS /CALM_Configuration/Content/Reports

Erstellen einer Richtlinie zur Bereichsdefinierung, die den Zugriff auf nachstehendes CALM-Modul erfordert	**Fügen Sie einen Filter mit folgendem EEM-Verzeichnispfad hinzu**
Agenten-Manager	pozFolder CONTAINS /CALM_Configuration/Modules/AgentManager

Erstellen einer Richtlinie zur Bereichsdefinierung, die den Zugriff auf nachstehendes CALM-Modul erfordert	Fügen Sie einen Filter mit folgendem EEM-Verzeichnispfad hinzu
Ereignisprotokollspeicher-	pozFolder CONTAINS /CALM_Configuration/Modules/logDepot
Berichtsserver	pozFolder CONTAINS /CALM_Configuration/Modules/calmReporter
Software-Update-Modul	pozFolder CONTAINS /CALM_Configuration/Modules/Subscription

Globale Ressourcen und CA EEM-Funktionalität

Sie können eine Richtlinie zur Bereichsdefinierung erstellen, die von der Zielsetzung her einer CALM-Richtlinie ähnelt, außer dass die Ressourcen global statt produktspezifisch sind. Globale Ressourcen sind Ressourcen, die über mehrere CA-Produkte hinweg verwendet werden. Sie können Richtlinien erstellen, die Zugriff auf bestimmte globale Ressourcen gewähren oder verweigern. Der Zugriff erfolgt bei allen Ressourcen über entsprechende Schaltflächen auf der Unterregisterkarte "Benutzer- und Zugriffsverwaltung" der Registerkarte "Verwaltung".

Nutzen Sie als Orientierungshilfe die folgende Tabelle, wenn Sie eine Richtlinie zur Bereichsdefinierung erstellen, die den angegebenen Identitäten die Möglichkeit gewährt oder verweigert, Lese- und Schreibaktionen durchzuführen, wenn die angegebene Ressource eine globale Ressource ist.

Aufgabe	Aktion	Globale Ressource
Anzeigen, Erstellen, Bearbeiten oder Löschen eines globalen Benutzers, einer globalen Benutzergruppe und einer Anwendungsbenutzergruppe (Rolle); Hinzufügen einer Anwendungsgruppe (Rolle) zu einem globalen Benutzer oder Erstellen eines globalen Benutzers mit einer Rolle	Lesen, Schreiben	Benutzer Benutzergruppe Globaler Benutzer Globale Benutzergruppe
Erstellen, Bearbeiten, Kopieren, Exportieren, Deaktivieren, Testen, Anzeigen oder Löschen einer Richtlinie; Hinzufügen eines Kalenders zu einer Richtlinie	Lesen, Schreiben	Richtlinie Kalender
Erstellen, Bearbeiten, Kopieren, Anzeigen oder Löschen eines Zugriffsfilters; Anzeigen von EEM-Ordnern	Lesen, Schreiben	Richtlinie

Aufgabe	Aktion	Globale Ressource
Erstellen eines Kalenders	Lesen, Schreiben	Kalender
Konfigurieren des Benutzerspeichers; Erstellen, Bearbeiten oder Anzeigen von Kennwortrichtlinien	Lesen, Schreiben	iPoz

Ziehen Sie zum Erstellen eines Filters für eine globale Ressource den Filter für die CALM-Anwendungszugriffsrichtlinie als Beispiel heran. Der Filter gibt u. a. die gegenseitige Zuordnung von Aktionen und Ressourcen an. Wenn Sie in einer vordefinierten Richtlinie auf "Bearbeiten" klicken, können Sie die Quelle überprüfen, um ein Beispiel für die Eingabe der Logik zu erhalten.

Planen von Benutzerrollen

Wenn die vordefinierten Anwendungsbenutzergruppen "Administrator", "Analyst" und "Auditor" für Ihre Bedürfnisse nicht ausreichen, können Sie benutzerdefinierte Rollen mit neuen Anwendungsbenutzergruppen erstellen. Beispiel: Um eine kleine Gruppe von Benutzern für die Verwaltung von Benutzerkonten zuzuweisen, wobei diese Benutzer keinen Zugriff auf nicht zugehörige Funktionen in CA Enterprise Log Manager haben, können Sie die Rolle "BenutzerKontoAdministrator" definieren, für diese Rolle eine Bereichsrichtlinie erstellen, diese Rolle der CALM-Richtlinie für den Zugriff auf die Anwendung hinzufügen und diese Rolle den Benutzern zuweisen, die Benutzerkonten verwalten sollen.

Die Benutzerplanung für CA Enterprise Log Manager besteht aus folgenden Schritten:

- Bestimmen der Anzahl der Benutzer, die CA Enterprise Log Manager verwalten, analysieren und überwachen sollen
- Ermitteln der Benutzer, um CA Enterprise Log Manager-Zugriff zu gewähren

Wenn Sie benutzerdefinierte Rollen mit zugehörigen Zugriffsrichtlinien erstellen möchten, sollten Sie das folgende Verfahren berücksichtigen:

- Ermitteln der Rolle, die den einzelnen CA Enterprise Log Manager-Benutzern zugewiesen werden soll
- Ermitteln der Art des Zugriffs auf CA Enterprise Log Manager-Ressourcen, der für die einzelnen Rollen erforderlich ist

Sie können auch die folgenden Alternativen für benutzerdefinierte Rollen (Anwendungsgruppen) berücksichtigen:

- Konfigurieren Sie Richtlinien zum Erstellen von dynamischen Benutzergruppen.
- Erstellen Sie globale Gruppen, und behandeln Sie sie wie Anwendungsgruppen. D. h., weisen Sie sie Benutzern und Richtlinien als Identitäten zu.

  Diese Vorgehensweise ist nützlich, wenn Richtlinien zum Einschränken des Zugriffs durch den geografischen Standort erstellt werden sollen, und Sie möchten, dass dieselben Benutzer dieselben Rechte für mehrere CA-Produkte haben. Eine globale Gruppe für "Standort-A_Admin" kann beispielsweise Benutzern zugewiesen werden, die mehrere CA-Produkte an Standort-A verwalten sollen. Richtlinien für die einzelnen CA-Produkte können erstellt werden, die denjenigen Servern Verwaltungsrechte gewähren, auf denen dieses Produkt an Standort-A installiert wurde.

Weitere Informationen:

Erstellen einer globalen Gruppe (siehe Seite 41)

Konfigurieren von benutzerdefinierten Benutzerrollen und Zugriffsrichtlinien

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.

Administratoren können Benutzerrollen und die entsprechenden Richtlinien wie folgt erstellen:

1. Führen Sie für jede von Benutzern von CA Enterprise Log Manager übernommene Rolle folgende Aufgaben durch:
   - Ermitteln Sie die Ressourcen, für die Zugriff gewährt werden muss.
   - Ermitteln Sie die Aktionen, die Sie auf den einzelnen Ressourcen zulassen möchten.
   - Ermitteln Sie die Identitäten oder Benutzer, auf die diese Rolle angewendet wird.

     Hinweis: Identitäten können andere Anwendungsgruppen sein, aus denen sich eine übergeordnete Gruppe zusammensetzt.
2. Wenn eine vordefinierte Anwendungsgruppe für Ihre Bedürfnisse zu breit angelegt ist, erstellen Sie eine neue Anwendungsgruppe und weisen Sie diese den angegebenen Benutzern zu. Es empfiehlt sich, einer benutzerdefinierten Anwendungsgruppe einen Namen zu geben, der die Rolle beschreibt, die die zugewiesenen Benutzer ausführen sollen.
3. Fügen Sie die neue Anwendungsgruppe der CALM-Richtlinie für den Zugriff auf die Anwendung hinzu, wobei die Richtlinie vom Typ "Zugriffskontrollliste" ist.

4. Wenn die neue Rolle auf einer oder mehreren Ressourcen Aktionen wie "Erstellen" durchführen muss, gehen Sie wie folgt vor:
   a. Konfigurieren Sie eine CALM-Richtlinie, die es der neuen Anwendungsgruppe ermöglicht, auf den angegebenen CA Enterprise Log Manager-Ressourcen die Aktion "Erstellen" oder andere gültige Aktionen durchzuführen.
   b. Konfigurieren Sie eine Bereichsrichtlinie, die der neuen Anwendungsgruppe Lese- und Schreibzugriff auf die Appobject-Ressource gewährt, und legen Sie einen Filter fest, der angibt, an welcher Stelle die angegebene Ressource in den EEM-Ordnern gespeichert wird. Geben Sie für jeden Filter das benannte Attribut "pozFolder" ein, das einen Wert enthält, der dem Pfad für den EEM-Ordner entspricht und mit "/CALM_Configuration" beginnt.
5. Wenn die neue Rolle nur eine bestimmte CA Enterprise Log Manager-Ressource anzeigen muss, konfigurieren Sie eine Bereichsrichtlinie, die den Lesezugriff auf "AppObject" ermöglicht, und legen Sie einen Filter mit dem benannten Attribut "pozFolder" fest, das einen Wert enthält, der dem Pfad für den EEM-Ordner entspricht, unter dem diese Ressource gespeichert ist, und mit "/CALM_Configuration" beginnt.
6. Testen Sie die Richtlinien.
7. Weisen Sie Benutzerkonten die neue Rolle zu.

Administratoren können eingeschränkten Benutzerzugriff auch mit Zugriffsfiltern erstellen. Wenn eine bestimmte Art von eingeschränktem Zugriff nur für einen Benutzer gilt, können Sie diesen Benutzer beim Zuweisen zu einer Anwendungsgruppe oder Rolle auslassen. So schränken Sie den Zugriff eines Benutzers ein:

1. Erstellen Sie einen Benutzer, weisen Sie jedoch keine Rolle zu.
2. Erteilen Sie dem Benutzer Zugriff auf die CA Enterprise Log Manager-Anwendung, indem Sie den Benutzer der CALM-Zugriffsrichtlinie hinzufügen.
3. Erstellen Sie eine Bereichsrichtlinie, die Lese- oder Schreibzugriff auf die Ressourcen "SicheresObjekt" und "AppObject" gewährt, und legen Sie einen Filter fest, bei dem das benannte Attribut "pozFolder" mit dem Wert des EEM-Ordners für die Ressource identisch ist. Wenn es sich bei der Ressource beispielsweise um Berichte handelt, legen Sie für das benannte Attribut "calmTag" den Wert einer Berichtskennung fest.
4. Erstellen Sie einen benutzerdefinierten Zugriffsfilter.

Administratoren können den Benutzerzugriff auf die CA Enterprise Log Manager-Ressourcen anpassen. Betrachten Sie die folgenden Beispiele:

- Erstellen Sie Rollen, um unterschiedlichen Gruppen von Administratoren bestimmte Verwaltungsaufgaben zuzuweisen. Erstellen Sie beispielsweise eine Rolle mit der Bezeichnung "BenutzerKontoAdministrator". Erstellen Sie eine Richtlinie, die Benutzern mit dieser Rolle Zugriff auf nur die Funktionalität gewährt, die zum Verwalten von Benutzern und Gruppen erforderlich ist. Eine Richtlinie dieser Art muss Lese- und Schreibzugriff auf die Ressource "GlobalerBenutzer" sowie auf die Ressourcen "Benutzer" und "BenutzerGruppe" gewähren.
- Erstellen Sie Rollen zum Verteilen von Analystenaufgaben auf die unterschiedlichen Arten von Berichten und Abfragen anhand von Kennungen. Erstellen Sie beispielsweise Rollen wie "SystemZugriffsanalyst" und "PCIAnalyst", und weisen Sie Analysten nur einer dieser eingeschränkten Analystenrollen zu. Erstellen Sie anschließend Richtlinien, die Zugriff auf eine Teilmenge dieser Ressourcen anhand von Kennungen gewähren. Erstellen Sie beispielsweise eine Richtlinie, die der Rolle "SystemZugriffsanalyst" Zugriff auf Berichte und Abfragen gewährt, die die Kennung "Systemzugriff" aufweisen, sowie eine weitere Richtlinie, die der Rolle "PCIAnalyst" Zugriff auf Berichte und Abfragen gewährt, die die Kennung "PCI" aufweisen. Erstellen Sie weitere Rollen und Richtlinien anhand anderer Kennungen. Richtlinien, die den Zugriff auf diese Weise einschränken, tun dies mit Hilfe von Zugriffsfiltern.

Administratoren können mit einem der folgenden Verfahren serverbasierte Richtlinien erstellen:

- Einschränken von Daten

  Sie können den Zugriff auf bestimmte Protokolle einschränken, indem Sie einen Datenzugriffsfilter erstellen, den Filter für das Feld "receiver_name" festlegen und einen Wert wie "systemstatus" oder "syslog" angeben.

- Einschränken der Konfiguration

  Sie können den Zugriff auf einen bestimmten CA Enterprise Log Manager-Server einschränken, indem Sie in der Ressourcenklasse "SicheresObjekt" eine Richtlinie erstellen, wobei "AppObject" als Ressource ausgewählt ist. Das bedeutet, dass Sie einen Filter wie den folgenden definieren müssen, um den Zugriff ausschließlich auf die Konfiguration des Berichtsservers auf einem bestimmten Host einzuschränken:

  ```
  pozFolder contains /CALM_Configuration/Modules/calmReporter/LogServer01
  ```

Weitere Informationen:

Beispielrichtlinien für benutzerdefinierte Integrationen (siehe Seite 148)
Beispielrichtlinien für Unterdrückungs- und Zusammenfassungsregeln (siehe Seite 150)
Erstellen eines Zugriffsfilters (siehe Seite 113)
Beschränken des Datenzugriffs für einen Benutzer: Windows-Administrator (siehe Seite 127)
Beschränken des Zugriffs für eine Rolle: PCI-Analyst (siehe Seite 141)

Erstellen einer Anwendungsbenutzergruppe (Rolle)

Sie können eine neue Anwendungsbenutzergruppe erstellen, um die Rollen zu unterstützen, die Sie benötigen. Nachdem sie eine neue Anwendungsbenutzergruppe erstellt haben, müssen Sie Zugriffsrichtlinien für diese Gruppe erstellen.

Wenn eine neue Gruppe Mitglied vorhandener Gruppen wird, müssen für diese Gruppe keine neuen Zugriffsrichtlinien erstellt werden. Stellen Sie sich folgendes Szenario vor: Sie benötigen für Benutzer, die Datenzuordnungs- und Nachrichtenanalysedateien erstellen sollen, eine Rolle, für Benutzer, die Unterdrückungs- und Zusammenfassungsregeln erstellen, eine weitere Rolle und eine dritte Rolle für Benutzer, die beide Aufgaben ausführen können. Sie können eine Anwendungsbenutzergruppe mit dem Namen "AdminDMMP" und einer Richtlinie, die Erstellungsrechte für die Ressource "Integration" gewährt, und eine andere Gruppe mit dem Namen "AdminSS" und der Richtlinie, die Erstellungsrechte für die Ressource "EventGrouping" gewährt, erstellen. Anschließend können Sie eine dritte Gruppe mit dem Namen "AdminDMMPSS" erstellen, die Mitglied der Gruppen "AdminDMMP" und "AdminSS" ist. Diese dritte Gruppe übernimmt automatisch die Richtlinien der beiden Mitgliedsgruppen.

Statt neue Anwendungsgruppen oder Rollen zu erstellen, können Sie die Rollen der vordefinierten Rollen "Analyst" und "Auditor" erweitern. Wenn Sie beispielsweise möchten, dass Analysten Unterdrückungs- und Zusammenfassungsregeln erstellen und Auditoren diese Regeln anzeigen können, können Sie eine CALM-Richtlinie, die das Recht zum Erstellen von Unterdrückungs- und Zusammenfassungsregeln gewährt, und eine Bereichsrichtlinie, die das Recht zum Anzeigen oder Bearbeiten von benutzerdefinierten Regeln gewährt, erstellen und der Rolle "Analyst" diese Richtlinien zuweisen. Anschließend können Sie eine Bereichsrichtlinie erstellen, die Benutzern das Recht zum Anzeigen von Unterdrückungs- und Zusammenfassungsregeln gewährt, und dieser Richtlinie die Gruppe "Auditor" zuweisen.

Nur Administratoren können neue Rollen erstellen.

So erstellen Sie eine neue Anwendungsbenutzergruppe (Rolle):

1. Klicken Sie auf die Registerkarte "Verwaltung" und auf die Unterregisterkarte "Benutzer- und Zugriffsverwaltung".
2. Klicken Sie auf "Gruppen".
3. Klicken Sie in der Liste "Benutzergruppen" links neben dem Ordner "Anwendungsgruppen" auf die Schaltfläche "Neue Anwendungsgruppe".
4. Geben Sie den Gruppennamen und eine Beschreibung ein.
5. Wenn diese neue Gruppe Zugriff haben soll, den Sie bereits für mindestens zwei benutzerdefinierte Anwendungsgruppen definiert haben, wählen Sie diese Anwendungsgruppen für die Mitgliedschaft aus. Andernfalls wählen Sie nichts aus.

   Hinweis: Wenn sich diese Gruppe aus vorhandenen Gruppen zusammensetzt, gelten für diese Gruppe die vorhandenen Richtlinien der einzelnen Gruppen. Es werden keine zusätzlichen Richtlinien benötigt.
6. Klicken Sie auf "Speichern".
7. Klicken Sie auf "Schließen".

Weitere Informationen:

Schritt 2: Erstellen der Rolle "PCI-Analyst" (siehe Seite 144)
Beispielrichtlinien für Unterdrückungs- und Zusammenfassungsregeln (siehe Seite 150)

Gewähren des Zugriffs auf CA Enterprise Log Manager für eine benutzerdefinierte Rolle

Beim Erstellen einer Anwendungsbenutzergruppe oder Rolle müssen Sie sicherstellen, dass Sie sie der vordefinierten CALM-Richtlinie für den Zugriff auf die Anwendung hinzufügen. Nur Identitäten, die dieser Richtlinie explizit hinzugefügt werden, haben Zugriff auf CA Enterprise Log Manager. Identitäten können einzelne Benutzer oder Mitglieder einer Benutzergruppe sein.

Falls die Situation auftritt, dass sich Benutzer, die einer neuen Benutzergruppe zugewiesen wurden, bei CA Enterprise Log Manager nicht anmelden können, überprüfen Sie, ob die Identitäten der CALM-Richtlinie für den Zugriff auf die Anwendung diese Gruppe enthalten.

So gewähren Sie einer benutzerdefinierten Anwendungsbenutzergruppe Zugriff auf CA Enterprise Log Manager:

1. Klicken Sie auf der Registerkarte "Verwaltung" auf "Benutzer- und Zugriffsverwaltung" und anschließend im linken Fenster auf "Zugriffsrichtlinien".
2. Klicken Sie auf "Bereichsrichtlinien", und wählen Sie "CALM-Anwendungszugriff" aus.
3. Suchen Sie unter "Identitäten" nach der neuen Anwendungsgruppe. Gehen Sie hierzu wie folgt vor:
   a. Wählen Sie als Typ "Anwendungsgruppe" aus.
   b. Klicken Sie auf "Identitäten suchen".
   c. Übernehmen Sie "Name" als Attribut und "LIKE" als Operator. Klicken Sie auf "Suchen".

      Der Name der neuen Anwendungsbenutzergruppe wird in der angezeigten Liste mit Identitäten angezeigt.
   d. Wählen Sie den Namen der neuen Anwendungsgruppe aus, und klicken Sie auf die Schaltfläche "Verschieben", um den Gruppennamen in das Feld "Ausgewählte Identitäten" zu verschieben.
4. Klicken Sie auf "Speichern".

Hinzufügen einer Identität zu einer vorhandenen Richtlinie

Beim Erstellen einer neuen Anwendungsbenutzergruppe können Sie die neue Gruppe ggf. zu vorhandenen Richtlinien hinzufügen. Wenn Sie einen Benutzer erstellen, der keine Rolle, aber mit einem Zugriffsfilter eingeschränkten Zugriff hat, können Sie diesen Benutzer zu vorhandenen Richtlinien hinzufügen.

Wichtig! Bei der Arbeit mit installierten Zugriffsrichtlinien müssen Sie besonders darauf achten, dass Sie diese nicht löschen, da diese Zugriffsrichtlinien weder gesperrt noch geschützt sind.

Wenn eine vordefinierte Zugriffsrichtlinie versehentlich gelöscht wird, können Benutzer erst wieder auf den CA Enterprise Log Manager-Server zugreifen, nachdem diese Richtlinie wiederhergestellt wurde. Sie können mit dem Hilfsprogramm "safex" Richtlinien wiederherstellen.

So fügen Sie eine Identität zu einer vorhandenen Richtlinie hinzu:

1. Klicken Sie auf der Registerkarte "Verwaltung" auf "Benutzer- und Zugriffsverwaltung" und anschließend im linken Fenster auf "Zugriffsrichtlinien".
2. Klicken Sie auf den Richtlinientyp, und wählen Sie die Richtlinie aus, die auf die neue Anwendungsbenutzergruppe angewendet wird. Zeigen Sie das Fenster "Identitäten" an.
3. Wählen Sie als Typ "Anwendungsgruppe" aus.
4. Klicken Sie auf "Identitäten suchen".
5. Übernehmen Sie "Name" als Attribut und "LIKE" als Operator. Klicken Sie auf "Suchen".

   Der Name der neuen Anwendungsbenutzergruppe wird in der angezeigten Liste mit Identitäten angezeigt.
6. Wählen Sie den Namen der neuen Anwendungsgruppe aus, und klicken Sie auf die Schaltfläche "Verschieben", um den Gruppennamen in das Feld "Ausgewählte Identitäten" zu verschieben.
7. Klicken Sie auf "Speichern".

Weitere Informationen:

Schritt 4: Hinzufügen des Benutzers "PCI-Analyst" zu vorhandenen Richtlinien (siehe Seite 145)

Erstellen einer CALM-Zugriffsrichtlinie

Sie können eine CALM-Richtlinie erstellen, um eine oder mehrere gültige Aktionen in einer oder mehreren CALM-Klassen zu ermöglichen oder zu verweigern.

Die folgenden CALM-Ressourcen sind anwendungsspezifisch, d. h. sie werden nur von folgendem CA Enterprise Log Manager-Produkt verwendet:

- Alarm
- Agentenkonfiguration
- Authentifizierungsschlüssel des Agenten
- ALLE_GRUPPEN
- Connector
- Daten
- Datenbank
- Ereignisgruppierung
- Integration
- Profil
- Bericht
- Kennung

So erstellen Sie eine neue CALM-Richtlinie von Grund auf:

1. Klicken Sie auf die Registerkarte "Verwaltung" und auf die Unterregisterkarte "Benutzer- und Zugriffsverwaltung".
2. Klicken Sie auf "Zugriffsrichtlinien".
3. Klicken Sie auf die Schaltfläche "Neue Zugriffsrichtlinie" links vom CALM-Ordner.
4. Geben Sie für die Richtlinie einen aussagefähigen Namen und wahlweise eine kurze Beschreibung ein.
5. Soll diese Richtlinie zeitlich begrenzt sein, wählen Sie im Kalender einen entsprechenden Zeitraum aus.
6. Übernehmen Sie CALM als Namen für die Ressourcenklasse.

7. Wählen Sie anhand folgender Kriterien im Fenster "Allgemein" den Typ aus:
   - Wählen Sie "Zugriffsrichtlinie" aus, um allen ausgewählten Identitäten die Berechtigung zu erteilen oder zu verweigern, sämtliche ausgewählten Aktionen bei allen für sie geltenden Ressourcen auszuführen.
   - Wählen Sie "Zugriffssteuerungsliste" aus, um allen ausgewählten Identitäten die Berechtigung zu erteilen oder zu verweigern, nur die ausgewählten Aktionen auf einer ausgewählten Ressource auszuführen.

     Hinweis: Es ist nicht möglich, Filter für mehrere Ressourcen zu speichern. Als Behelfslösung können separate Richtlinien erstellt werden, d. h. für jede Ressourcen/Filter-Kombination eine Richtlinie.
   - Wählen Sie "Zugriffssteuerungsliste für Identitäten" aus, um jeder ausgewählten Identität die Berechtigung zu erteilen oder zu verweigern, ausgewählte Aktionen in allen ausgewählten Ressourcen auszuführen, auf die sie zutreffen.
8. Wählen Sie im Bereich "Identitäten" wie folgt die Benutzer oder Gruppen aus, für die diese Richtlinie gilt:
   a. Wählen Sie unter "Typ" die Option "Anwendungsgruppe" oder eine der anderen Optionen aus. Klicken Sie auf "Identitäten suchen" und anschließend auf "Suchen".
   b. Wählen Sie aus den vorgegebenen Identitäten aus, und klicken Sie auf die Schaltfläche "Verschieben", um sie in das Feld "Ausgewählte Identitäten" zu verschieben.
9. Führen Sie bei einer Richtlinie des Typs "Zugriffsrichtlinie" die Zugriffsrichtlinienkonfiguration wie folgt durch:
   a. Geben Sie eine CALM-Ressource in das Feld "Ressource hinzufügen" ein, und klicken Sie auf "Hinzufügen".
   b. Wählen Sie die Aktionen aus, bei denen die ausgewählten Identitäten in der Lage sein müssen, sie in allen ausgewählten Ressourcen auszuführen. Folgende Aktionen sind hierbei zulässig: Anmerken, Erstellen, Datenzugriff, Bearbeiten und Planen. Es ist nicht möglich, das Recht zur Ausführung einer bestimmten Aktion für eine Ressource zu erteilen, jedoch nicht für eine andere Ressource, obwohl die Aktion für Letztere zulässig ist.

10. Führen Sie bei einer Richtlinie des Typs "Zugriffssteuerungsliste" die Konfiguration der Zugriffssteuerungsliste wie folgt durch:
    a. Geben Sie eine CALM-Ressource in das Feld "Ressource hinzufügen" ein, und klicken Sie auf "Hinzufügen".
    b. Wählen Sie die Aktionen aus, bei denen die ausgewählten Identitäten in der Lage sein müssen, sie in dieser Ressource auszuführen. Hierbei sind eine oder mehrere der folgenden Aktionen zulässig: Anmerken, Erstellen, Datenzugriff, Bearbeiten und Planen.
    c. Wiederholen Sie die letzten zwei Schritte für jede Ressource, auf die sich diese Richtlinie beziehen soll.

       Mit diesem Ressourcentyp haben Sie die Möglichkeit, das Recht zur Ausführung einer Aktion wie "Erstellen" nur für eine bestimmte Ressource, aber nicht für eine andere Ressource zu erteilen.
11. Führen Sie bei einer Richtlinie des Typs "Zugriffssteuerungsliste für Identitäten" die Konfiguration der Zugriffssteuerungsliste für Identitäten wie folgt durch:
    a. Wählen Sie für jede ausgewählte Identität alle Aktionen aus, die in allen Ressourcen, für die sie jeweils zulässig sind, gewährt oder verweigert werden sollen.
    b. Geben Sie für jede hinzuzufügende Ressource eine CALM-Ressource in das Feld "Ressource hinzufügen" ein, und klicken Sie auf "Hinzufügen":
12. Überprüfen Sie oben die Kontrollkästchen, und markieren Sie alle Zutreffenden.
    - Wählen Sie "Ausdrücklich verweigern", um eine zugriffgewährende Richtlinie in eine Richtlinie umzuwandeln, die den Zugriff verweigert.
    - Wählen Sie "Deaktiviert", um diese Richtlinie, falls Sie neu ist, vorübergehend zu inaktivieren.
    - Wählen Sie "Vorbereitstellung" und anschließend "Bezeichnungen zuweisen", und fügen Sie die Bezeichnungen hinzu, wenn Sie diese Richtlinie zu Testzwecken verwenden und die Richtlinien mit Hilfe von benutzerdefinierten Bezeichnungen kategorisieren möchten.
13. Klicken Sie auf "Speichern" und dann im linken Fensterbereich auf "Schließen".

Erstellen von Richtlinien zur Bereichsdefinierung

Sie können Richtlinien zur Bereichsdefinierung in jeder globalen Ressource erstellen. Die Aktionen in Richtlinien zur Bereichsdefinierung sind auf Lesen und Schreiben beschränkt.

- Folgende globale Ressourcen werden von vielen CA-Produkten (Anwendungen) verwendet:
  - Kalender
  - Globaler Benutzer
  - Globale Benutzergruppe
  - iPoz
  - Richtlinie
  - Benutzer
  - Benutzergruppe
  - AppObject
- Mit der globalen Ressource "AppObject" können Sie Richtlinien zur Bereichsdefinierung in anwendungsspezifischen Ressourcen und Modulen erstellen. Hierzu können Sie einen Filter hinzufügen, der den relevanten EEM-Ordner festlegt und angibt, wo der anwendungsspezifische Inhalt oder das Module gespeichert wird.
  - EEM-Inhaltsordner, die Sie mit der Ressource "AppObject" in Filtern verwenden können, umfassen folgende:
    - Ereignisgruppierung
    - Integration (Server)
    - Profil
    - Bericht
  - CA Enterprise Log Manager-Modulordner, die Sie mit der "AppObject"-Ressource in Filtern verwenden können, umfassen folgende:
    - Ereignisprotokollspeicher-
    - Berichtsserver
    - Automatisches Software-Update

Sollte keine Richtlinie vorhanden sein, deren Einstellungen Sie übernehmen können, haben Sie die Möglichkeit, eine Richtlinie von Grund auf neu zu erstellen. Wenn Sie eine Richtlinie zur Bereichsdefinierung erstellen, die mit einer von Ihnen erstellten CALM-Richtlinie verknüpft ist, geben Sie dieselben Identitäten an wie bei der zugehörigen CALM-Richtlinie.

Nur Administratoren können Zugriffsrichtlinien erstellen, bearbeiten, löschen und anzeigen.

So erstellen Sie eine neue CALM-Richtlinie mit expliziter Erteilung:

1. Klicken Sie auf die Registerkarte "Verwaltung" und auf die Unterregisterkarte "Benutzer- und Zugriffsverwaltung".
2. Klicken Sie auf "Zugriffsrichtlinien".
3. Klicken Sie links neben dem Ordner "Richtlinien zur Bereichsdefinierung" auf die Schaltfläche "Neue Richtlinie zur Bereichsdefinierung".
4. Vergeben Sie einen aussagefähigen Namen für die Richtlinie. Verwenden Sie hierzu beispielsweise die Rolle bzw. Rollen, für die die Richtlinie gilt, und den Aufgabenbereich. Sehen Sie sich als Referenzbeispiel die Namen der vordefinierten Richtlinien an.
5. Geben Sie eine kurze Beschreibung ein, um die nähere Bedeutung des Namens zu erläutern.
6. Normalerweise wird SafeObject als Name für die Ressourcenklasse akzeptiert.
7. Wählen Sie anhand folgender Kriterien im Fenster "Allgemein" den Typ aus:
   - Wählen Sie "Zugriffsrichtlinie" aus, um allen ausgewählten Identitäten die Fähigkeit zu gewähren oder zu verweigern, sämtliche ausgewählte Aktionen bei allen auf sie zutreffenden Ressourcen auszuführen.
   - Wählen Sie "Zugriffssteuerungsliste" aus, um allen ausgewählten Identitäten die Fähigkeit zu gewähren oder zu verweigern, nur die ausgewählten Aktionen auf einer ausgewählten Ressource auszuführen.

     Hinweis: Es ist nicht möglich, Filter für mehrere Ressourcen zu speichern. Als Behelfslösung können separate Richtlinien erstellt werden, d. h. für jede Ressource/Filter-Kombination eine Richtlinie.
   - Wählen Sie "Zugriffssteuerungsliste für Identitäten" aus, um jeder ausgewählten Identität die Fähigkeit zu gewähren oder zu verweigern, ausgewählte Aktionen auf allen ausgewählten Ressourcen auszuführen, die auf sie zutreffen.

8. Wählen Sie im Falle einer Richtlinie des Typs "Zugriffsrichtlinie" oder "Zugriffssteuerungsliste" im Bereich "Identitäten" die Benutzer oder Gruppen aus, für die diese Richtlinie gilt.
   a. Wählen Sie unter "Typ" die Option "Anwendungsgruppe" aus. Klicken Sie auf "Identitäten suchen" und anschließend auf "Suchen".
   b. Wählen Sie aus den vorgegebenen Identitäten aus, und klicken Sie auf die Schaltfläche "Verschieben", um sie in das Feld "Ausgewählte Identitäten" zu verschieben.

9. Bei einer Richtlinie des Typs "Zugriffsrichtlinie" sind standardmäßig alle Aktionen für alle Ressourcen ausgewählt. Führen Sie die Zugriffsrichtlinienkonfiguration wie folgt durch, um dies individuell anzupassen:

   a. Wählen Sie aus der Dropdown-Liste "Ressource hinzufügen" eine Ressource aus, und klicken Sie auf "Hinzufügen".

      - Wählen Sie "AppObject" aus, wenn es sich bei den Ressourcen, für die ein Lese- oder Schreibzugriff konfiguriert werden soll, um CA Enterprise Log Manager-spezifische Ressourcen handelt.
      - Wählen Sie "Benutzer" und "Globaler Benutzer" aus, um auf der Unterregisterkarte "Benutzer- und Zugriffsverwaltung" der Registerkarte "Verwaltung" den Zugriff auf die Schaltfläche "Benutzer" zu ermöglichen.
      - Wählen Sie "Benutzergruppe" und "Globale Benutzergruppe" aus, um auf der Unterregisterkarte "Benutzer- und Zugriffsverwaltung" der Registerkarte "Verwaltung" den Zugriff auf die Schaltfläche "Gruppen" zu ermöglichen.
      - Wählen Sie "Richtlinie" aus, um auf der Unterregisterkarte "Benutzer- und Zugriffsverwaltung" der Registerkarte "Verwaltung" den Zugriff auf die Schaltflächen "Zugriffsrichtlinien", "EEM-Ordner" und "Testrichtlinien" zu ermöglichen.
      - Wählen Sie "Kalender" aus, um auf der Unterregisterkarte "Benutzer- und Zugriffsverwaltung" der Registerkarte "Verwaltung" den Zugriff auf die Schaltfläche "Kalender" zu ermöglichen.
      - Wählen Sie "iPoz" aus, um auf der Unterregisterkarte "Benutzer- und Zugriffsverwaltung" der Registerkarte "Verwaltung" den Zugriff auf die Schaltflächen "Kennwortrichtlinie" und "Benutzerspeicher" zu ermöglichen.

   b. Wählen Sie "Lesen", um den Anzeigezugriff zu gewähren/zu verweigern. Wählen Sie "Schreiben", um den Bearbeitungszugriff zu gewähren/zu verweigern. Wenn Sie keine der Optionen auswählen, werden alle Aktionen aktiviert.

      Hinweis: Um einen Erstellzugriff zu gewähren/zu verweigern, müssen Sie eine CALM-Zugriffsrichtlinie definieren und CA Enterprise Log Manager-Ressourcen individuell auswählen.

   c. Fügen Sie bei Bedarf einen generischen Filter hinzu, der für die ausgewählten Ressourcen gilt.

10. Führen Sie bei einer Richtlinie des Typs "Zugriffssteuerungsliste" die Konfiguration der Zugriffssteuerungsliste wie folgt durch:
    a. Wählen Sie aus der Dropdown-Liste "Ressource hinzufügen" eine Ressource aus, und klicken Sie auf die Schaltfläche "Hinzufügen (+)".
    b. Wählen Sie bei "Aktionen" die Option "Lesen" bzw. "Schreiben" oder beide Optionen aus.
    c. Klicken Sie auf die Schaltfläche "Filter bearbeiten", um das Filterformular zu öffnen. Erstellen Sie einen Filter für die zugehörige Ressource, indem Sie unter "Links", "Operator" und "Rechts" jeweils einen Typ auswählen oder einen Wert eingeben.
    d. Wenn der Filter einen Ressourcennamen als Wert enthält, markieren Sie das Kontrollkästchen mit der Bezeichnung "Ressourcennamen als reguläre Ausdrücke behandeln". Ansonsten können Sie das Kontrollkästchen leer lassen.

    Wichtig! Definieren Sie eine Richtlinie für jede Ressource/Filter-Kombination.

11. Führen Sie bei einer Richtlinie des Typs "Zugriffssteuerungsliste für Identitäten" die Konfiguration der Zugriffssteuerungsliste für Identitäten wie folgt durch:
    a. Wählen Sie unter "Typ" eine der angegebenen Optionen aus. Wählen Sie zum Beispiel "Anwendungsgruppe" aus. Klicken Sie auf die Verknüpfung "Identitäten suchen", und klicken Sie auf die Schaltfläche "Suchen", um die Mitglieder des von Ihnen ausgewählten Typs anzuzeigen.
    b. Wählen Sie die Identitäten aus, und klicken Sie auf die Schaltfläche "Verschieben", um das Fenster "Ausgewählte Identitäten" auszufüllen.
    c. Legen Sie für jede ausgewählte Identität die Aktionen "Lesen" oder "Schreiben" fest, oder wählen Sie beide Aktionen aus.

       Die identitätsspezifischen Aktionen gelten für alle ausgewählten Ressourcen. Das heißt, eine bestimmte Identität kann alle ausgewählten Ressourcen entweder anzeigen, anzeigen und bearbeiten oder nur bearbeiten.
    d. Fügen Sie die Ressourcen hinzu, auf denen die Ausführung der identitätsspezifischen Aktionen gewährt oder verweigert werden soll.

12. Überprüfen Sie die Kontrollkästchen, und markieren Sie alle Zutreffenden.
    - Wählen Sie "Ausdrücklich verweigern", um eine zugriffgewährende Richtlinie in eine Richtlinie umzuwandeln, die den Zugriff verweigert.
    - Wählen Sie "Deaktiviert", um diese Richtlinie, falls neu, vorübergehend zu inaktivieren.
    - Wählen Sie "Vorbereitstellung" und anschließend "Bezeichnungen zuweisen" aus, und fügen Sie die Bezeichnungen hinzu, wenn Sie diese Richtlinie zu Testzwecken verwenden und die Richtlinien mit Hilfe von benutzerdefinierten Bezeichnungen kategorisieren möchten.
13. Klicken Sie auf "Speichern" und anschließend auf "Schließen" im linken Fensterbereich.

Weitere Informationen

Schritt 3: Erstellen einer Systemzugriffsrichtlinie für Windows-Administratoren (siehe Seite 131)

Erstellen einer Richtlinie auf der Grundlage einer vorhandenen Richtlinie

Sie können eine neue Zugriffsrichtlinie erstellen, indem Sie eine vorhandene Zugriffsrichtlinie kopieren und die Kopie ändern. Mit diesem Verfahren sparen Sie sich die Zeit, die erforderlich ist, die Angaben einer vorhandenen Richtlinie zu kopieren, die nur geringfügig geändert werden muss, um Ihren aktuellen Anforderungen zu entsprechen.

Nur Administratoren können Zugriffsrichtlinien erstellen, bearbeiten, löschen oder anzeigen.

So erstellen Sie eine Richtlinie auf der Grundlage einer vorhandenen Richtlinie:

1. Klicken Sie auf die Registerkarte "Verwaltung" und auf die Unterregisterkarte "Benutzer- und Zugriffsverwaltung".
2. Klicken Sie auf "Zugriffsrichtlinien".
3. Wählen Sie CALM- oder Bereichsrichtlinien aus, je nachdem, welchen Richtlinientyp Sie als Vorlage verwenden möchten.
4. Klicken Sie auf den Namenslink, um die zu kopierende Richtlinie zu öffnen.
5. Klicken Sie auf "Speichern unter".

   Das Explorer-Dialogfeld mit der Benutzereingabe wird angezeigt.

6. Geben Sie den Namen der neuen Richtlinie ein, die auf der geöffneten Richtlinie basieren soll, und klicken Sie auf "OK".
7. Nehmen Sie die erforderlichen Änderungen vor.

   Ersetzen Sie beispielsweise die kopierte Identität mit dem Namen der Rolle (benutzerdefinierte Anwendungsgruppe), auf die diese Richtlinie angewendet wird. Ändern Sie ggf. die auf den kopierten Ressourcen zulässigen Aktionen. Klicken Sie ggf. auf "Filter", und geben Sie einen weiteren Filter für die neue Rolle an.
8. Klicken Sie auf "Speichern" und anschließend auf "Schließen".
9. Überprüfen Sie die neue Richtliniendefinition.
   a. Wählen Sie den Richtlinientyp erneut aus, um alle Richtlinien anzuzeigen.
   b. Vergleichen Sie die neue Richtlinie mit der ursprünglichen Richtlinie, und überprüfen Sie, ob alle geplanten Änderungen in der neuen Richtlinie berücksichtigt sind.
   c. Klicken Sie auf "Schließen".
10. Testen Sie die Richtlinie.

Weitere Informationen:

Schritt 5: Erstellen einer Richtlinie auf der Basis der Richtlinie zum Anzeigen und Bearbeiten von Berichten durch Analysten (siehe Seite 145)

Testen von neuen Richtlinien

Sie haben die Möglichkeit, mit Hilfe der Funktion "Testrichtlinien" zu testen, ob eine neue Richtlinie syntaktisch korrekt ist. Mit der Funktion "Testrichtlinien" können Sie anhand der von Ihnen definierten Zugriffsrichtlinien Ad-hoc-Abfragen ausführen. Sie können eine Berechtigung als Abfrage des folgenden Typs betrachten: "Kann {Identität} die {Aktion} für die Ressource mit dem Typ {Ressourcenklasse} und dem Namen {Ressource} [mit folgenden {Attributen}] [zum {angegebenen Zeitpunkt}] ausführen?" Das Ergebnis ALLOW bedeutet, dass die von Ihnen eingegebene Identität die angegebene Aktion für die angegebene Ressource mit den angegebenen Attributen zur angegebenen Zeit ausführen darf.

Bevor Sie beginnen, sollten Sie die Richtlinie bereithalten:

So testen Sie eine Richtlinie:

1. Klicken Sie auf die Registerkarte "Verwaltung" und auf die Unterregisterkarte "Benutzer- und Zugriffsverwaltung".
2. Klicken Sie auf "Testrichtlinien".

   Die Seite "Berechtigungsprüfungsparameter" wird angezeigt.
3. Wenn Sie für die Richtlinie, die Sie prüfen möchten, die Option "Vorbereitstellung" ausgewählt und Bezeichnungen hinzugefügt haben, aktivieren Sie das Kontrollkästchen, das angibt, dass Sie Vorbereitstellungsrichtlinien einschließen und die zugehörigen Bezeichnungen hinzufügen möchten.
4. Füllen Sie die Eingabefelder aus. Falls die Richtlinie Filter umfasst, geben Sie die Filter in der Reihenfolge an, in der sie in der Richtlinie angezeigt werden.
5. Klicken Sie auf "Berechtigungsprüfung ausführen".
6. Überprüfen Sie das Ergebnis, und fahren Sie auf eine der folgenden Arten fort:
   - Falls das Ergebnis ALLOW lautet, melden Sie sich bei CA Enterprise Log Manager als Benutzer an, der in dieser neuen Richtlinie als Identität angegeben ist. Testen Sie die Effizienz, den Gültigkeitsbereich und den Umfang der Richtlinie, bevor Sie sie in der Produktionsumgebung einsetzen.
   - Lautet das Ergebnis DENY, überprüfen Sie Ihre Einträge in der Abfrage. Wenn sie korrekt sind, kehren Sie zur Richtlinie zurück, und/oder nehmen Sie dort die erforderlichen Korrekturen vor.

Erstellen einer Richtlinie für dynamische Benutzergruppen

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.

Sie können eine dynamische Gruppe erstellen, die sich aus Benutzern, Anwendungsgruppen, globalen Gruppen oder dynamischen Gruppen zusammensetzt. So können Sie beispielsweise eine dynamische Gruppe aus globalen Gruppen oder Anwendungsgruppen auf der Grundlage von Name, Beschreibung oder Gruppenmitgliedschaft erstellen. Oder Sie können eine dynamische Gruppe aus Benutzern mit unterschiedlichen Rollen auf der Grundlage eines gemeinsamen Attributs im globalen Benutzerprofil erstellen. Beispiel:

- Berufsbezeichnung
- Abteilung oder Büro
- Stadt, Staat oder Land

Nur Administratoren können Richtlinien für dynamische Benutzergruppen erstellen.

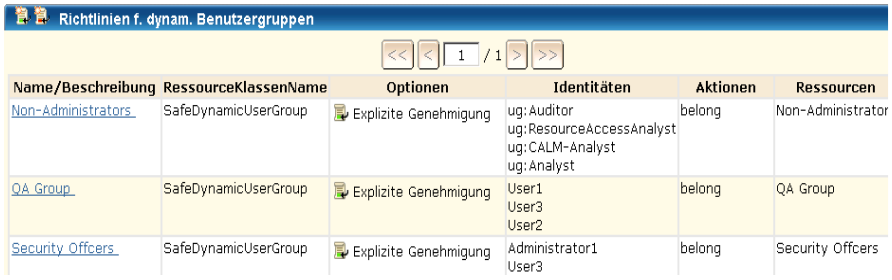
So erstellen Sie eine Richtlinie für dynamische Benutzergruppen:

1. Klicken Sie auf die Registerkarte "Verwaltung" und auf die Unterregisterkarte "Benutzer- und Zugriffsverwaltung".
2. Klicken Sie auf "Zugriffsrichtlinien".
3. Klicken Sie auf "Neue Richtlinie für dynamische Gruppe".

   Die Seite "Neue Richtlinie für dynamische Gruppe" wird angezeigt.
4. Geben Sie unter "Name" einen Gruppennamen ein, der angibt, wes diese Gruppe von Benutzern gemeinsam hat. Optional können Sie eine Beschreibung eingeben.
5. Wählen Sie einen Richtlinientyp aus. Die Standardeinstellung ist "Zugriffsrichtlinie".

6. Wählen Sie Identitäten wie folgt aus:
   a. Wählen Sie für "Typ" "Benutzer", "Anwendungsgruppe", "Globale Gruppe" oder "Dynamische Gruppe" aus, und klicken Sie auf "Identitäten suchen".
   b. Geben Sie für "Attribut", "Operator" und "Wert" den Ausdruck ein, mit dem die Kriterien für die Mitgliedschaft in dieser Gruppe festgelegt wird, und klicken Sie auf "Suchen".

      Wenn Sie beispielsweise "Benutzer" ausgewählt haben, können Sie "Berufsbezeichnung Wie Manager" eingeben und auf "Suchen" klicken, um alle Benutzer mit der Berufsbezeichnung "Manager" zu suchen.
   c. Wählen Sie aus den angezeigten Identitäten diejenigen aus, die Mitglied dieser dynamischen Gruppe werden sollen, und klicken Sie auf den Pfeil "Verschieben", um Ihre Auswahl in das Feld "Ausgewählte Identitäten" zu verschieben.
7. Wählen Sie unter "Aktionen" den Operator "belong" aus.
8. Geben Sie in das Feld "Ressource hinzufügen" den Wert ein, den Sie in das Feld "Name" eingegeben haben, und klicken Sie auf die Schaltfläche "Hinzufügen". Damit wird angegeben, dass die ausgewählten Identitäten zu der dynamischen Gruppenressource gehören, die Sie eben erstellt haben.
9. Optional können Sie weitere Filter hinzufügen.
10. Klicken Sie auf "Speichern".
11. Klicken Sie auf den Link für die Richtlinien für dynamische Benutzergruppen, und überprüfen Sie die neue dynamische Benutzergruppe, die Sie erstellt haben. Beispiel:



Erstellen eines Zugriffsfilters

Sie können einen Zugriffsfilter erstellen, um den Zugriff auf Protokolldaten zu beschränken, die den Filterkriterien entsprechen. Standardmäßig haben alle CA Enterprise Log Manager-Anwendungsbenutzer Abfragezugriff auf Ereignisprotokolldaten, die in den Ereignisprotokollspeichern des aktiven CA Enterprise Log Manager-Servers, von gleichgeordneten Servern in einem Netzverbund oder von untergeordneten Servern in einem hierarchischen Verbund gespeichert sind.

Sie können den Zugriff auf den Ereignisprotokollspeicher von einem oder mehreren bestimmten CA Enterprise Log Manager-Servern beschränken, indem Sie Datenzugriffsfilter erstellen. Sie können Zugriffsfilter auf einen Benutzer oder auf eine Gruppe anwenden.

So erstellen Sie einen Zugriffsfilter für eine benutzerdefinierte Rolle:

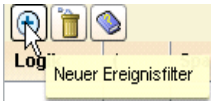
1. Klicken Sie auf die Registerkarte "Verwaltung" und auf die Unterregisterkarte "Benutzer- und Zugriffsverwaltung".
2. Klicken Sie auf "Neuer Zugriffsfilter".

   Der Assistent zum Erstellen von Zugriffsfiltern wird angezeigt.
3. Geben Sie unter "Details" den Namen und eine Beschreibung für den Filter ein.
4. Klicken Sie auf "Identitäten". Wählen Sie einen Identitätstyp aus; klicken Sie auf die Schaltfläche "Suchen", um verfügbare Identitäten anzuzeigen, und verwenden Sie die Wechselsteuerung, um diejenigen auszuwählen, auf die dieser Zugriffsfilter angewendet werden soll.

   Wählen Sie beispielsweise die Anwendungsgruppe aus, die Sie für diesen Zweck erstellt haben.

5. Legen Sie die Zugriffsfilter fest.
   a. Klicken Sie auf "Zugriffsfilter".
   b. Klicken Sie auf die Schaltfläche "Neuer Ereignisfilter".



   c. Fügen Sie eine oder mehrere Ausdrücke hinzu, die den Zugriffsfilter definieren.
   d. Klicken Sie auf "Speichern und schließen".

   Der Zugriffsfilter, den Sie erstellt haben, wird angezeigt.
6. Klicken Sie auf "Schließen".

Weitere Informationen:

Schritt 4: Erstellen eines Datenzugriffsfilters für Windows-Administratoren (siehe Seite 135)
Erstellen einer Anwendungsbenutzergruppe (Rolle) (siehe Seite 96)

Verwalten von Benutzerkonten und Zugriffsrichtlinien

Als Administrator können Sie die folgenden Verwaltungsaufgaben für Benutzerkonten und Zugriffsrichtlinien durchführen:

- Sperren von Benutzerkonten, so dass sich der jeweilige Benutzer nicht mehr bei CA Enterprise Log Manager anmelden kann
- Aufheben von Sperren von Benutzerkonten, die gesperrt wurden, sofern die Kennwortrichtlinie nicht zulässt, dass ein Benutzer die Sperre eines gesperrten Benutzerkontos aufhebt.
- Hinzufügen neuer Benutzerkonten
- Bearbeiten vorhandener Benutzerkonten
- Sperren oder Löschen von Benutzerkonten, die Benutzern gehören, die keinen Zugriff auf CA Enterprise Log Manager mehr benötigen
- Bearbeiten vorhandener Zugriffsrichtlinien
- Löschen von Zugriffsrichtlinien, die nicht mehr benötigt werden
- Erstellen, Bearbeiten oder Löschen von Delegierungsrichtlinien
- Erstellen, Bearbeiten oder Löschen von Zugriffsfiltern mit den entsprechenden, automatisch erstellten Verpflichtungsrichtlinien
- Erstellen einer übergeordneten Rolle aus vorhandenen Rollen mit eingeschränktem Zugriff
- Hinzufügen einer neuen benutzerdefinierten Rolle und der entsprechenden Zugriffsrichtlinien

Erstellen von Kalendern

Sie können einen neuen Kalender erstellen, um den Benutzerzugriff in bestimmten Zeiträumen besser einschränken zu können. Kalender fungieren als Teil von Zugriffsrichtlinien. Wenn Sie einen Kalender definieren, können Sie Zeitblöcke in Stunden, Wochentagen oder Daten aus- oder einschließen.

So erstellen Sie einen Kalender:

1. Klicken Sie auf die Registerkarte "Verwaltung", auf "Benutzer- und Zugriffsverwaltung" und anschließend auf die Schaltfläche "Kalender".

   Die Seite "Kalender" wird angezeigt.

2. Klicken Sie oben links in der Kalenderliste auf das Symbol "Neuer Kalender".

   Der Detailbereich "Neuer Kalender" wird angezeigt.

3. Geben Sie einen Namen ein, der die Zielrichtlinie angibt, und geben Sie eine Beschreibung der gewünschten Verwendung ein.
4. Legen Sie mit Hilfe der Kalendersymbole Start- und Enddaten für den Kalender fest.
5. Klicken Sie auf "Einschlusszeitblock hinzufügen" oder "Ausschlusszeitblock hinzufügen", um innerhalb des Geltungszeitraums des Kalenders Ausnahmezeiträume zu erstellen.
6. Klicken Sie auf "Speichern" und anschließend auf "Schließen".

Weitere Informationen:

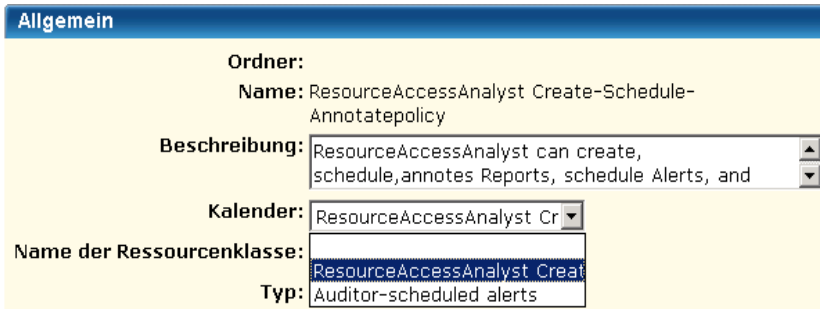
Hinzufügen eines Kalenders zu Richtlinien (siehe Seite 116)

Hinzufügen eines Kalenders zu Richtlinien

Wenn Sie eine Richtlinie erstellen, können Sie einen vorhandenen Kalender auswählen, in dem angegeben ist, wann die festgelegten Identitäten die ausgewählten Aktionen für die festgelegten Ressourcen ausführen können. In einem Kalender können Start- und Enddaten sowie Zeitblöcke in Stunden oder Wochentagen definiert sein.

So fügen Sie einer Richtlinie einen Kalender hinzu:

1. Klicken Sie auf die Registerkarte "Verwaltung" und auf die Unterregisterkarte "Benutzer- und Zugriffsverwaltung".
2. Öffnen Sie die Richtlinie, für die dieser Kalender gilt.
   a. Klicken Sie auf "Zugriffsrichtlinien".
   b. Wählen Sie den Richtlinientyp aus.
   c. Wählen Sie die Richtlinie aus.
3. Öffnen Sie die Dropdown-Liste "Kalender", und wählen Sie den Kalender aus, den Sie für diese Richtlinie erstellt haben.



4. Klicken Sie auf "Speichern", um zu speichern, dass der Kalender einer vorhandenen Richtlinie hinzugefügt wurde.

Weitere Informationen:

Erstellen von Kalendern (siehe Seite 115)

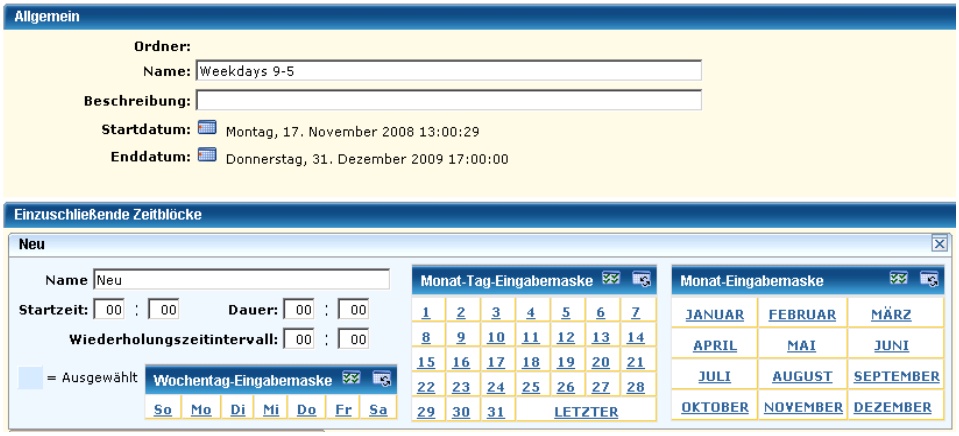
Beispiel: Den Zugriff auf Werktage beschränken

Sie können die Tageszeit bzw. die Wochentage, in der bzw. an denen eine bestimmte Benutzergruppe Zugriff auf CA Enterprise Log Manager erhält, einschränken durch Erstellen eines Kalender für die Zeiträume, in denen Zugriff gewährt wird, einer benutzerdefinierten Rolle, einer neuen Richtlinie auf der Grundlage der Richtlinie, die Zugriff zu CA Enterprise Log Manager gewährt, und indem Sie dieser Richtlinie die Kalender- sowie die benutzerdefinierte Rolle zuweisen.

Beispiel: Beschränken des Zugriffs auf CA Enterprise Log Manager durch einen externen Auditor auf Werktage

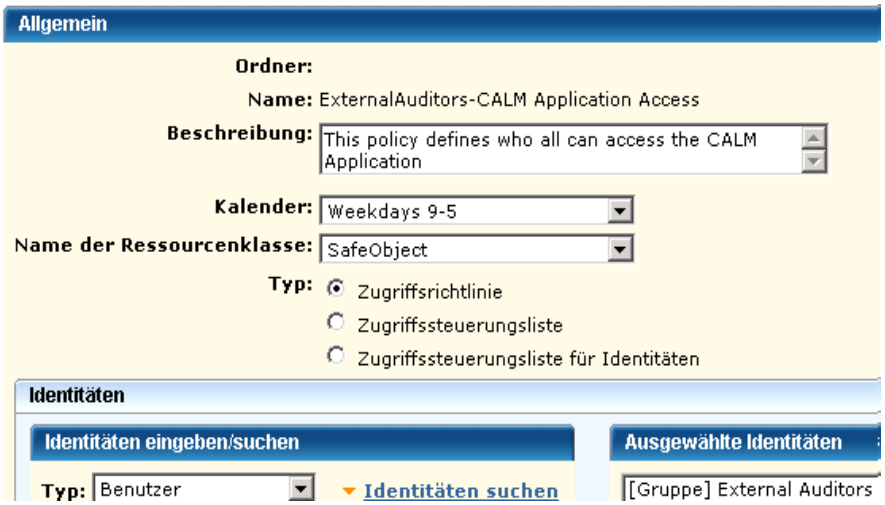
Um den Zugriff bestimmter Gruppen auf CA Enterprise Log Manager auf Werktage zu beschränken, erstellen Sie einen Kalender für Werktage und fügen Sie ihn den Richtlinien hinzu, die Auditoren bestimmte Zugriffsrechte gewähren.

Wenn Sie z. B. den Zugriff auf CA Enterprise Log Manager durch externe Auditoren auf die Geschäftszeit beschränken möchten, erstellen Sie einen Kalender, der die Wochentage Montag bis Freitag, 9:00 bis 17:00 Uhr, für alle Monate des Jahres angibt.



Erstellen Sie eine Rolle für externe Auditoren.

Öffnen Sie die CALM-Anwendungszugriff-Bereichsrichtlinie und speichern Sie sie unter "ExterneAuditoren-CALM-Anwendungszugriff", wählen Sie den Kalender für Werktage, 9 bis 17 Uhr, und die Benutzergruppe "Externe Auditoren" als Identität aus.



Wichtig! Verwenden Sie die Kalenderfunktion nur bei solchen Richtlinien, die Zugriff gewähren. Verwenden Sie sie nicht bei solchen Richtlinien, die den Zugriff verweigern.

Weitere Informationen:

Erstellen von Kalendern (siehe Seite 115)
Erstellen einer Anwendungsbenutzergruppe (Rolle) (siehe Seite 96)
Erstellen einer Richtlinie auf der Grundlage einer vorhandenen Richtlinie (siehe Seite 108)
Hinzufügen eines Kalenders zu Richtlinien (siehe Seite 116)

Exportieren von Zugriffsrichtlinien

Sie können jederzeit sämtliche Richtlinien eines ausgewählten Typs exportieren. Hierbei kann es sich sowohl um vordefinierte Richtlinien als auch um benutzerdefinierte Richtlinien handeln. Der Export von Richtlinien stellt eine gute Möglichkeit zur Speicherung einer aktuellen Sicherung dar.

Bei einem Export wird für jede ausgewählte Richtlinie eine XML-Datei erstellt. Hierbei werden alle XML-Dateien in einer Datei namens "CAELM[1].xml.gz" komprimiert.

So exportieren Sie Zugriffsrichtlinien:

1. Klicken Sie auf die Registerkarte "Verwaltung" und auf die Unterregisterkarte "Benutzer- und Zugriffsverwaltung".
2. Klicken Sie auf "Zugriffsrichtlinien".
3. Wählen Sie den Typ der zu exportierenden Zugriffsrichtlinien aus, und klicken Sie auf "Exportieren".

   Das Dateidownload-Dialogfeld wird eingeblendet.
4. Klicken Sie auf "Speichern", und speichern Sie die Datei unter einem eindeutigen Namen.
5. Klicken Sie auf "Schließen".

Weitere Informationen:

Sichern aller Zugriffsrichtlinien (siehe Seite 67)

Löschen von benutzerdefinierten Richtlinien

Sie können eine benutzerdefinierte Richtlinie aus jedem der folgenden Gründe löschen:

- Sie haben sie unter einem anderen Namen gespeichert und planen keine weiteren Änderungen, so dass Sie das Duplikat löschen müssen.
- Es gibt unter den für die Richtlinie definierten Identitäten keine aktiven Mitgliedschaften mehr, so dass die Richtlinie nicht länger in Verwendung ist.

Wichtig! Achten Sie darauf, keine vordefinierte Richtlinie zu löschen. Sollte dies passieren, können Sie sie mit einer exportierten Sicherung wiederherstellen.

So löschen Sie eine benutzerdefinierte Richtlinie:

1. Klicken Sie auf die Registerkarte "Verwaltung" und auf die Unterregisterkarte "Benutzer- und Zugriffsverwaltung".
2. Klicken Sie auf "Zugriffsrichtlinien".
3. Wählen Sie entweder "CALM-Richtlinien" oder "Bereichsrichtlinien", abhängig vom Typ der Richtlinie, die Sie löschen möchten.
4. Klicken Sie auf den Namen der zu löschenden Richtlinie.
5. Klicken Sie auf "Löschen".
6. Klicken Sie auf "OK", um den Löschvorgang zu bestätigen.

Löschen von Zugriffsfiltern und Verpflichtungsrichtlinien

Sie können einen Zugriffsfilter und die von diesem generierte Verpflichtungsrichtlinie löschen, um die Beschränkung des Datenzugriffs zu entfernen.

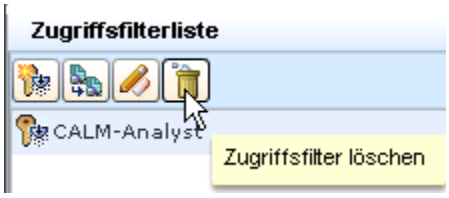
Löschen Sie die von dem Filter generierte Verpflichtungsrichtlinie nicht aus den Zugriffsrichtlinien.

So löschen Sie einen Zugriffsfilter und die zugehörige Verpflichtungsrichtlinie:

1. Klicken Sie auf die Registerkarte "Verwaltung" und anschließend auf "Benutzer- und Zugriffsverwaltung".

   Die Zugriffsfilterliste wird oben im linken Fensterbereich angezeigt.

2. Wählen Sie den zu löschenden Filter aus, und klicken Sie auf die Schaltfläche "Zugriffsfilter löschen".

   Die Warnmeldung "Bestätigung des Löschens des Zugriffsfilters" wird angezeigt.

3. Klicken Sie auf "Ja", um den ausgewählten Zugriffsfilter und die zugewiesene Verpflichtungsrichtlinie zu entfernen.

Beispiel: Einem Nicht-Administrator gestatten, Archive zu verwalten

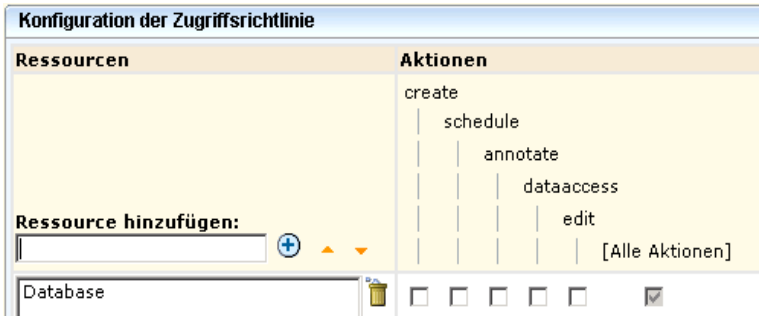
Angenommen, Sie möchten einer Gruppe Nicht-Administratoren gestatten, die automatische Archivierung zu verwalten. Zu diesem Zweck können Sie eine Gruppe "ArchivAdministrator" erstellen sowie eine CALM-Richtlinie, die die Aktion "Bearbeiten" hinsichtlich der Ressourcendatenbank gestattet. Dies ermöglicht den Lesezugriff auf den Datenbank-Archivkatalog, um Abfragen durchzuführen, Schreibzugriff auf den Archivkatalog zur Neukatalogisieren (ReCatalog) sowie die Verwendung des LMArchive-Hilfsprogramms für die manuelle Archivierung oder des Shell-Skripts "restore-ca-elm" zur Wiederherstellung automatisch archivierter Datenbanken.

So gestatten Sie Nicht-Administratoren, die automatische Archivierung durchzuführen:

1. Erstellen Sie eine Rolle mit der Bezeichnung "ArchivAdministrator".
   a. Wählen Sie die Registerkarte "Verwaltung" und dann die Unter-Registerkarte "Benutzer- und Zugriffsverwaltung".
   b. Wählen Sie "Gruppen".
   c. Klicken Sie auf "Neue Anwendungsgruppe".
   d. Geben Sie "ArchivAdministrator" als Namen ein.
   e. Klicken Sie auf "Speichern".

      Die Anwendungsgruppe bzw. Rolle "ArchivAdministrator" wird erstellt.
   f. Klicken Sie auf "Schließen".

2. Erstellen Sie eine CALM-Richtlinie, die Bearbeitungszugriff auf die Datenbankressource erlaubt.
   a. Klicken Sie auf "Zugriffsrichtlinien".
   b. Klicken Sie auf "Neue Zugriffsrichtlinie", um eine neue CALM-Richtlinie zu erstellen.
   c. Geben Sie "ArchivAdministrator-Richtlinie" in das Feld "Name" ein.
   d. Geben Sie als Beschreibung ein, dass "ArchivAdministrator" das LMArchive-Hilfsprogramm und das Shell-Skript "restore-ca-elm" ausführen darf.
   e. Wählen Sie als Identitäten "Anwendungsgruppe" für den Typ, klicken Sie auf "Suchidentitäten" und dann auf "Suchen".
   f. Wählen Sie "ArchivAdministrator", und klicken Sie dann auf den Pfeil zum Verschieben.
   g. Geben Sie unter "Ressource hinzufügen" "Datenbank" ein, und klicken Sie auf "Hinzufügen".
   h. Wählen Sie "Bearbeiten" als Aktion.



   i. Klicken Sie auf "Speichern". Klicken Sie auf "Schließen".

3. Testen Sie die Richtlinie, und überprüfen Sie, ob das Ergebnis ZULASSEN ist.

Ergebnis	Richtlinie	Identität	Ressourcenklasse	Ressource	Aktion
ZULASSEN	ArchiveAdministrator policy	ug:ArchiveAdministrator	CALM	Database	edit

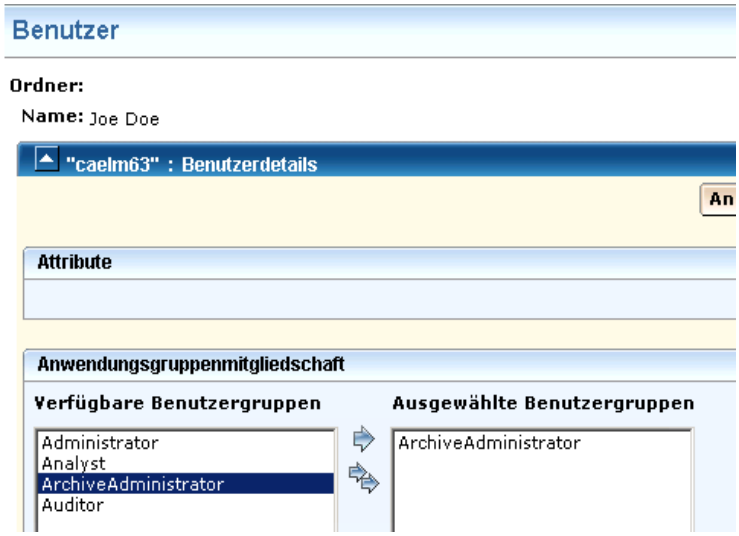
4. Gestatten Sie der "ArchivAdministrator"-Rolle, sich bei CA Enterprise Log Manager anzumelden.
   a. Klicken Sie unter "Zugriffsrichtlinien" auf "CALM".
   b. Wählen Sie "CALM-Anwendungszugriff".
   c. Suchen Sie unter "Identitäten" nach der Anwendungsgruppe "ArchivAdministrator", und verschieben Sie sie nach "Ausgewählte Identitäten".

   d. Klicken Sie auf "Speichern". Klicken Sie auf "Schließen". Klicken Sie auf "Schließen".

      Die Registerkarte "Benutzer- und Zugriffsverwaltung" wird mit den Schaltflächen im linken Fensterbereich eingeblendet.

5. Weisen Sie die Rolle "ArchivAdministrator" einem oder mehreren Benutzern zu.
   a. Klicken Sie auf "Benutzer".
   b. Geben Sie den Namen einer Person, der Sie diese Rolle zuweisen möchten, unter "Benutzer suchen" als Wert ein, und klicken Sie dann auf "Los".

      Der ausgewählte Benutzername wird unter dem Ordner "Benutzer" eingeblendet.
   c. Wählen Sie den Link für den ausgewählten Benutzer aus.
   d. Klicken Sie auf "Anwendungsbenutzerdetails hinzufügen".
   e. Verschieben Sie "ArchivAdministrator" in die Liste "Ausgewählte Benutzergruppen".



   f. Klicken Sie auf "Speichern". Klicken Sie auf "Schließen".
   g. Wiederholen Sie dies für jeden Benutzer, dem Sie diese Rolle zuweisen möchten.
   h. Klicken Sie auf "Schließen".

6. (Optional) Überprüfen Sie die Ergebnisse von CA Enterprise Log Manager.
   a. Klicken Sie auf "Abmelden", um sich als Administrator abzumelden.
   b. Melden Sie sich als derjenige Benutzer an, dem Sie die Rolle "ArchivAdministrator" zugewiesen haben.
   c. Klicken Sie auf die Registerkarte "Verwaltung" und auf die Unter-Registerkarte "Protokollerfassung".
   d. Wählen Sie "Archivkatalogabfrage".
   e. Achten Sie darauf, die Schaltflächen "Abfrage" und "Neukatalogisieren" zu verwenden.
7. (Optional) Führen Sie das Wiederherstellungsskript "restore-ca-elm" mit den Berechtigungsnachweisen desjenigen Benutzers durch, dem die Rolle "ArchivAdministrator" zugewiesen wurde, um zu prüfen, ob die Richtlinie wie erwartet funktioniert.

Weitere Informationen:

Wiederherstellen automatisch archivierter Dateien (siehe Seite 220)

Beschränken des Datenzugriffs für einen Benutzer: Windows-Administrator

Sie können die Berichte, die Benutzer anzeigen können, auf Benutzer mit einer festgelegten Kennung beschränken. Außerdem können Sie die Daten, die Benutzer in diesen Berichten anzeigen können, auf Daten beschränken, die von festgelegten Ereignisquellen generiert wurden. Die Beschränkung des Zugriffs auf Berichte mit einer bestimmten Kennung erfolgt über eine Zugriffsrichtlinie. Mit einem Zugriffsfilter hingegen wird der Datenzugriff auf Ereignisse beschränkt, die an einen bestimmten CA Enterprise Log Manager-Server zurückgegeben werden. Wenn ein Zugriffsfilter definiert wurde, ist die Zuweisung einer Rolle optional. Dies bedeutet, dass Sie einen neuen Benutzer erstellen können, ohne ihm eine Rolle zuzuweisen, und den Datenzugriff für diesen Benutzer trotzdem mit einem Zugriffsfilter beschränken können.

Betrachten Sie das Szenario für das Unternehmen ABC mit vier Datenzentren in den Vereinigten Staaten. Der Administrator möchte dem Windows-Administrator in der Region Houston Lesezugriff auf Windows-Ereignisse geben, die vom Domänen-Controller im Bereich Houston verarbeitet werden. Die Windows-Ereignisse, die von dem auf dem Domänen-Controller in Houston installierten CA Enterprise Log Manager-Server verarbeitet werden, werden von Quellen gesendet, bei denen die Hostnamen mit der Zeichenfolge "ABC-HOU-WDC" beginnen.

Dieses Beispiel erläutert Ihnen Schritt für Schritt, wie Sie einen Benutzer "Windows-Administrator" erstellen und dabei sicherstellen, dass dieser Benutzer nur Berichte mit der Kennung "Systemzugriff" anzeigen kann und dass die Daten in diesen Berichten auf Ereignisse von Ereignisquellen mit Hostnamen beschränkt sind, die mit der genannten Benennungskonvention beginnen.

Im Beispiel finden Sie Details zu jedem der folgenden Schritte:

1. Erstellen Sie den neuen Benutzer "Windows-Administrator".
2. Gewähren Sie dem Benutzer "Windows-Administrator" grundlegenden Zugriff auf CA Enterprise Log Manager. Fügen Sie diese Identität der CALM-Anwendungszugriffsrichtlinie hinzu.
3. Beschränken Sie den Zugriff auf Berichte für "Windows-Administrator" auf solche Berichte, die mit "Systemzugriff" gekennzeichnet sind. Erstellen Sie eine Richtlinie zur Bereichsdefinierung mit Lesezugriff auf "AppObject" und mit Filtern, die den EEM-Ordner als Speicherort für Berichte angeben und festlegen, dass "calmTag" mit dem Wert von "Systemzugriff" identisch ist. Testen Sie die Richtlinie.
4. Beschränken Sie die Daten, die der Benutzer "Windows-Administrator" anzeigen kann, auf die Daten, die vom Domänen-Controller in der Region von "Windows-Administrator" generiert werden. Erstellen Sie einen Zugriffsfilter mit dem Namen "Datenzugriff von Windows-Administrator", der die Abfrage- und Berichtsdaten, die "Windows-Administrator" anzeigen kann, auf Windows-Ereignisse von Ereignisquellen mit einem Hostnamen beschränkt, der mit "ABC-HOU-WDC" beginnt.
5. Melden Sie sich als Benutzer "Windows-Administrator" bei CA Enterprise Log Manager an, und werten Sie den durch die Richtlinien bereitgestellten Zugriff aus.
6. Falls der Zugriff so stark beschränkt ist, dass der Benutzer die ihm zugedachten Aufgaben nicht ausführen kann, erweitern Sie den Zugriff durch zusätzliche Richtlinien.

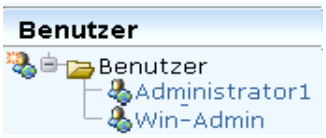
Schritt 1: Erstellen des Benutzers "Windows-Administrator"

Sie können einen Benutzer ohne Rolle (Anwendungsgruppe) erstellen, wenn Sie den Datenzugriff mit einem Zugriffsfilter festlegen.

Den ersten Schritt des gesamten Prozesses, durch den Sie den Datenzugriff auf diese Weise beschränken können, bildet die Erstellung des Benutzers.

Nur wenn das globale Benutzerkonto für den Import aus einem externen Verzeichnis nicht verfügbar ist, erstellen Sie einen Benutzer. Fügen Sie beim Erstellen eines solchen Kontos keine Anwendungsbenutzerdetails hinzu. In diesem Beispielszenario lautet der Benutzername "Windows-Administrator".

Wenn Sie nach Benutzern suchen, wird der neue Name in der Liste aufgeführt.



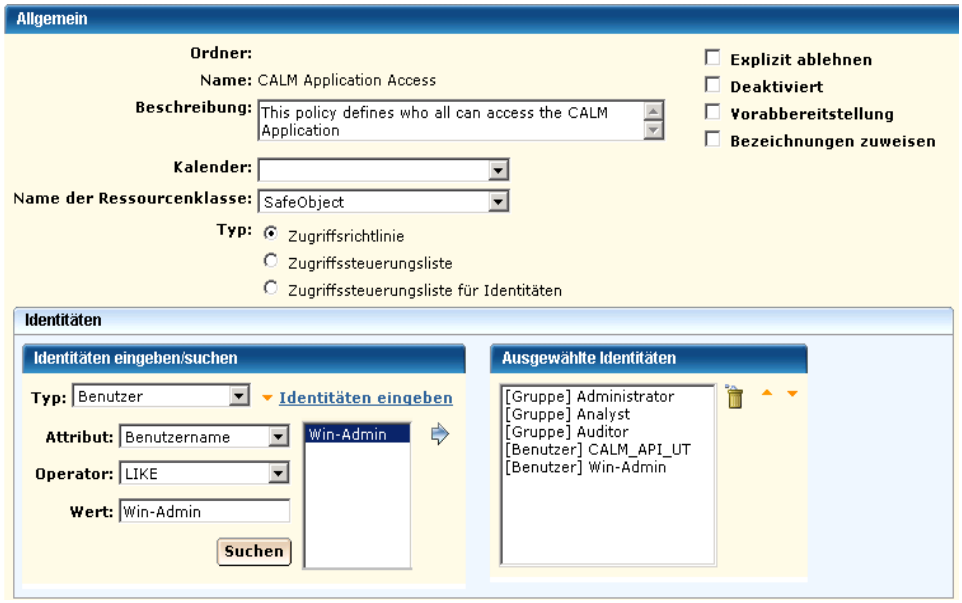
Weitere Informationen:

Erstellen eines globalen Benutzers (siehe Seite 42)

Schritt 2: Hinzufügen des Benutzers "Windows-Administrator" zur CALM-Anwendungszugriffsrichtlinie

Der zweite Schritt beim Beschränken des Datenzugriffs eines Benutzers mit dem Namen "Windows-Administrator" besteht darin, dieser Identität den Zugriff auf die CA Enterprise Log Manager-Anwendung zu gewähren.

Fügen Sie den neuen Benutzer der CALM-Anwendungszugriffsrichtlinie hinzu. Sie gehen dabei genauso vor, als würden Sie CA Enterprise Log Manager Zugriff auf eine neue Rolle gewähren. Die einzige Ausnahme besteht darin, dass Sie "Typ" beim Suchen von Identitäten auf "Benutzer" festlegen.



Weitere Informationen

Gewähren des Zugriffs auf CA Enterprise Log Manager für eine benutzerdefinierte Rolle (siehe Seite 98)

Schritt 3: Erstellen einer Systemzugriffsrichtlinie für Windows-Administratoren

In Schritt 2 gewähren Sie Zugriff für die Anmeldung bei der CA Enterprise Log Manager-Anwendung.

Durch Schritt 3 wird der Zugriff auf die CA Enterprise Log Manager-Anwendung nach der Anmeldung beschränkt, beziehungsweise es wird ein Zugriffsbereich definiert. Grundsätzlich können Sie den angegebenen Identitäten entweder nur Lesezugriff oder sowohl Lese- als auch Schreibzugriff gewähren.

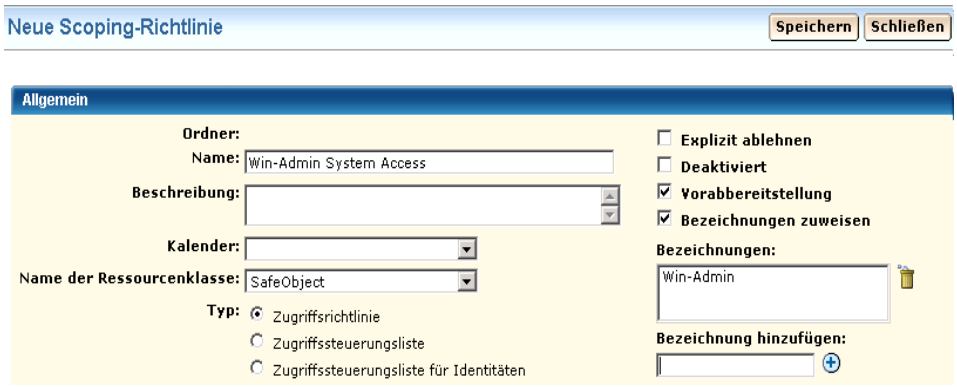
Die Auswahl des Richtlinientyps bestimmt die Granularität, mit der Sie zugelassene Aktionen festlegen können.

- Zugriffsrichtlinien ermöglichen ausgewählte Aktionen für die betreffenden ausgewählten Ressourcen.
- Durch Zugriffskontrolllisten-Richtlinien können Sie festlegen, welche Aktionen für jede hinzugefügte Aktion zulässig sind.
- Durch Zugriffskontrolllisten-Richtlinien können Sie festlegen, welche Aktionen von den einzelnen Identitäten für die betreffenden Ressourcen zulässig sind.

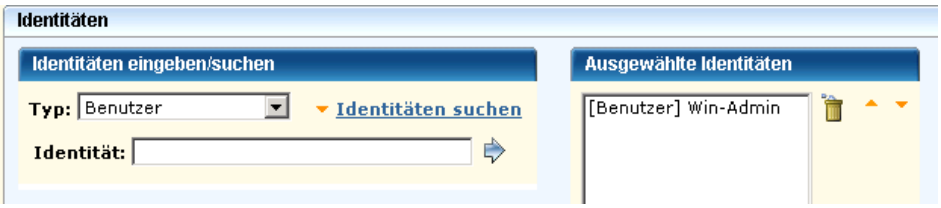
Sie können einen beschränkten Zugriff auf eine Ressource zulassen, indem Sie einen Filter erstellen, der den EEM-Ordner für die jeweilige Ressource festlegt, und anschließend Beschränkungen für den Ordner angeben.

Dieses Beispiel veranschaulicht, wie Sie den Zugriff generell auf einen Lesezugriff beschränken und dabei weitere Beschränkungen für eine spezifische Funktion festlegen. Insbesondere in Schritt 3 wird der Benutzer "Windows-Administrator" auf die Anzeige von Systemzugriffsberichten beschränkt. Das folgende Beispiel erläutert, wie Sie eine Richtlinie zur Bereichsdefinierung mit dem Namen "Systemzugriff von Windows-Administrator" erstellen, die Lesezugriff auf "SafeObject" und "AppObject" gewährt und Filter festlegt, die den Berichtszugriff auf Berichte mit der Kennung "Systemzugriff" beschränkt. Es veranschaulicht zudem, wie Sie die Richtlinie testen und nach der Überprüfung die Einstellung "Vorbereitstellung" entfernen.

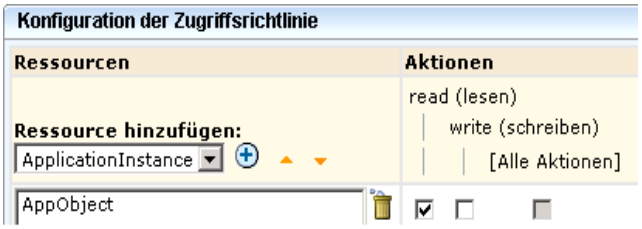
Der Bereich "Allgemein" einer Richtlinie zur Bereichsdefinierung, durch die sich der Anwendungszugriff auf einen reinen Lesezugriff oder sowohl auf Lese- als auch auf Schreibzugriff einstellen lässt, legt "SafeObject" als Ressourcenklassenname fest. Im folgenden Beispiel ist der Richtlinienname von "Systemzugriff von Windows-Administrator" dargestellt. Es empfiehlt sich, für eine neue Richtlinie das Kontrollkästchen "Vorbereitstellung" zu aktivieren, bis Sie sie getestet haben und sich davon überzeugt haben, dass sie für den Einsatz in einer Produktionsumgebung geeignet ist.



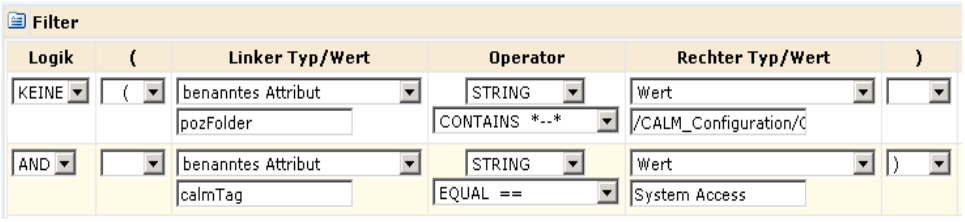
Sie können den Zugriff entweder Benutzern oder Gruppen gewähren. In diesem Beispiel wird der Zugriff dem neuen Benutzer "Windows-Administrator" gewährt.



Die für CA Enterprise Log Manager erstellte Richtlinie der "höchsten Ebene" ist die CALM-Zugriffsrichtlinie. CAELM ist dabei die Anwendungsinstanz. Mit dieser Richtlinie zur Bereichsdefinierung wird festgelegt, dass die Leseaktion für die Anwendungsobjekte ("AppObject") zulässig ist. "AppObject" bezieht sich auf alle Anwendungsfunktionen.

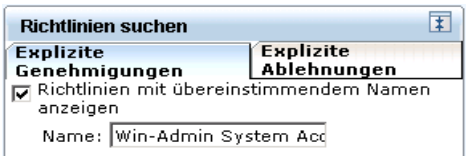


Sie können die angegebene zulässige Aktion für alle Objekte weiter beschränken, indem Sie Filter festlegen. Filter werden oftmals paarweise angegeben. Dabei legt der erste Filter den CA EEM-Ordner fest, in dem Daten zu einer bestimmten Funktion gespeichert werden. Der zweite Filter legt eine Beschränkung für Objekte an diesem Speicherort fest. Durch den ersten Filter im folgenden Beispiel wird der Zugriff des CA EEM-Ordners auf den Ordner beschränkt, in dem die Berichtsressource gespeichert ist. Insbesondere legt er fest, dass "pozFolder" das Verzeichnis "/CALM_Configuration/Content/Reports" enthält. Der zweite Filter beschränkt den Zugriff auf Berichte mit der Kennung "Systemzugriff", indem er festlegt, dass "calmTag" mit "Systemzugriff" identisch ist.

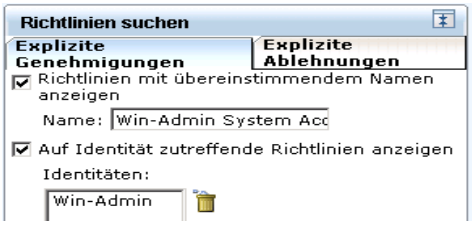


Nach dem Speichern einer Richtlinie können Sie danach suchen, um sie zu überprüfen. Sie haben die Möglichkeit, anhand des Namens, der Identität oder der Ressource nach Richtlinien zu suchen. Sie können einen Teilwert eingeben. Darüber hinaus können Sie mehrere Kriterien eingeben. Im Folgenden finden Sie Beispiele für dieses Szenario.

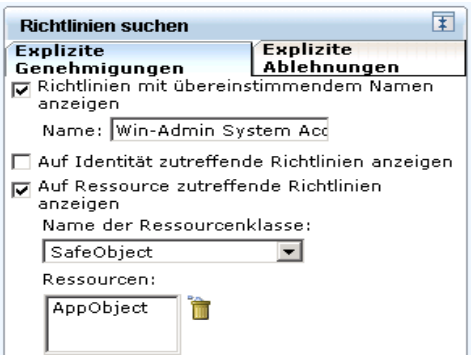
Bei der Suche anhand des vollständigen Namens wird genau die Richtlinie angezeigt, die Sie benötigen.



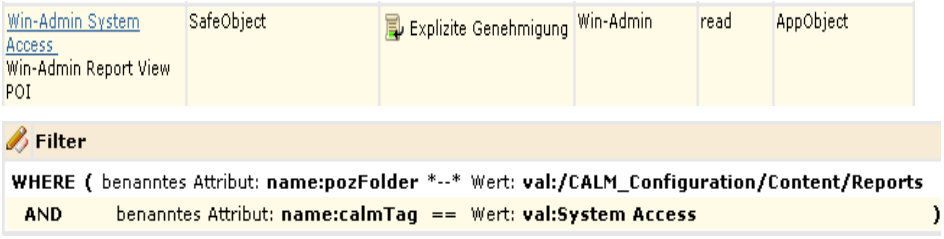
Wenn Sie nur anhand der Identität suchen, werden sämtliche Richtlinien angezeigt, die für diese Identität gelten, also auch die Richtlinien, die für alle Identitäten gelten.



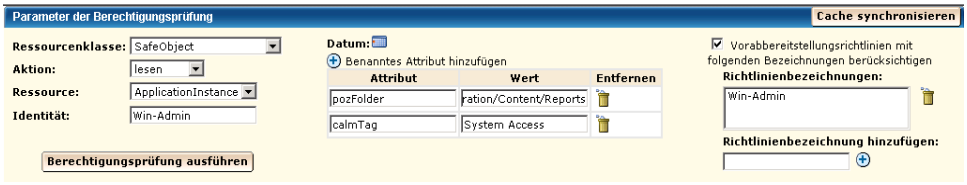
Bei einer ausschließlichen Suche anhand der Ressource, bei der "AppObject" die Ressource ist, werden alle vom System bereitgestellten und benutzerdefinierten Richtlinien angezeigt, die Lesezugriff oder Lese- und Schreibzugriff auf eine Identität gewähren.



Wenn die von Ihnen gesuchte benutzerdefinierte Richtlinie in der Richtlinientabelle angezeigt wird, überprüfen Sie die Werte, einschließlich der Filter. Falls Ihnen Angaben auffallen, die korrigiert werden müssen, können Sie auf den Namenslink klicken, um die Richtlinie zum Bearbeiten neu anzuzeigen.

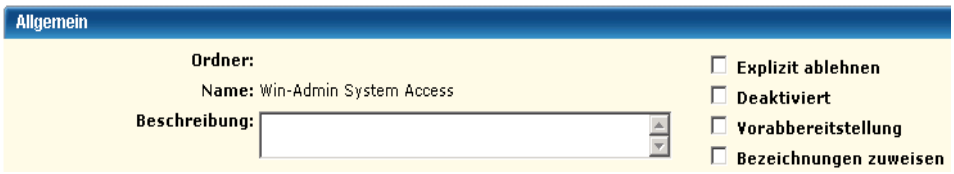


Es empfiehlt sich, jede neue Richtlinie zu testen. Achten Sie darauf, dass Sie die Attribut/Wert-Paare in der Reihenfolge eingeben, in der Sie die Filter eingegeben haben. Beginnen Sie dabei mit dem Attribut der höheren Ebene.



Vergewissern Sie sich, dass das Ergebnis ALLOW lautet.

Deaktivieren Sie anschließend das Kontrollkästchen "Vorbereitstellung" für die Richtlinie. Andernfalls können Sie sich nicht als "Windows-Administrator" anmelden, um auszuwerten, welche Aktionen dieser Benutzer ausführen kann.



Weitere Informationen:

Testen von neuen Richtlinien (siehe Seite 110)

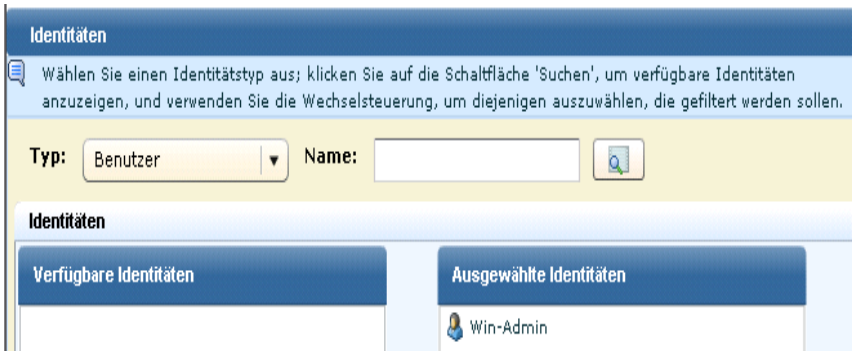
Schritt 4: Erstellen eines Datenzugriffsfilters für Windows-Administratoren

In Schritt 3 wird der Benutzer "Windows-Administrator" auf die Anzeige von Systemzugriffsberichten beschränkt. Auf dieser Zugriffsebene kann der Benutzer "Windows-Administrator" auf Systemzugriffsberichte für alle vier Regionen des Unternehmens ABC zugreifen.

In Schritt 4 wird ein Zugriffsfilter erstellt, mit dem die Daten, die der Benutzer "Windows-Administrator" anzeigen kann, auf die Systemzugriffsberichte für den Domänen-Controller in Houston beschränkt werden.

Die Erstellung eines Datenzugriffsfilters beginnt mit dem Festlegen seines Namens. Der in diesem Szenario verwendete Name lautet "Datenzugriff von Windows-Administrator".

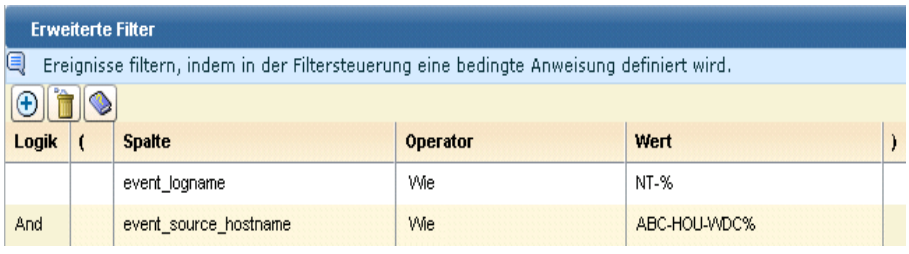
Im Bereich "Identitäten" geben Sie die Identitäten an, auf die der Zugriffsfilter angewendet werden soll. Ein Filter kann auf Benutzer oder Gruppen angewendet werden. In diesem Szenario wird der Filter nur auf den Benutzer "Windows-Administrator" angewendet.



Definieren Sie unter "Zugriffsfilter" jede Bedingung für den Wert einer CEG-Spalte. Auf den LIKE-Operator folgende Werte können eines der folgenden Platzhalterzeichen enthalten:

- _ (Unterstrich) – stellt ein beliebiges einzelnes Zeichen dar.
- % (Prozentzeichen) – stellt eine Zeichenfolge mit einer beliebigen Anzahl von Zeichen dar.

Der erste Filter für dieses Szenario nutzt die Tatsache aus, dass alle Windows-Ereignisse das Präfix "NT-" aufweisen. Wenn Sie die Daten auf Windows-Ereignisse beschränken möchten, können Sie angeben, dass die CEG-Spalte "event_logname" Daten enthalten muss, die die Zeichenfolge "NT-%" einschließen. Um die Windows-Ereignisse weiterhin auf solche Ereignisse zu beschränken, die von einem bestimmten Domänen-Controller stammen, ist in diesem Beispiel festgelegt, dass "event_source_hostname" Daten aufweisen muss, die basierend auf den lokalen Konventionen eine Zeichenfolge einschließen. Der Wert "ABC-HOU-WDC%" basiert auf der Benennungskonvention für einen durch Bindestriche verbundenen Namen, der sich aus Abkürzungen für das Unternehmen, die Region und das Präfix für den Domänen-Controller-Typ zusammensetzen.



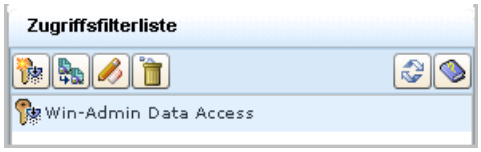
Logik	(	Spalte	Operator	Wert	)
		event_logname	Wie	NT-%	
And		event_source_hostname	Wie	ABC-HOU-WDC%	

Hinweis: Falls keine Ereignisquellen mit einer standardisierten Benennungskonvention vorhanden sind, können Sie eine Schlüsselwertliste mit den gewünschten Ereignisquellen-Hostnamen ("event_source_hostname") erstellen und den Namen der Schlüsselwertliste als Wert verwenden.

Wenn nur zwei Filter vorhanden sind und die Logik AND lautet, sind keine Klammern erforderlich. Bei der Eingabe eines komplexen Ausdrucks wie dem folgenden sind Klammern erforderlich.

```
(event_logname like NT-%
And event_source_hostname=ABC-%)
Or (event_logname like CALM-%
And event_source_hostname=XYZ-%)
```

Wenn Sie einen Datenzugriffsfilter speichern, wird sein Name in der Zugriffsfilterliste angezeigt.



Bei einer Suche nach Richtlinien, die eine Übereinstimmung mit dem Benutzernamen "Windows-Administrator" aufweisen, werden die drei Richtlinien für "Alle Identitäten" sowie drei weitere Richtlinien angezeigt: die CALM-Anwendungszugriffsrichtlinie, der "Windows-Administrator" hinzugefügt wurde, die von Grund auf neu erstellte Richtlinie "Systemzugriff von Windows-Administrator" und die Datenrichtlinie, die beim Definieren eines Zugriffsfilters automatisch hinzugefügt wird. Die Datenrichtlinie wird im Folgenden zuerst aufgeführt. Sie können sie auch unter den Pflichtrichtlinien anzeigen. Sie erstellen Pflichtrichtlinien niemals direkt mit CA Enterprise Log Manager.

Zugriffsrichtlinien

CALM Application Access This policy defines who all can access the CALM Application	SafeObject	Explizite Genehmigung	ug:Administrator ug:Analyst ug:Auditor Win-Admin	read write	ApplicationInstance AppObject Policy User GlobalUser
49aea1da-caelm54abaf7fc-8876c80-34 **Bezeichnungen:** DataPolicy	SafeObligation	Explizite Genehmigung	Win-Admin	FulfillOnGrant	dataaccess/CALM/Data
Win-Admin System Access **Bezeichnungen:** Win-Admin	SafeObject	Explizite Genehmigung Vorabbereitstellung	Win-Admin	read	AppObject

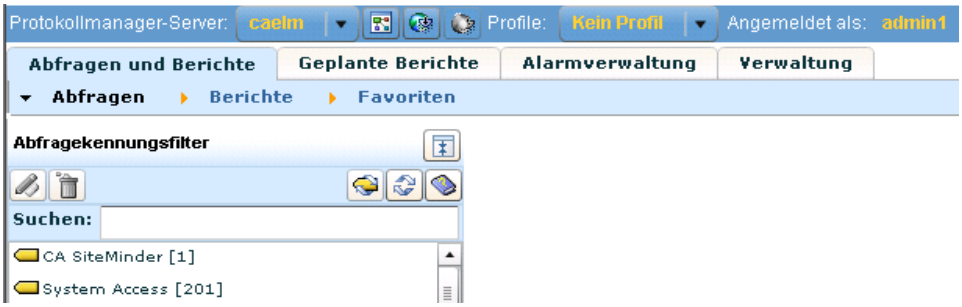
Weitere Informationen:

Erstellen eines Zugriffsfilters (siehe Seite 113)

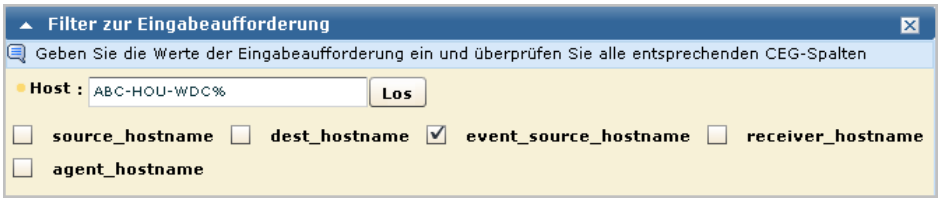
Schritt 5: Anmelden als Benutzer "Windows-Administrator"

Bevor Sie Richtlinien für einen bestimmten Benutzer oder eine Anwendungsbenutzergruppe erstellen, melden Sie sich als dieser Benutzer oder als entsprechendes Gruppenmitglied an und bestimmen Sie, welche Aktionen Sie ausführen dürfen und welche nicht. Überprüfen Sie zunächst, ob die Beschränkungen, die eingerichtet sein sollten, tatsächlich funktionieren. Überprüfen Sie dann, ob Sie die Aufgaben, die die entsprechenden Benutzer erledigen sollen, ausführen können.

Für dieses Szenario erwarten Sie, dass Sie nur Berichte oder Aktionsalarme anzeigen können, die mit "Systemzugriff" gekennzeichnet sind. Im Beispiel ist "Systemzugriff" der einzige verfügbare Abfragekennungsfilter. Somit wird Ihre Erwartung bestätigt.



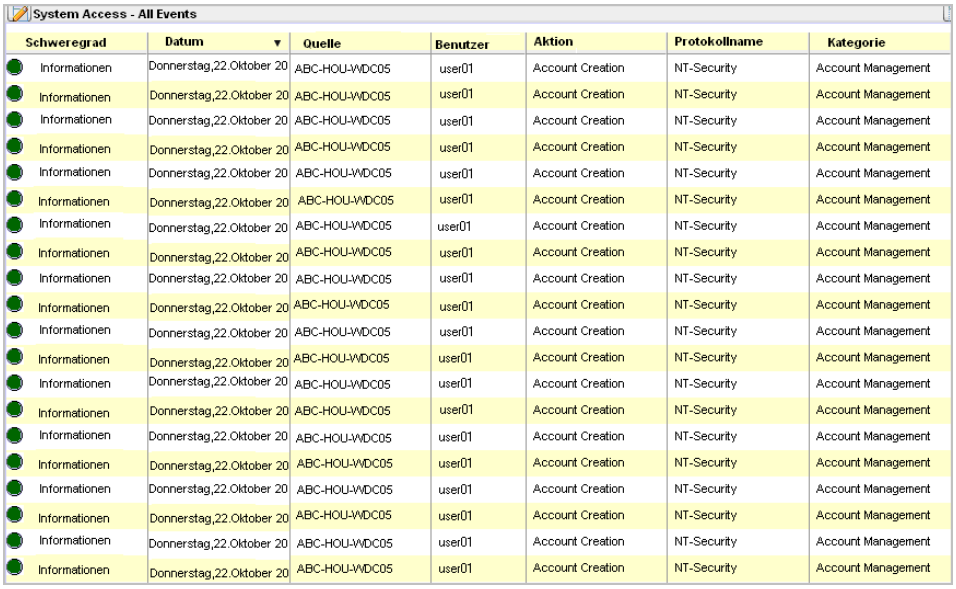
Mit Hilfe der Funktion "Eingabeaufforderungen" können Sie einen Zugriffsfilter schnell testen. Diese Funktion ist jedoch für den Benutzer "Windows-Administrator" nicht verfügbar. Alle Eingabeaufforderungsabfragen weisen die Kennung "Ereignisanzeige" auf. Mit dem Richtlinienfilter "calmTag=Event Viewer" kann der Zugriff auf Eingabeaufforderungsfilter gewährt werden.



Am besten testen Sie einen Zugriffsfilter, indem Sie die in einem Bericht angezeigten Daten überprüfen. Betrachten Sie den folgenden Zugriffsfilter: die CEG-Spalte "event_logname" beginnt mit "NT-" und die CEG-Spalte "event_source_hostname" mit "ABC-HOU-WDC" beginnt. Letzteres ist eine Abkürzung für das Unternehmen ABC, den Standort Houston und "Windows-Domänen-Controller".

```
event_logname Like NT-% AND event_source_hostname Like ABC-HOU-WDC%
```

Das folgende Beispiel zeigt einen Bericht, der von einem Benutzer angezeigt wird, für den dieser Zugriffsfilter gilt. Beachten Sie, dass die Daten in der Spalte "Protokollname" mit "NT-" beginnen und dass die Daten in der Spalte "Quelle" mit "ABC-HOU-WDC" beginnen.



System Access - All Events

Schweregrad	Datum	Quelle	Benutzer	Aktion	Protokollname	Kategorie
Informationen	Donnerstag,22.Oktober 20	ABC-HOU-WDC05	user01	Account Creation	NT-Security	Account Management
Informationen	Donnerstag,22.Oktober 20	ABC-HOU-WDC05	user01	Account Creation	NT-Security	Account Management
Informationen	Donnerstag,22.Oktober 20	ABC-HOU-WDC05	user01	Account Creation	NT-Security	Account Management
Informationen	Donnerstag,22.Oktober 20	ABC-HOU-WDC05	user01	Account Creation	NT-Security	Account Management
Informationen	Donnerstag,22.Oktober 20	ABC-HOU-WDC05	user01	Account Creation	NT-Security	Account Management
Informationen	Donnerstag,22.Oktober 20	ABC-HOU-WDC05	user01	Account Creation	NT-Security	Account Management
Informationen	Donnerstag,22.Oktober 20	ABC-HOU-WDC05	user01	Account Creation	NT-Security	Account Management
Informationen	Donnerstag,22.Oktober 20	ABC-HOU-WDC05	user01	Account Creation	NT-Security	Account Management
Informationen	Donnerstag,22.Oktober 20	ABC-HOU-WDC05	user01	Account Creation	NT-Security	Account Management
Informationen	Donnerstag,22.Oktober 20	ABC-HOU-WDC05	user01	Account Creation	NT-Security	Account Management
Informationen	Donnerstag,22.Oktober 20	ABC-HOU-WDC05	user01	Account Creation	NT-Security	Account Management
Informationen	Donnerstag,22.Oktober 20	ABC-HOU-WDC05	user01	Account Creation	NT-Security	Account Management
Informationen	Donnerstag,22.Oktober 20	ABC-HOU-WDC05	user01	Account Creation	NT-Security	Account Management
Informationen	Donnerstag,22.Oktober 20	ABC-HOU-WDC05	user01	Account Creation	NT-Security	Account Management
Informationen	Donnerstag,22.Oktober 20	ABC-HOU-WDC05	user01	Account Creation	NT-Security	Account Management
Informationen	Donnerstag,22.Oktober 20	ABC-HOU-WDC05	user01	Account Creation	NT-Security	Account Management
Informationen	Donnerstag,22.Oktober 20	ABC-HOU-WDC05	user01	Account Creation	NT-Security	Account Management
Informationen	Donnerstag,22.Oktober 20	ABC-HOU-WDC05	user01	Account Creation	NT-Security	Account Management
Informationen	Donnerstag,22.Oktober 20	ABC-HOU-WDC05	user01	Account Creation	NT-Security	Account Management
Informationen	Donnerstag,22.Oktober 20	ABC-HOU-WDC05	user01	Account Creation	NT-Security	Account Management
Informationen	Donnerstag,22.Oktober 20	ABC-HOU-WDC05	user01	Account Creation	NT-Security	Account Management
Informationen	Donnerstag,22.Oktober 20	ABC-HOU-WDC05	user01	Account Creation	NT-Security	Account Management
Informationen	Donnerstag,22.Oktober 20	ABC-HOU-WDC05	user01	Account Creation	NT-Security	Account Management
Informationen	Donnerstag,22.Oktober 20	ABC-HOU-WDC05	user01	Account Creation	NT-Security	Account Management

Schritt 6: Erweitern von gewährten Aktionen

Der in den Schritten 2, 3 und 4 dieses Beispiels definierte Richtlinien- und Zugriffsfilter gibt dem Benutzer "Windows-Administrator" die Möglichkeit, Systemzugriffsberichte anzuzeigen, bei deren Daten Beschränkungen bestehen. Mit diesem Zugriff allein kann der Benutzer "Windows-Administrator" weder einen Bericht oder Alarm planen noch einen Bericht mit Anmerkungen versehen. Damit der Benutzer "Windows-Administrator" diese Aktionen ausführen kann, fügen Sie ihn der Richtlinie für den Zugriff auf den Berichtsserver durch Analysten und Auditoren und der Richtlinie zum Erstellen, Planen und Anmerken durch Analysten hinzu. Im Folgenden finden Sie ein Beispiel dieser Richtlinien mit hinzugefügtem Benutzer "Windows-Administrator":

Analyst Auditor Report Server Access Policy Analyst ,Auditor can Schedule Reports and Alerts against all available Report Servers	SafeObject	Explizite Genehmigung	ug:Analyst ug:Auditor Win-Admin	read	AppObject
Analyst Create-Schedule-Annotate policy Analyst can create/schedule Reports, create profiles, schedule Action Alerts,Annotate Reports	CALM	Explizite Genehmigung	ug:Analyst Win-Admin	create schedule annotate	Report Alert Tag Profile

Damit der Benutzer "Windows-Administrator" einen Bericht erstellen kann, muss ihm in der Richtlinie "Systemzugriff von Windows-Administrator" zusätzlich Schreibzugriff gewährt werden. Hierzu öffnen Sie diese Richtlinie zum Bearbeiten und fügen den zulässigen Aktionen den Schreibzugriff hinzu.

Win-Admin System Access Win-Admin Report View POI	SafeObject	Explizite Genehmigung	Win-Admin	read	AppObject

Wenn Sie festlegen möchten, dass der Benutzer "Windows-Administrator" Eingabeaufforderungen verwenden kann, können Sie den Filter für die Richtlinie "Systemzugriff von Windows-Administrator" so ändern, dass das Attribut "calmTag" entweder mit "Systemzugriff" oder mit "Ereignisanzeige" identisch ist.

Filter

Logik	(	Linker Typ/Wert	Operator	Rechter Typ/Wert	)
KEINE		benanntes Attribut pozFolder	STRING CONTAINS *--*	Wert /CALM_Configuration/C	
AND	(	benanntes Attribut calmTag	STRING EQUAL ==	Wert System Access	
OR		benanntes Attribut calmTag	STRING EQUAL ==	Wert Event Viewer	)

Beschränken des Zugriffs für eine Rolle: PCI-Analyst

Sie können eine Rolle erstellen, die einer vordefinierten Rolle ähnelt, und schnell auf der Basis von vordefinierten Richtlinien modellierte Richtlinien generieren. Die benutzerdefinierte Rolle ähnelt der vordefinierten Rolle möglicherweise insofern, dass sie denselben Zugriff auf dieselben Ressourcentypen gewährt. Im Unterschied zur vordefinierten Rolle beschränkt sie den Zugriff jedoch basierend auf einem in der vordefinierten Rolle nicht vorhandenen Filter. Diese vordefinierte Rolle wurde eventuell verschiedenen Richtlinien als Identität hinzugefügt. Wenn eine Richtlinie so konfiguriert wurde, dass sie für Ihre neue Rolle gilt, fügen Sie die neue Rolle lediglich der vorhandenen Richtlinie hinzu. Falls die Konfiguration es erfordert, dass Sie den Typ, die Ressourcen, die Aktionen oder die Filter ändern, können Sie aus der Kopie der vorhandenen Richtlinie eine neue Richtlinie erstellen.

In diesem Beispiel werden Ihnen die einzelnen Schritte beim Erstellen einer Rolle für einen Analysten erläutert, der nur mit Berichten arbeiten soll, die eine Kennung "PCI" aufweisen. Die zugehörige Richtlinie für diese Rolle wird aus einer Kopie einer vorhandenen Richtlinie für alle Analysten erstellt.

Der Prozess umfasst die folgenden Schritte:

1. Planen Sie die Richtlinien, die Sie benötigen. Beginnen Sie mit der Ermittlung der vorhandenen Richtlinien, die Sie für die neue Rolle nutzen möchten.
2. So erstellen Sie die neue Anwendungsbenutzergruppe (Rolle) "PCI-Analyst":
3. Gewähren Sie dem PCI-Analysten grundlegenden Zugriff auf CA Enterprise Log Manager. Fügen Sie diese Identität der CALM-Anwendungszugriffsrichtlinie hinzu.
4. Räumen Sie dem PCI-Analysten denselben Zugriff auf Berichtsserver und dieselbe Berichterstellungsfähigkeit ein, über die Analysten verfügen. Fügen Sie den ermittelten Richtlinien die Identität "PCI-Analyst" hinzu.
5. Beschränken Sie den Berichtszugriff auf die Berichte, die mit dem PCI-Attribut "calmTag" gekennzeichnet sind. Verwenden Sie die Richtlinie, die die Möglichkeit zur Anzeige und Bearbeitung von Berichten gibt, als zu ändernde Vorlage.
6. Weisen Sie die Rolle "PCI-Analyst" zur Auswertung einem Testbenutzer zu.
7. Melden Sie sich als Testbenutzer an, und werten Sie den Zugriff aus.

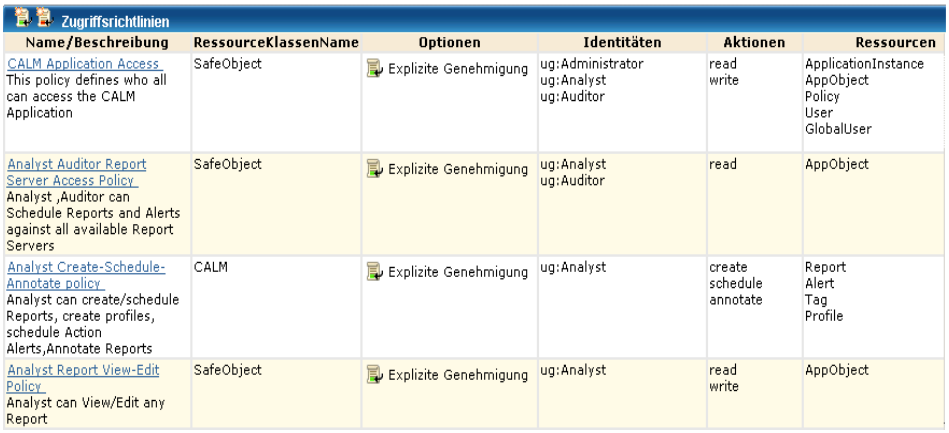
   Falls der durch die Rolle und die Richtlinien zulässige Zugriff Ihren Erwartungen entspricht, weisen Sie die Rolle allen Personen zu, die PCI-Berichte analysieren sollen.

Schritt 1: Planen der zu erstellenden Rolle und Richtlinien

Angenommen, Sie möchten eine Rolle erstellen, die Analysten ähnelt, deren Zugriff jedoch auf PCI-relevante Berichte und Abfragen beschränkt ist. Planen Sie einen Namen für die Rolle, durch den ihre Funktion beschrieben wird, beispielsweise "PCI-Analyst".

Bevor Sie mit der Erstellung neuer Rollen oder Anwendungsbenutzergruppen beginnen, denken Sie darüber nach, welche Richtlinien zur Unterstützung der neuen Rolle erforderlich sind. Es empfiehlt sich, zunächst vorhandene Richtlinien zu ermitteln, die als Vorlagen dienen könnten. Suchen Sie unter "Identitäten" nach einer Rolle, die der von Ihnen geplanten Rolle ähnelt.

In diesem Beispielszenario handelt es sich dabei um die Rolle "ug:Analyst". Aktivieren Sie unter "Suchrichtlinien" die Option "Richtlinien mit zutreffender Identität anzeigen". Geben Sie die Identität **ug:Analyst** ein, und klicken Sie auf "Los". Zu den angezeigten Richtlinien zählen die Richtlinien für "Alle Identitäten" und diejenigen Richtlinien, bei denen unter "Identitäten" explizit "ug:Analyst" genannt ist.



Zugriffsrichtlinien

Name/Beschreibung	RessourceKlassenName	Optionen	Identitäten	Aktionen	Ressourcen
CALM Application Access This policy defines who all can access the CALM Application	SafeObject	Explizite Genehmigung	ug:Administrator ug:Analyst ug:Auditor	read write	ApplicationInstance AppObject Policy User GlobalUser
Analyst Auditor Report Server Access Policy Analyst ,Auditor can Schedule Reports and Alerts against all available Report Servers	SafeObject	Explizite Genehmigung	ug:Analyst ug:Auditor	read	AppObject
Analyst Create-Schedule-Annotate policy Analyst can create/schedule Reports, create profiles, schedule Action Alerts,Annotate Reports	CALM	Explizite Genehmigung	ug:Analyst	create schedule annotate	Report Alert Tag Profile
Analyst Report View-Edit Policy Analyst can View/Edit any Report	SafeObject	Explizite Genehmigung	ug:Analyst	read write	AppObject

Im Folgenden finden Sie die Richtliniennamen, die diese Rolle einschließen:

- Unter "Bereichsrichtlinien": CALM-Anwendungszugriffsrichtlinie
- Unter "Bereichsrichtlinien": Richtlinie für den Zugriff auf den Berichtsserver durch Analysten und Auditoren
- Unter "Bereichsrichtlinien": Richtlinie zum Anzeigen und Bearbeiten von Berichten durch Analysten
- Unter "CALM": Richtlinie zum Erstellen, Planen und Anmerken durch Analysten

Untersuchen Sie für jeden einzelnen Richtlinienkandidaten die Definition, und bestimmen Sie, welche der folgenden Aktionen auszuführen sind:

- Neue Rolle als Identität hinzufügen, für die diese Richtlinie gilt. Dies ist die beste Wahl, wenn die Richtlinie ohne Änderung auf die neue Rolle angewendet werden kann.

  Diese Aktion ist für folgende Richtlinien in diesem Beispiel geeignet:

  - CALM-Anwendungszugriffsrichtlinie, durch die alle Identitäten definiert werden, die auf CA Enterprise Log Manager zugreifen können
  - Richtlinie für den Zugriff auf den Berichtsserver durch Analysten und Auditoren, durch die alle Identitäten definiert werden, die Berichte und Alarme anhand aller verfügbaren Berichtsserver planen können. Für diese Rolle ist auf Berichtsservern keine Beschränkung erforderlich.
  - Richtlinie zum Erstellen, Planen und Anmerken durch Analysten

- Speichern Sie die Richtlinie unter einem neuen Namen, und ändern Sie ihre Definition.

  Diese Aktion eignet sich für folgende Richtlinie in diesem Beispiel, wobei die neue Ausfertigung nur die neue Identität einschließen und über einen zusätzlichen Filter verfügen würde, mit dem der Lese-/Schreibzugriff auf Berichte mit der Kennung "PCI" beschränkt wird:

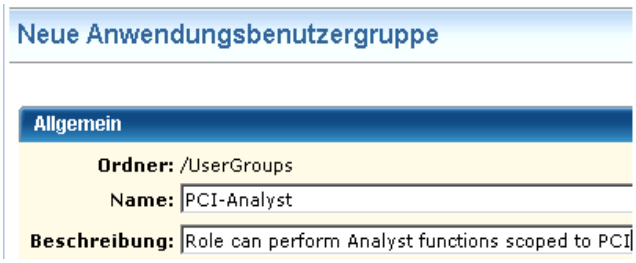
  - Richtlinie zum Anzeigen und Bearbeiten von Berichten durch Analysten

Schritt 2: Erstellen der Rolle "PCI-Analyst"

Sie können eine benutzerdefinierte Rolle erstellen, durch die eine beliebige Aufgabe dargestellt wird, die mehrere Benutzer mit der CA Enterprise Log Manager-Anwendung ausführen. Eine Rolle ist mit einer Anwendungsbenutzergruppe identisch.

Den ersten Schritt des Prozesses zur Beschränkung des Zugriffs für eine Rolle bildet die Erstellung der Rolle.

Wenn Sie eine benutzerdefinierte Rolle erstellen, bei der es sich um keine Übermenge einer bestehenden Rolle handelt, treffen Sie unter "Verfügbare Benutzergruppen" keine Auswahl.



Weitere Informationen:

Erstellen einer Anwendungsbenutzergruppe (Rolle) (siehe Seite 96)

Schritt 3: Hinzufügen des Benutzers "PCI-Analyst" zur CALM-Anwendungszugriffsrichtlinie

Nachdem Sie eine neue Rolle erstellt haben, gewähren Sie dieser Rolle im nächsten Schritt die grundlegende Möglichkeit zur Anmeldung bei der CA Enterprise Log Manager-Anwendung. Standardmäßig verfügen nur die vordefinierten Rollen über Anmeldezugriff. Fügen Sie der CALM-Anwendungszugriffsrichtlinie diese Anwendungsgruppe hinzu.

Weitere Informationen:

Gewähren des Zugriffs auf CA Enterprise Log Manager für eine benutzerdefinierte Rolle (siehe Seite 98)

Schritt 4: Hinzufügen des Benutzers "PCI-Analyst" zu vorhandenen Richtlinien

Sobald Sie die Richtlinien ermittelt haben, die für eine Anwendungsbenutzergruppe gelten, bei der die neue Rolle eine Teilmenge darstellt, fügen Sie die neue Rolle der aktuellen Liste der Identitäten hinzu.

Für dieses Szenario fügen Sie die Rolle "PCI-Analyst" den folgenden vorhandenen Richtlinien hinzu:

- Richtlinie für den Zugriff auf den Berichtsserver durch Analysten und Auditoren
- Richtlinie zum Erstellen, Planen und Anmerken durch Analysten

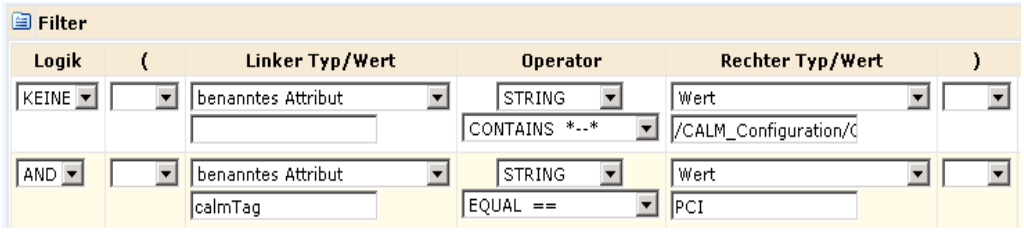
Weitere Informationen:

Hinzufügen einer Identität zu einer vorhandenen Richtlinie (siehe Seite 99)

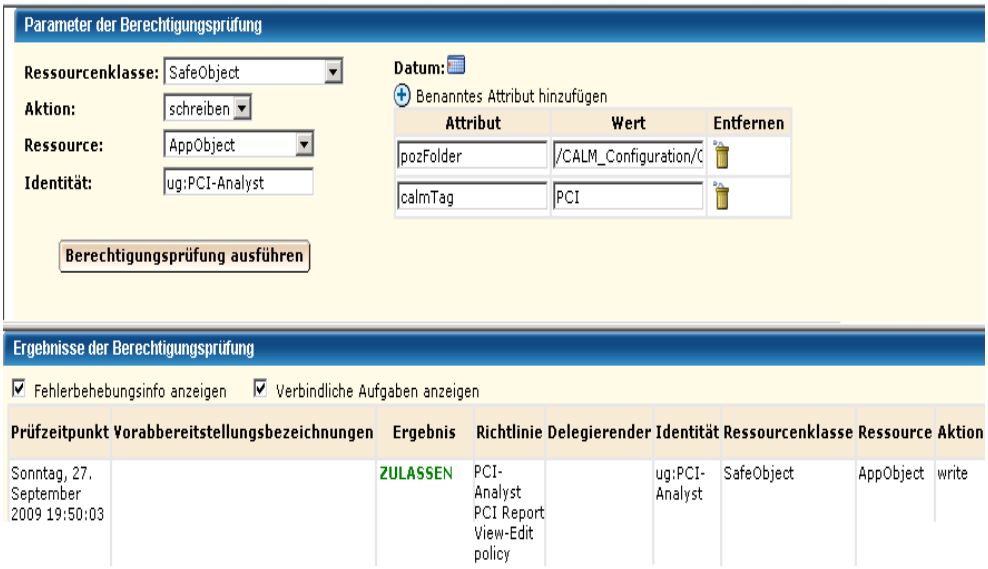
Schritt 5: Erstellen einer Richtlinie auf der Basis der Richtlinie zum Anzeigen und Bearbeiten von Berichten durch Analysten

Wenn Sie eine Richtlinie basierend auf einer vorhandenen Richtlinie erstellen, können Sie die vorhandene Richtlinie kopieren und unter einem neuen Namen speichern. Anschließend benennen Sie diese um, bearbeiten die Beschreibung so, dass sie der neuen Rolle entspricht, und ersetzen die vorhandenen Identitäten durch Ihre neue Identität. Wenn die Richtlinie, die Ihnen als Vorlage dient, einen für die neue Rolle zu umfassenden Zugriff ermöglicht, erstellen Sie Filter, um den Zugriff zu beschränken.

Für das Szenario des PCI-Analysten kopieren Sie die Richtlinie zum Anzeigen und Bearbeiten von Berichten durch Analysten, speichern sie unter einem neuen Namen und ersetzen die Identität durch die Gruppe "PCI-Analyst". Fügen Sie ihr dann einen Filter hinzu, um den Berichtszugriff auf die Berichte zu beschränken, die mit dem PCI-Attribut "calmTag" gekennzeichnet sind.



Es empfiehlt sich, eine auf einer vorhandenen Richtlinie basierende Richtlinie genauso zu testen, als hätten Sie sie von Grund auf neu erstellt. Wenn Sie eine Richtlinie mit einem Filter testen, achten Sie darauf, dass Sie den Filter genau so eingeben, wie er in der Richtlinie angegeben ist. Denken Sie bei der Eingabe eines Gruppennamens für die Identität daran, dass Sie diesem das Präfix "ug:" voranstellen, beispielsweise "ug:PCI-Analyst".



Weitere Informationen:

Erstellen einer Richtlinie auf der Grundlage einer vorhandenen Richtlinie (siehe Seite 108)
Testen von neuen Richtlinien (siehe Seite 110)

Schritt 6: Zuweisen der Rolle "PCI-Analyst" zu einem Benutzer

Nachdem Sie eine neue Rolle und deren unterstützende Richtlinien erstellt haben, sollten Sie sich als Benutzer anmelden, dem nur diese Rolle zugewiesen ist, um auszuwerten, ob ihm der benötigte Zugriff ermöglicht wird. Nach dieser Überprüfung kann die neue Rolle den Konten sämtlicher Benutzer hinzugefügt werden, die die Aufgaben ausführen sollen, für die diese Rolle entworfen wurde.

Sie können zum Testen einer neuen Rolle ein temporäres Benutzerkonto erstellen und dieses nach Abschluss der Tests wieder löschen. Alternativ können Sie einen Benutzer namens "Testbenutzer" erstellen und die Rollenzuweisung bei jeder Wiederverwendung ersetzen.

Weitere Informationen:

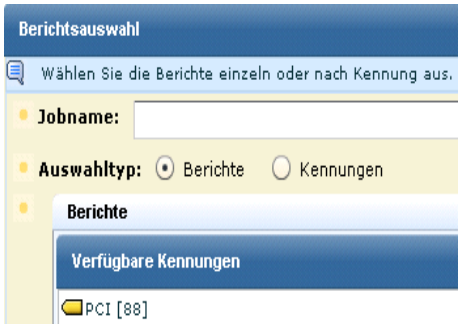
Zuweisen einer Rolle zu einem globalen Benutzer (siehe Seite 44)

Schritt 7: Anmelden als Benutzer "PCI-Analyst" und Bewerten des Zugriffs

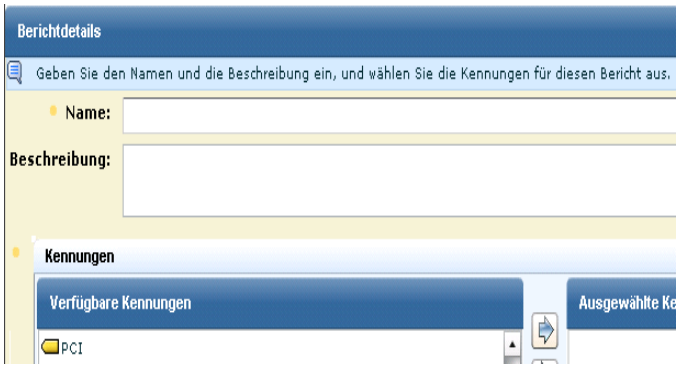
Überprüfen Sie, ob die Richtlinien ausreichen, um den Zugriff auf Berichte und Alarme zu beschränken, die mit "PCI" gekennzeichnet sind. Weisen Sie die Rolle "PCI-Analyst" einem Benutzer zu, und melden Sie sich als dieser neue Benutzer bei CA Enterprise Log Manager an-

Zeigen Sie Berichtskennungen an. Überprüfen Sie, ob Sie nur Berichte anzeigen können, die die Kennung "PCI" aufweisen.

Planen Sie einen Bericht. Überprüfen Sie, ob Sie nur Berichte planen können, die die Kennung "PCI" aufweisen.



Erstellen Sie einen Bericht. Überprüfen Sie, ob "PCI" als einzige Kennung für den neuen Bericht verfügbar ist.



Beispielrichtlinien für benutzerdefinierte Integrationen

Sie können Nicht-Administratoren die Möglichkeit einräumen, benutzerdefinierte Integrationen zu erstellen, indem Sie eine benutzerdefinierte Rolle, eine CALM-Richtlinie und eine Bereichsrichtlinie erstellen. Sie können weiteren Nicht-Administratoren die Möglichkeit einräumen, benutzerdefinierte Integrationen anzuzeigen, indem Sie eine zusätzliche benutzerdefinierte Rolle mit einer zugehörigen Bereichsrichtlinie erstellen. Diese beiden benutzerdefinierten Rollen fügen Sie der CALM-Anwendungszugriffsrichtlinie hinzu und weisen diesen Rollen Benutzer zu.

In den folgenden Beispielverfahren wird gezeigt, wie Sie dabei vorgehen:

1. Erstellen Sie eine Anwendungsbenutzergruppe mit der Bezeichnung "DM-XMP-Dateien-Erstellen".
2. Erstellen Sie eine Anwendungsbenutzergruppe mit der Bezeichnung "DM-XMP-Dateien-Anzeigen".
3. Gewähren Sie "DM-XMP-Dateien-Erstellen" und "DM-XMP-Dateien-Anzeigen" Zugriff auf das CA Enterprise Log Manager-Produkt.

Name/Beschreibung	RessourceKlassenName	Identitäten	Aktionen	Ressourcen
CALM Application Access This policy defines who all can access the CALM Application	SafeObject	ug:Administrator ug:Analyst ug:Auditor ug:Create-DM-XMP-Files ug:View-DM-XMP-Files	read write	ApplicationInstance Policy User GlobalUser

4. Erstellen Sie eine CALM-Richtlinie, mit der "DM-XMP-Dateien-Erstellen" die Möglichkeit eingeräumt wird, Datenzuordnungsdateien und Meldungsanalysedateien mit Hilfe von ELM-Schemadefinitionen zu erstellen, solange sie bei CA Enterprise Log Manager angemeldet sind.

Name/Beschreibung	RessourceKlassenName	Identitäten	Aktionen	Ressourcen
Integration-Create policy Can create data mapping and message parsing files using common event grammar.	CALM	ug:Create-DM-XMP-Files	create	Integration

5. Erstellen Sie eine Bereichsrichtlinie, mit der "DM-XMP-Dateien-Erstellen" die Möglichkeit eingeräumt wird, die benutzerdefinierten DM-Dateien und die XMP-Datei mit Hilfe von ELM-Schemadefinitionen zu bearbeiten und anzuzeigen, die im EEM-Ordner "/CALM_Configuration/Content/Mapping" oder "/CALM_Configuration/Content/Parsing" gespeichert sind.

Name/Beschreibung	RessourceKlassenName	Identitäten	Aktionen	Ressourcen
Edit-DM-XMP-Files with CEG Policy Can edit data mapping files and message pasing files using common event grammar saved to the EEM folders /CALM_Configuration/Content/...	SafeObject	ug:Create-DM-XMP-Files	read write	AppObject

Filter		
WHERE	name:pozFolder *--*	val:/CALM_Configuration/Content/Mapping
OR	name:pozFolder *--*	val:/CALM_Configuration/Content/Parsing

6. Erstellen Sie eine Bereichsrichtlinie, mit der "DM-XMP-Dateien-Erstellen" die Möglichkeit eingeräumt wird, die benutzerdefinierten DM-Dateien und die XMP-Datei anzuzeigen, die im EEM-Ordner "/CALM_Configuration/Content/Mapping" oder "/CALM_Configuration/Content/Parsing" gespeichert sind.

   Hinweis Die CEG-Richtlinie gewährt allen Identitäten das Recht, die ELM-Schemadefinitionen einzusehen.

Name/Beschreibung	RessourceKlassenName	Identitäten	Aktionen	Ressourcen
View-DM-XMP-Files Can view data mapping files and message parsing files.	SafeObject	ug:View-DM-XMP-Files	read	AppObject

Filter
WHERE (name:pozFolder *--* val:/CALM_Configuration/Content/Mapping **OR** name:pozFolder *--* val:/CALM_Configuration/Content/Parsing)

7. Testen Sie die Richtlinien.
8. Weisen Sie sowohl "DM-XMP-Dateien-Erstellen" als auch "DM-XMP-Dateien-Anzeigen" Benutzer zu.

Beispielrichtlinien für Unterdrückungs- und Zusammenfassungsregeln

Sie können Nicht-Administratoren autorisieren, benutzerdefinierte Unterdrückungs- und Zusammenfassungsregeln zu erstellen, indem Sie eine benutzerdefinierte Rolle, eine CALM-Richtlinie und eine Bereichsrichtlinie erstellen. Sie können weiteren Nicht-Administratoren die Möglichkeit einräumen, benutzerdefinierte Unterdrückungs- und Zusammenfassungsregeln anzuzeigen, indem Sie eine zusätzliche benutzerdefinierte Rolle mit einer zugehörigen Bereichsrichtlinie erstellen. Diese beiden benutzerdefinierten Rollen fügen Sie der CALM-Anwendungszugriffsrichtlinie hinzu und weisen diesen Rollen Benutzer zu.

In dem folgenden Beispielverfahren wird gezeigt, wie Sie dabei vorgehen:

1. Erstellen Sie eine Anwendungsbenutzergruppe mit der Bezeichnung "SUP-SUM-Regeln-Erstellen".
2. Erstellen Sie eine Anwendungsbenutzergruppe mit der Bezeichnung "SUP-SUM-Regeln-Anzeigen".
3. Gewähren Sie beiden Rollen Zugriff auf das CA Enterprise Log Manager-Produkt.

Name/Beschreibung	RessourceKlassenName	Identitäten	Aktionen	Ressourcen
CALM Application Access This policy defines who all can access the CALM Application	SafeObject	ug:Administrator ug:Analyst ug:Auditor ug:Create-Sup-Sum-Rules ug:View-Sup-Sum-Rules	read write	ApplicationInstance Policy User GlobalUser

4. Erstellen Sie eine CALM-Richtlinie, mit der "SUP-SUM-Regeln-Erstellen"-Benutzern die Möglichkeit eingeräumt wird, Unterdrückungs- und Zusammenfassungsregeln zu erstellen oder zu importieren, solange sie bei CA Enterprise Log Manager angemeldet sind.

Name/Beschreibung	RessourceKlassenName	Optionen	Identitäten	Aktionen	Ressourcen
EventGroup-Create policy Can create custom summarization and suppressionrules or import rules.	CALM	Explizite Genehmigung	ug:Create-Sup-Sum-Rules	create	EventGrouping

5. Erstellen Sie eine Bereichsrichtlinie, mit der "SUP-SUM-Regeln-Erstellen"-Benutzern die Möglichkeit eingeräumt wird, benutzerdefinierte Unterdrückungs- und Zusammenfassungsregeln zu bearbeiten und anzuzeigen, die im EEM-Ordner "/CALM_Configuration/Content/Rules/Suppression" oder "/CALM_Configuration/Content/Rules/Summarization" gespeichert sind.

Name/Beschreibung	RessourceKlassenName	Identitäten	Aktionen	Ressourcen
View-Edit-SUP-SUM-Rules Can view or edit suppression and summarization rules that have been saved to Content/Rules/Summarization or Content/Rules Suppression folders.	SafeObject	ug:Create-Sup-Sum-Rules	read write	AppObject

Filter			
WHERE	name:pozFolder	*--*	val:/CALM_Configuration/Content/Rules/Summarization
OR	val:pozFolder	*--*	val:/CALM_Configuration/Content/Rules/Suppression

6. Erstellen Sie eine Bereichsrichtlinie, mit der "SUP-SUM-Regeln-Anzeigen"-Benutzern die Möglichkeit eingeräumt wird, benutzerdefinierte Unterdrückungs- und Zusammenfassungsregeln anzuzeigen.

Name/Beschreibung	RessourceKlassenName	Identitäten	Aktionen	Ressourcen
View-SUP-SUM-Rules Can view suppression and summarization rules that have been saved to Content/Rules/Summarization or Content/Rules Suppression folders.	SafeObject	ug:View-Sup-Sum-Rules	read	AppObject

Filter			
WHERE	name:pozFolder	*--*	val:/CALM_Configuration/Content/Rules/Summarization
OR	val:pozFolder	*--*	val:/CALM_Configuration/Content/Rules/Suppression

7. Testen Sie die Richtlinien
8. Weisen Sie den neuen Rollen Benutzer zu. Z. B. möchten externe Auditoren vielleicht die Möglichkeit haben, Ihre Unterdrückungs- und Zusammenfassungsregeln anzuzeigen. Um dies zu gestatten, könnten Sie solchen Benutzern eine Rolle ähnlich wie "SUP-SUM-Regeln-Anzeigen" zuweisen.

Eine Alternative zur Erstellung zweier neuer Rollen ausdrücklich für die Aufgaben "Erstellen/Bearbeiten/Anzeigen" wäre es, die vordefinierten Rollen "Analyst" und "Auditor" zu erweitern. Z. B. könnten Sie die Schritte 1, 2, 3 und 8 des zuvor beschriebenen Verfahrens weglassen und stattdessen "Analyst" als Identität der Richtlinie "EreignisGruppierung erstellen" und "SUP-SUM-Regeln-Anzeigen" zuweisen bzw. die Benutzergruppe "Auditor" als Identität zu "SUP-SUM-Regeln-Anzeigen" hinzufügen.

Weitere Informationen:

Erstellen einer Anwendungsbenutzergruppe (Rolle) (siehe Seite 96)
Gewähren des Zugriffs auf CA Enterprise Log Manager für eine benutzerdefinierte Rolle (siehe Seite 98)
Testen von neuen Richtlinien (siehe Seite 110)
Zuweisen einer Rolle zu einem globalen Benutzer (siehe Seite 44)

Kapitel 5: Services und CA-Adapter

Dieses Kapitel enthält folgende Themen:

Service-Aufgaben

Sie können globale Konfigurationen festlegen, die für alle CA Enterprise Log Manager-Server gelten. Es gibt zwei Arten individueller Service-Konfigurationen, die Sie anzeigen und bearbeiten können: Globale Service-Konfigurationen gelten für alle Instanzen eines Einzelservice in der Umgebung. Lokale Service-Konfigurationen gelten nur für einen bestimmten ausgewählten Service-Host.

Hinweis: Globale Konfigurationen unterscheiden sich von globalen *Service*-Konfigurationen insofern, als dass erstere die Funktionsweise aller CA Enterprise Log Manager-Server steuern, während zweitere nur die Funktionsweise eines ausgewählten Service beeinflussen. Beispielsweise können Sie das Aktualisierungsintervall aller Services (globale Konfiguration) oder Richtlinien zur Berichtsaufbewahrung für alle Berichtsserver (globale Service-Konfiguration) festlegen.

Zudem können Sie über die Bereiche für die Service-Konfiguration selbstüberwachende Ereignisse anzeigen.

Zu den verfügbaren Services gehören:

- Agenten-Manager
- Alarm-Service
- Korrelationsservice
- Ereignisprotokollspeicher
- Incident-Service
- ODBC-Server
- Dienst abfragen
- Berichtsserver
- Regeltestservice
- Automatisches Software-Update - Service
- Systemstatus

Einige Services können Sie wahlweise nach Namen oder Hosts anzeigen. Sie können den Systemstatus-Dienst verwenden, um Informationen über einen einzelnen CA Enterprise Log Manager-Server einzuholen und ihn zu steuern.

Weitere Informationen:

Bearbeiten einer globalen Service-Konfiguration (siehe Seite 159)
Bearbeiten lokaler Service-Konfigurationen (siehe Seite 160)

Löschen von Service-Hosts

Wenn Sie einen CA Enterprise Log Manager-Server deinstallieren, müssen Sie die Hostkonfiguration aus dem Management-Server-Repository löschen. Durch das Löschen dieses Verweises bleibt der Server mit der Liste seiner registrierten CA Enterprise Log Manager-Server aktuell.

So löschen Sie einen Service-Host:

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

   Die Service-Liste wird angezeigt.

2. Klicken Sie im Dialogfeld "Service anzeigen nach" oben in der Liste auf "Host".

   Eine erweiterbare Strukturliste mit Service-Hosts wird angezeigt.

3. Wählen Sie den Host aus, den Sie löschen möchten, und klicken Sie auf "Löschen".

   Der Host wird aus der Liste entfernt.

Wichtig! Beim Löschen eines Hosts wird keine Warnung angezeigt. Wenn Sie auf "Löschen" klicken, wird der Host sofort gelöscht. Sie müssen daher sicher sein, dass Sie den Host wirklich löschen möchten.

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: 600

   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: 60

Automatische Aktualisierung aktivieren

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 Unterregisterkarte "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 Dashboard-Einstellungen können geändert werden:

   Start des Standard-Dashboards aktivieren

   Zeigt das Standard-Dashboard an, wenn Sie auf die Registerkarten "Abfragen" und "Berichte" klicken. Diese Einstellung ist standardmäßig aktiviert.

   Standard-Dashboard

6. 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.

7. Klicken Sie auf "Speichern".

Bearbeiten einer globalen Service-Konfiguration

Globale Service-Konfigurationen sind Einstellungen, die sich auf alle Instanzen eines bestimmten Service in Ihrer Umgebung beziehen. Mit einer globalen Service-Konfiguration werden *keine* lokalen Service-Einstellungen, die sich von den globalen Einstellungen unterscheiden, überschrieben.

Die maximalen und minimalen Konfigurationswerte werden in den einzelnen Service-Abschnitten ausführlich erläutert. Beim Versuch, Werte außerhalb des zulässigen Bereichs zu speichern, wird CA Enterprise Log Manager standardmäßig je nachdem auf den minimalen oder maximalen Wert gesetzt.

So bearbeiten Sie eine globale Service-Konfiguration:

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

   Die Service-Liste wird angezeigt.

2. Wählen Sie den Service aus, dessen Konfiguration bearbeitet werden soll.

   Im Detailbereich wird die globale Service-Konfiguration angezeigt.

3. Ändern Sie die Konfiguration wie gewünscht.

   Hinweis: Mit "Zurücksetzen" können Sie die Eingabefelder auf den zuletzt gespeicherten Wert zurücksetzen. Sie können eine einzelne Änderung oder mehrere Änderungen zurücksetzen, bis Sie auf "Speichern" klicken. Nach dem Speichern von Änderungen können Sie diese nur noch einzeln zurücksetzen.

4. Klicken Sie auf "Speichern", wenn Sie die Änderungen abgeschlossen haben.

   Sämtliche Konfigurationsänderungen werden auf alle Hosts des ausgewählten Service angewendet, es sei denn, sie haben andere lokale Einstellungen.

Bearbeiten lokaler Service-Konfigurationen

Lokale Service-Konfigurationen können nach Service- oder Hostserver angezeigt oder bearbeitet werden. Mit Hilfe einer lokalen Service-Konfiguration können Sie Services oder Einstellungen steuern, die nicht für die gesamte Umgebung gelten oder erforderlich sind und somit globale Einstellungen nur für bestimmte Hosts überschreiben. Beispielsweise sollen Aktionsalarme auf einem bestimmten CA Enterprise Log Manager-Server länger gespeichert werden als auf den anderen Servern. Hierfür eignet sich eine lokale Konfiguration.

Die maximalen und minimalen Konfigurationswerte werden in den einzelnen Service-Abschnitten ausführlich erläutert. Beim Versuch, Werte außerhalb des zulässigen Bereichs zu speichern, wird CA Enterprise Log Manager standardmäßig je nachdem auf den minimalen oder maximalen Wert gesetzt.

So bearbeiten Sie eine lokale Service-Konfiguration:

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

   Die Service-Liste wird angezeigt.

2. Klicken Sie auf den Pfeil neben dem Service, dessen Konfiguration bearbeitet werden soll.

   Der Service wird erweitert, und alle Service-Hosts werden angezeigt.

3. Klicken Sie auf den gewünschten Service-Host.

   Die ausgewählte Service-Konfiguration wird im Detailfenster angezeigt.

4. Ändern Sie die Konfiguration wie gewünscht. Jedes Eingabefeld, Menü und Steuerelement in der Anzeige der lokalen Konfiguration hat eine Schaltfläche für die lokale/globale Konfiguration. Diese hat zwei Einstellungen.

   Globale Konfiguration: 

   Lokale Konfiguration: 

   Durch Klicken auf die Schaltfläche ändert sich die globale in die lokale Einstellung. Der zugehörige Wert ist nun verfügbar. Damit die Einstellung wirksam wird, muss der Wert für die lokale Konfiguration beibehalten werden. Wird der Wert für die globale Konfiguration eingestellt, ist die globale Einstellung für diesen Listener in Kraft.

Hinweis: Wenn Sie auf "Zurücksetzen" klicken, werden die zuletzt gespeicherten Konfigurationswerte für alle verfügbaren Konfigurationen angezeigt. Sie können eine einzelne Änderung oder mehrere Änderungen zurücksetzen, bis Sie auf "Speichern" klicken. Nach dem Speichern von Änderungen können Sie diese nur noch einzeln zurücksetzen.

5. Klicken Sie auf "Speichern", wenn Sie die Änderungen abgeschlossen haben.

   Sämtliche Änderungen werden nur für den ausgewählten Service-Host übernommen.

Service-Konfigurationen

Dieser Abschnitt enthält Informationen und Richtlinien zur Durchführung von Konfigurationsänderungen an folgenden CA Enterprise Log Manager-Services:

- Alarm-Service: steuert Lieferungseinstellungen für Aktionsalarme, einschließlich SMTP-Server, CA IT PAM- und SNMP-Trap-Einstellungen.
- Korrelationsservice: steuert Korrelationsregeln und das Routing von Ereignissen für die Erstellung von Incidents.
- Ereignisprotokollspeicher: speichert alle verfeinerten und aufgezeichneten Rohereignisse.
- Incidents-Service: steuert die Erstellung und Speicherung von durch Ereigniskorrelation entstandenen Incidents.
- ODBC-Server: bietet Zugriff auf den CA Enterprise Log Manager-Ereignisprotokollspeicher von einer externen Anwendung wie beispielsweise BusinessObjects Crystal Reports.
- Berichtsserver: regelt die Verteilung, Formatierung und Aufbewahrung von Berichten und Alarmen.
- Automatisches Software-Update - Service: leitet Inhalts- und Konfigurationsaktualisierungen an den Verwaltungsserver und binäre Aktualisierungen an Software-Update-Clients weiter.

Weitere Informationen:

Abonnement (siehe Seite 243)

Hinweise zum Alarm-Service

Der Alarm-Service steuert die Lieferung von Aktionsalarmen. Folgende Aufgaben können im Bereich der Konfiguration des Alarm-Service erledigt werden:

- Festlegen des Mail-Servers, der Admin-E-Mail-Adresse, des SMTP-Port und der Authentifizierungsinformationen für die Lieferung von Alarmen im Bereich "E-Mail-Einstellungen".
- Konfigurieren der CA IT PAM-Integration für Aktionsalarme.
- Konfigurieren der ObserveIT-Integration.
- Festlegen von SNMP-Traps für die Lieferung von Aktionsalarmen.

Weitere Informationen:

Konfigurieren Sie CA Enterprise Log Manager für das Funktionieren mit ObserveIT. (siehe Seite 166)
Konfigurieren der Integration mit einem SNMP Trap-Ziel (siehe Seite 168)

Konfigurieren der CA IT PAM-Integration

Sie können die CA IT PAM-Integration so konfigurieren, dass einer oder auch beide der folgenden CA IT PAM-Prozesstypen genutzt werden können:

- Ereignis-/Alarmausgabeprozess: Ein Prozess, der die Verarbeitung auf einem Drittanbietersystem auslöst
- Prozess mit dynamischen Werten: Ein Prozess, der einen Eingabeschlüssel akzeptiert und aktuelle Werte für diesen Schlüssel in einer kommagetrennten Datei (*.csv) zurückgibt

Folgender Vorgang betrifft beide allgemeinen Einstellungen.

So konfigurieren Sie die IT PAM-Integration

1. Klicken Sie auf die Registerkarte "Verwaltung" und auf die Unterregisterkarte "Services".
2. Klicken Sie auf "Alarm-Service".

   Das Dialogfeld "Globale Service-Konfiguration: Alarm-Service" wird angezeigt.

3. Blättern Sie zum Bereich "IT PAM".
4. Geben Sie den vollqualifizierten Hostnamen des Servers an, auf dem CA IT PAM installiert ist, akzeptieren Sie die Standard-Portnummer 8080, und geben Sie gültige Anmeldeinformationen für CA IT PAM ein.
5. Gehen Sie für den Ereignis-/Alarmausgabeprozess im Abschnitt "Ereignis-/Alarmausgabeprozess" wie folgt vor:
   a. Wenn Sie die importierte Beispieldatei "EventAlertOutput.xml" verwenden, akzeptieren Sie den Standardeintrag für den Ereignis-/Alarmausgabeprozess. Andernfalls ersetzen Sie diesen Eintrag mit dem Namen Ihres eigenen Ereignis-/Alarmausgabeprozesses und seinem Pfad.

      Hinweis: Name und Pfad des Prozesses werden unter "Folders" (Ordner) im ITPAM-Client angezeigt.

   b. Falls Sie die Beispieldatei "EventAlertOutput.xml" importiert haben, definieren Sie die Standardwerte für "ReportedBy" (Gemeldet von), "Severity" (Schweregrad), "Priority" (Priorität) und "EndUser" (Endbenutzer) wie folgt:
      a. Wählen Sie einen Parameter aus, und klicken Sie auf "Standardwert hinzufügen".

         Das Dialogfeld "Wert hinzufügen" wird angezeigt.

      b. Geben Sie den Standardwert ein, und klicken Sie auf "OK".

   c. Falls Sie Ihren eigenen Ereignis-/Alarmausgabeprozess angegeben haben, löschen Sie die angezeigten Parameter und fügen Ihre eigenen hinzu. Definieren Sie dann für jeden Parameter den Standardwert.

6. Gehen Sie bei der geplanten Aktualisierung der Schlüsselliste im Abschnitt "Aktualisierung der Schlüsselliste" wie folgt vor:
   a. Wählen Sie den Server aus, der die Schlüsselliste anhand der Liste "Standardserver" aktualisiert.
   b. Wählen Sie die Option "Aktiviert" aus.

      Die Parameter, die für das Festlegen eines Ablaufplans erforderlich sind, werden angezeigt.
   c. Wählen Sie die Zeitzone und die Startzeit aus, zu der der Aktualisierungsplaner ausgeführt wird.
   d. Wählen Sie die Wiederholungsfrequenz des Aktualisierungsplaners aus und geben Sie die erforderlichen Details an.
7. Klicken Sie auf "Speichern".

   Es wird die folgende Bestätigungsmeldung angezeigt: "Die Konfigurationsänderungen wurden erfolgreich gespeichert." Die IT PAM-Integration ist nun konfiguriert.

Weitere Informationen:

Erstellen einer Liste mit Schlüssel (siehe Seite 372)

ObserveIT-Integration

Sie können CA Enterprise Log Manager mit ObserveIT integrieren, um die Aufzeichnung von Benutzersitzungen zu untersuchen.

Mit ObserveIT haben Sie folgende Möglichkeiten:

- Überwachen der Konfigurationsaktivitäten aller Benutzer
- Überwachen aller verdächtigen Benutzeraktivitäten
- Generieren von Berichten zu allen Benutzeraktivitäten

Sie können entweder eine einzelne Instanz oder mehrere Instanzen von ObserveIT verwenden.

Hinweis: Weitere Informationen zum Überwachen von Benutzeraktivitäten finden Sie in der Dokumentation von ObserveIT.

Weitere Informationen:

Hinweise zur Integration (siehe Seite 165)
Konfigurieren Sie CA Enterprise Log Manager für das Funktionieren mit ObserveIT. (siehe Seite 166)
Anzeigen der Aufzeichnung einer Benutzersitzung (siehe Seite 167)

Integrieren von CA Enterprise Log Manager mit ObserveIT

Dieses Thema stellt eine Übersicht über die Schritte dar, die Sie als Administrator ausführen müssen, um CA Enterprise Log Manager mit ObserveIT zu integrieren.

Führen Sie folgende Schritte durch, um CA Enterprise Log Manager mit ObserveIT zu integrieren:

- Konfigurieren Sie CA Enterprise Log Manager für das Funktionieren mit ObserveIT.
- Zeigen Sie die Aufzeichnung einer Benutzersitzung an.

Hinweise zur Integration

CA Enterprise Log Manager unterstützt die Integration mit ObserveIT 5.2.5.1. Bevor Sie CA Enterprise Log Manager mit ObserveIT integrieren, gehen Sie wie folgt vor:

- Stellen Sie sicher, dass Sie den ObserveIT-Server installiert haben.
- Wenn Sie die Aufzeichnung von Benutzersitzungen von mehreren Instanzen von ObserveIT untersuchen wollen, stellen Sie sicher, dass Sie den zentralisierten ObserveIT-Verwaltungsserver installiert haben.
- Wenn Sie ObserveIT-Protokolle von einer Ereignisquelle erfassen wollen, stellen Sie sicher, dass Sie einen ObserveIT-Connector für jede ObserveIT-Datenbank auf der Ereignisquelle bereitgestellt haben. Weitere Informationen zum ObserveIT-Connector finden Sie im *Connector-Handbuch für ObserveIT*.

Hinweis: Weitere Informationen zur Installation von ObserveIT finden Sie in der Dokumentation zu ObserveIT.

Konfigurieren Sie CA Enterprise Log Manager für das Funktionieren mit ObserveIT.

CA Enterprise Log Manager arbeitet mit ObserveIT, damit Sie die Aufzeichnung einer Benutzersitzung anzeigen können. Um CA Enterprise Log Manager mit ObserveIT zu integrieren, müssen Sie den ObserveIT-Server über die CA Enterprise Log Manager-Schnittstelle konfigurieren.

So konfigurieren Sie CA Enterprise Log Manager so, dass es mit ObserveIT arbeitet

1. Klicken Sie auf "Verwaltung", "Service" und "Alarm-Service".

   Das Fenster "Globale Service-Konfiguration: Alarm-Service" wird angezeigt. Standardmäßig öffnet sich die Registerkarte "Verwaltung".

   Hinweis: Sie können einen individuellen CA Enterprise Log Manager-Server so konfigurieren, dass er auf einer lokalen Konfigurationsebene mit ObserveIT arbeitet.

2. Füllen Sie folgende Felder im Bereich ObserveIT entsprechend aus, und klicken Sie auf "Speichern":

   ObserveIT-Server-URL

   Legt die Adresse des ObserveIT-Servers fest.

   Hinweis: Wenn Sie eine einzelne Instanz von ObserveIT verwenden, müssen Sie die Adresse des einzelnen ObserveIT-Servers im folgenden Format angeben:

   `http://observeit_Anwendungsserver:Portnummer_der_Installation_von_ObserveIT/ObserveIT`

   Wenn Sie mehrere Instanzen von ObserveIT verwenden, müssen Sie die Adresse des zentralisierten Verwaltungsservers im folgenden Format angeben:

   `http://observeit_zentralisierter_Verwaltungsserver/ObserveITCentralizedManagement/`

   Benutzername

   Gibt den Benutzernamen des Administrators an, der Zugriff auf den ObserveIT-Server hat.

   Kennwort

   Gibt das Kennwort an, das dem Administrator des ObserveIT-Servers zugeordnet ist.

3. (Optional) Klicken Sie auf "Verbindung testen".

Die Verbindung zum ObserveIT-Server wurde unterbrochen. Wenn die Verbindung erfolgreich ist, wird die Meldung "Verbindungsinformationen für ObserveIT erfolgreich validiert" angezeigt. Der ObserveIT-Anwendungsserver wird über den CA Enterprise Log Manager-Server konfiguriert.

Weitere Informationen:

Hinweise zur Integration (siehe Seite 165)
Anzeigen der Aufzeichnung einer Benutzersitzung (siehe Seite 167)

Anzeigen der Aufzeichnung einer Benutzersitzung

CA Enterprise Log Manager ermöglicht es Ihnen, eine von ObserveIT aufgezeichnete Benutzersitzung anzuzeigen. Sie müssen ein Administrator oder Analyst sein, um die Aufzeichnung einer Benutzersitzung anzeigen zu können. Sie können die Aufzeichnung einer Benutzersitzung anzeigen, wenn Sie den Abfrage-Viewer über CA Enterprise Log Manager-API starten.

So zeigen Sie die Aufzeichnung einer Benutzersitzung an

1. Klicken Sie mit der rechten Maustaste auf ein Ereignis in einem Bericht, und wählen Sie "Host untersuchen mithilfe der Aufzeichnung von Benutzersitzungen" aus.

   Das Dialogfeld "Ereignisse zur Aufzeichnung von ObserveIT-Benutzersitzungen" wird geöffnet. Das Dialogfeld zeigt alle Aufzeichnungen von Benutzersitzungen an, die innerhalb des Zeitraums zwischen dem ausgewählten Ereignis und der aktuellen Zeit verfügbaren sind.

2. Klicken Sie auf das Videosymbol einer Sitzung, die Sie anzeigen möchten.

   Hinweis: Ein Videosymbol ist nur aktiviert, wenn es innerhalb des ausgewählten Zeitraums ein Ereignis gibt.

   Das Fenster "ObserveIT - Slide Viewer" öffnet sich. Die ausgewählte Aufzeichnung der Benutzersitzung wird abgespielt.

Weitere Informationen:

Hinweise zur Integration (siehe Seite 165)
Konfigurieren Sie CA Enterprise Log Manager für das Funktionieren mit ObserveIT. (siehe Seite 166)

Konfigurieren der Integration mit einem SNMP Trap-Ziel

Konfigurieren Sie die SNMP-Integration im Rahmen der Global Service-Konfiguration für den Berichtsserver. Die Konfiguration umfasst die IP-Adresse und den Port eines SNMP-Trap-Ziels.

Sie können die SNMP-Integration entweder vor oder nach der Vorbereitung des Zielprodukts für das Empfangen und Auswerten von SNMP-Traps von CA Enterprise Log Manager konfigurieren.

Wenn Sie einen Alarm für einen SNMP-Trap-Empfänger erstellen, können Sie ein oder mehrere Ziele angeben. Bei dieser Konfiguration handelt es sich um die Standardkonfiguration. Sie gilt für alle Server, die unter "Berichtsserver" aufgelistet werden.

So konfigurieren Sie die SNMP-Integration:

1. Klicken Sie auf die Registerkarte "Verwaltung" und auf die Unterregisterkarte "Services".
2. Klicken Sie auf "Alarm-Service".

   Das Dialogfeld "Globale Service-Konfiguration: Alarm-Service" wird angezeigt.
3. Blättern Sie zum Bereich "SNMP-Konfiguration".
4. Geben Sie die IP-Adresse oder den Hostnamen des Zielservers für die SNMP-Traps ein.
5. Übernehmen Sie den Standardport "162", oder ändern Sie ihn.
6. Klicken Sie auf "Speichern".

Hinweise zum Korrelationsservice

Der Korrelationsservice steuert die auf den Korrelationsserver angewandten Regeln. Wenn Sie eine Regel anwenden, wird sie aktiv.

Sie können Benachrichtigungsziele mit Regeln verbinden, und Regeln von der Konfigurationsseite des Korrelationsservice aus aktivieren oder deaktivieren. Sie können wählen, welche CA Enterprise Log Manager-Server Ereignisse zum ausgewählten Korrelationsserver umlenken, oder eine Ereignisbeschränkung festlegen.

Ereignisbeschränkung

Definiert, wie viele Ereignisse pro Incident beibehalten werden, wenn die Kumulierung aktiviert ist. Die Ereignisbeschränkung verhindert übermäßigen Datenverkehr, der durch die Korrelation in Zeiträumen mit hoher Aktivität verursacht wird. Wenn diese Beschränkung erreicht wird, gehen zusätzliche Ereignisse verloren. Wenn Sie die Beschränkung zum Beispiel auf 100 festgelegt haben, kann eine einzelne Regel bis zu 100 aufgezeichnete Ereignisse umfassen, einschließlich der ursprünglichen, qualifizierenden Ereignisse. Die Kumulierung wird fortgesetzt, bis die Ereignisbeschränkung erreicht wird, oder Lücken- oder Grenzwerte die Regel zurücksetzen, wobei Zweiteres häufiger auftritt.

Sie können auch angewendete Korrelationsregeln entfernen, indem Sie sie deaktivieren.

So entfernen Sie Regeln aus der Liste der angewendeten Regeln

1. Heben Sie die Zeile der Korrelationsregel hervor, die Sie entfernen wollen.
2. (Optional) Sie können Steuerung gedrückt halten und klicken, oder Steuerung und die Umschalttaste drücken, um mehrere Zeilen hervorzuheben.
3. Klicken Sie auf "Entfernen".

   Die hervorgehobenen Regeln werden von der aktiven Liste entfernt.
4. Klicken Sie auf "Speichern", um die Konfiguration zu bestätigen. Wenn Sie nicht gespeichert haben, können Sie auf "Zurücksetzen" klicken, um von der Liste entfernte Regeln wiederherzustellen.

   Hinweis: Diese Prozedur entfernt Korrelationsregeln nur von der aktiven Liste. Sie werden nicht von der Regelbibliothek entfernt.

Hinweise zu Ereignisprotokollspeicher

Der Ereignisprotokollspeicher nutzt ein föderiertes Speichersystem für Ereignisprotokolle. Jeder Hostserver hat einen eigenen lokalen Ereignisprotokollspeicher und kann eine Verbindung zu anderen Ereignisprotokollspeichern der Umgebung herstellen. Bei der Abfrage von Ereignisinformationen von einem Server werden sowohl der eigene Ereignisprotokollspeicher als auch die über die Föderation angeschlossenen Ereignisprotokollspeicher durchsucht. Ereignisdaten lassen sich so flexibel und effizient speichern und archivieren.

Mit den Archivierungseinstellungen im Ereignisprotokollspeicher können Sie angeben, wo und wie oft Daten archiviert werden sollen. Es werden sowohl warme (aktive) Ereignisprotokollspeicher als auch kalte (archivierte) Ereignisprotokollinformationen abgefragt. Ereignisinformationen im Offline-Speicher (Remote) werden nicht abgefragt.

Folgende Ereignisprotokoll- und Archivierungseinstellungen sind konfigurierbar:

Maximale Zeilenzahl

Legt die maximale Anzahl von Ereignissen fest, die in der Datenbank des Ereignisprotokollspeichers enthalten sein können. Erreicht die Anzahl diesen Wert, werden alle Daten in der Datenbank komprimiert und in die aktive Datenbank verschoben.

Minimum: 50000

Maximum: 100000000

Maximale Anzahl an Archivtagen

Gibt die Anzahl der Tage an, die archivierte Dateien im Archiv aufbewahrt werden, bevor Sie gelöscht werden.

Minimum: 1

Maximum: 28000

Festplattenspeicher für Archiv

Legt den Prozentsatz des verbleibenden Festplattenspeichers fest, bei dem die ältesten Archivdateien automatisch gelöscht werden. Der Standardwert ist beispielsweise 10. Fällt die Menge des verfügbaren Ereignisprotokollspeicherplatzes unter 5 %, werden die ältesten Dateien aus dem Protokoll gelöscht, um Speicherplatz zu gewinnen.

Minimum: 10

Maximum: 90

Exportrichtlinie

Gibt an, wie viele Stunden eine mittels einer externen Sicherung im Archiv wiederhergestellte Datei im Ereignisprotokollspeicher bleibt, bis sie gelöscht wird.

Minimum: 0

Maximum: 168

Zusammenfassungs-/und Unterdrückungsregeln

Bestimmt, welche der verfügbaren Zusammenfassungs- und Unterdrückungsregeln auf die eingegangenen Ereignisse angewendet werden. Neue Zusammenfassungs- und Unterdrückungsregeln müssen erst von einem Administrator angewendet werden, bevor mit ihnen Ereignisse verfeinert werden.

Weiterleitungsregeln

Bestimmt, welche der verfügbaren Ereignis-Weiterleitungsregeln auf die erhaltenen Ereignisse angewendet werden.

Untergeordnete Föderation

Regelt, welche der verfügbaren Ereignisprotokollspeicher dem aktuellen Server untergeordnet sind. So lassen sich eigene Föderationsstrukturen erstellen, um verschiedene Zugriffsebenen für Abfragen zu regulieren. Diese Einstellung ist nur als lokale Einstellung verfügbar.

Anhand von Protokolleinstellungen wird geregelt, wie einzelne CA Enterprise Log Manager-Module interne Nachrichten erfassen. Diese Einstellungen sind nur als lokale Einstellungen verfügbar. Üblicherweise dienen Protokolleinstellungen zur Fehlerbehebung. Im Allgemeinen müssen diese Einstellungen nicht geändert werden. Bevor Sie Änderungen daran vornehmen, machen Sie sich mit den Protokolldateien und dem Protokollierungsverfahren vertraut.

Protokollebene

Bestimmt Typ und Ebene der Informationen, die in der Protokolldatei aufgezeichnet werden. Die Optionen in der Dropdown-Liste sind nach Detailgenauigkeit angeordnet. Die erste Option bietet den niedrigsten Detailgrad, die letzte den höchsten.

Auf alle Protokollierungen anwenden

Bestimmt, ob mit der Einstellung "Protokollebene" alle Protokolleinstellungen aus der Eigenschaftsdatei des Protokolls überschrieben werden. Diese Einstellung gilt nur dann, wenn die Einstellung "Protokollebene" niedriger ist (d. h. einen höheren Detailgrad hat) als die Standardeinstellung.

Mit den Einstellungen zur automatischen Archivierung können Sie geplante Jobs zur Datenbankarchivierung aktivieren und steuern. Bei diesen Jobs werden aktive Datenbanken auf einen Remote-Server verschoben.

Hinweis: Bevor Sie geplante Datenbankjobs von einem CA Enterprise Log Manager-Server auf einen anderen CA Enterprise Log Manager-Server oder einen Remote-Server verschieben, müssen Sie zwischen den Servern die nicht interaktive Authentifizierung konfigurieren. Weitere Informationen finden Sie im Abschnitt "Konfigurieren von nicht interaktiver Authentifizierung" des *CA Enterprise Log Manager-Implementierungshandbuchs*.

Für die automatische Archivierung können folgende Werte festgelegt werden:

Aktiviert

Mit der Ausführung eines automatischen Archivierungsjobs wird begonnen. Bei der automatischen Archivierung wird das SCP-Hilfsprogramm entsprechend den anderen Einstellungen verwendet.

Sicherungstyp

Gibt den Typ der Sicherung an: Bei einer vollständigen Archivierung werden alle Datenbanken kopiert, bei einer Zuwachssicherung nur die noch nicht gesicherten Datenbanken.

Standard: Zuwachs

Häufigkeit

Bestimmt, ob die Archivierung täglich oder stündlich erfolgt. Geben Sie die Uhrzeit für die tägliche Archivierung mithilfe der Startzeit an. Stündliche Archivierungsjobs werden zu jeder vollen Stunde durchgeführt.

Startzeit

Gibt an, wann eine tägliche Archivierung erfolgt. Die Zeitangabe erfolgt in ganzen Stunden. Es gilt die Ortszeit des Servers. Die Uhrzeit wird im 24-Stunden-Format angegeben.

Obergrenzen: 0-23, wobei 0 für Mitternacht und 23 für 23 Uhr steht.

EEM-Benutzer

Bestimmt den Benutzer, der berechtigt ist, Abfragen im Archiv durchzuführen, das Archiv neu zu katalogisieren, das LMArchive-Hilfsprogramm und das Shellskript "restore-ca-elm" auszuführen, um Archivdatenbanken zu Prüfzwecken wiederherzustellen. 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.

Standard: Log Manager-Administratorbenutzer

EEM-Kennwort

Gibt das Kennwort des Benutzers an, der über die im Feld "EEM-Benutzer" angegebenen Rechte verfügt.

Remote-Server

Gibt den Hostnamen oder die IP-Adresse des Remote-Servers an, auf dem die Datenbankinformationen bei der automatischen Archivierung kopiert werden.

Remote-Benutzer

Gibt den Benutzernamen an, mit dem sich SCP am Remote-Server anmeldet.

Standard: caelmservice

Remote-Standort

Gibt den Zielspeicherort der Archivdatei auf dem Remote-Server an.

Standard: /opt/CA/LogManager

Remote-ELM-Server

Gibt an, ob der Remote-Server ein Verwaltungsserver ist oder nicht. Wenn ja, wird die Datenbank nach Abschluss bei der automatischen Archivierung vom lokalen Computer gelöscht, und der Remote-Computer wird aufgefordert, sich neu zu katalogisieren.

Zeitraum zum Empfang des Korrelationsereignisses

Steuert, wie groß die zeitliche Abweichung bei der Erstellung von Incidents sein darf. Die zwei Werte ermöglichen es Ihnen, einen späteren Wert (Zukunft) und einen früheren Wert (Vergangenheit) als den aktuellen Zeitpunkt des CA Enterprise Log Manager-Servers festzulegen. Wenn ein Ereignis nicht in dieses Fenster fällt, wird es nicht zur Korrelation weitergeleitet.

Weitere Informationen:

Protokollspeicherung (siehe Seite 199)
Anwenden von Unterdrückungs- oder Zusammenfassungsregeln (siehe Seite 565)

Hinweise zum Incident-Service

Sie können steuern, wie der Incident-Service Ereignisse speichert und Incidents für einen ausgewählten CA Enterprise Log Manager-Server erstellt. Sie können die folgenden Werte festlegen:

Ablaufuhrzeit

Gibt an, wie viele Tage der Service Incidents in der Incident-Datenbank behält. Wenn der Wert 0 ist, werden Ereignisse niemals gelöscht. Abgelaufene Incidents werden nicht angezeigt.

Beschränkungswerte für die Generierung von Incidents

Gibt an, wie oft eine einzelne Korrelationsregel Incidents erstellen kann, wodurch Sie die Zahl der unerwünschten mehrfachen Incidents reduzieren können. Zum Zweck der Beschränkung bei der Generierung von Incidents werden unterschiedliche Versionen einer Regel als separate Regeln betrachtet. Wenn Sie in Ihrer Umgebung also mehrere Versionen einer Regel angewandt haben, werden diese separat beschränkt. Grenzwerte umfassen:

Aktiviert

Zeigt an, ob Beschränkung bei der Generierung von Incidents angewendet werden.

Anzahl

Legt einen Schwellenwert für die Anzahl von Incidents fest, die von einer einzelnen Regel generiert werden. Dieser Wert funktioniert mit dem Zeitwert, wenn dieser Wert größer als 0 ist. Nachdem diese Zahlen erreicht worden sind, wendet der Incident-Service das Limit "Blockierte Zeit" an. Wenn Sie also die Anzahl auf 3 festlegen und die Zeit auf 10, wird das Limit angewendet, nachdem eine einzelne Regel in 10 Sekunden mehr als 3 Incidents generiert hat.

Zeit

Legt einen Schwellenwert in Sekunden für die Anzahl von Incidents fest, die von einer einzelnen Regel generiert werden. Dieser Wert funktioniert mit dem Wert "Anzahl", falls dieser Wert größer als 0 ist. Nachdem diese Zahlen erreicht worden sind, wendet der Incident-Service das Limit "Blockierte Zeit" an. Wenn Sie also die Anzahl auf 3 festlegen und die Zeit auf 10, wird das Limit angewendet, nachdem eine einzelne Regel in 10 Sekunden mehr als 3 Incidents generiert hat.

Blockierte Zeit

Legt ein Intervall in Sekunden fest, wenn eine Regel davon blockiert ist, weitere Incidents zu erstellen. Wenn dieses Limit erreicht ist, erstellt die Regel keine Incidents, bis die Zeit abläuft.

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:

- Festlegen von Firmennamen und Logo, Kopf- und Fußzeileninhalt, Farbe, Schriftarten und anderen PDF-Berichtseinstellungen im Bereich "Berichtskonfiguration".
- 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.

Hinweise zum Regeltestservice

Der Regeltestservice steuert die CA Enterprise Log Manager-Tests der Korrelationsregeln. Sie können folgende Werte für den Regeltest festgelegen:

Ereignisbeschränkung

Definiert, wie viele Ereignisse pro Incident beibehalten werden, wenn die Kumulierung aktiviert ist. Die Ereignisbeschränkung verhindert übermäßigen Datenverkehr, der durch die Korrelation in Zeiträumen mit hoher Aktivität verursacht wird. Wenn diese Beschränkung erreicht wird, gehen zusätzliche Ereignisse verloren. Wenn Sie die Beschränkung zum Beispiel auf 100 festgelegt haben, kann eine einzelne Regel bis zu 100 aufgezeichnete Ereignisse umfassen, einschließlich der ursprünglichen, qualifizierenden Ereignisse. Die Kumulierung wird fortgesetzt, bis die Ereignisbeschränkung erreicht wird, oder Lücken- oder Grenzwerte die Regel zurücksetzen, wobei Zweiteres häufiger auftritt.

Höchstanzahl gleichzeitig stattfindender Regeltests

Definiert die Anzahl der Regeltests, die gleichzeitig auf einem einzelnen CA Enterprise Log Manager-Server ausgeführt werden können.

Hinweise zu automatischen Software-Updates

Die automatischen Software-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-Server für automatische Software-Updates regelmäßig auf Aktualisierungen. Spätere Installationen werden als Clients dieses Proxy-Servers konfiguriert, die ihn regelmäßig wegen Aktualisierungen kontaktieren. Wenn die Clients den Server nicht kontaktieren, wird ein selbstüberwachendes Ereignis protokolliert.

Das Standardsystem sorgt für eine Verringerung des Netzwerkdatenverkehrs, indem die Notwendigkeit, dass jeder Server eine direkte Verbindung mit dem CA-Server für automatische Software-Updates 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 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 Services automatischer Software-Updates folgende Hinweise bezüglich bestimmter Einstellungen und deren Auswirkungen:

Standard-Proxy für automatische Software-Updates

Legt den standardmäßigen Proxy-Server für den Service automatischer Software-Updates fest. Der Standard-Proxy für automatische Software-Updates muss über eine Internetverbindung verfügen. Werden keine anderen Proxys für automatische Software-Updates festgelegt, erhält der Server die automatischen Software-Updates vom CA-Server, lädt binäre Aktualisierungen auf alle Clients herunter und verteilt Inhaltsaktualisierungen an den CA Enterprise Log Manager-Benutzerspeicher. Sind andere Proxys konfiguriert, kontaktieren Clients diesen Server im Zusammenhang mit Aktualisierungen, wenn keine Proxy-Liste für automatische Software-Updates 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.

Öffentlicher Schlüssel

Legt den Schlüssel fest, mit dem die Signatur für Updates getestet und überprüft wird. 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.

Wichtig! Aktualisieren Sie diesen Wert nie manuell.

Proxy für automatische Software-Updates

Bestimmt, ob der lokale Server ein Proxy für automatische Software-Updates ist. Wenn das Kontrollkästchen für den Proxy für automatische Software-Updates deaktiviert ist, ist der Server ein Client für automatische Software-Updates.

Jetzt aktualisieren

Startet einen bedarfsgesteuerten Aktualisierungszyklus unmittelbar für den ausgewählten Server. Sie können ein bedarfsgesteuertes Update nur jeweils auf einem Server ausführen; diese Option ist nicht global verfügbar. Aktualisieren Sie den Proxy-Server für automatische Software-Updates, bevor Sie seinen Client für automatische Software-Updates aktualisieren.

Online-Proxy für automatische Software-Updates

Bestimmt, ob der lokale Server ein Online-Proxy für automatische Software-Updates ist. Ein Online-Proxy für automatische Software-Updates verwendet seinen Internet-Zugriff, um Aktualisierungen von dem CA-Server für automatische Software-Updates zu erhalten und diese in der CA Enterprise Log Manager-Umgebung zu verteilen. Um einen Server als einen Online-Proxy für automatische Software-Updates zu bestimmen, wählen Sie sowohl das Kontrollkästchen "Proxy für automatische Software-Updates" als auch die Option "Online-Proxy für automatische Software-Updates" aus. Dieser Wert ist nur als lokale Einstellung verfügbar.

Offline-Proxy für automatische Software-Updates

Bestimmt, ob der lokale Server ein Offline-Proxy für automatische Software-Updates ist. Ein Offline-Proxy für automatische Software-Updates ist ein Server, der Software-Updates über die Kopie eines manuellen Verzeichnisses (mittels "scp") von einem Online-Proxy für automatische Software-Updates erhält. Offline-Proxys für automatische Software-Updates benötigen keinen Internetzugang. Um einen Server als einen Offline-Proxy für automatische Software-Updates zu bestimmen, wählen Sie sowohl das Kontrollkästchen "Proxy für automatische Software-Updates" als auch die Option "Offline-Proxy für automatische Software-Updates" aus. Dieser Wert ist nur als lokale Einstellung verfügbar.

Hinweis: Weitere wichtige Informationen zur Konfiguration von automatischen Software-Updates im Offline-Modus finden Sie im *CA Enterprise Log Manager-Administrationshandbuch.*

RSS-Feed-URL

Bestimmt die URL des CA-Servers für automatische Software-Updates. Über diese URL greifen Online-Proxys auf den CA-Server für automatische Software-Updates zu und laden Aktualisierungen herunter.

Zum Herunterladen verfügbare Module

Ermöglicht es Ihnen, aus den zum Herunterladen verfügbaren Modulen diejenigen Module auszuwählen, die sich für Ihre CA Enterprise Log Manager-Umgebung eignen. Klicken Sie auf "Durchsuchen", um diesen Dialog anzuzeigen. Die Module, die Sie auswählen, werden in der Modulliste angezeigt.

Die ausgewählten Module werden über automatische Software-Updates vom CA-Server für automatische Software-Updates heruntergeladen. Module können auf globaler Ebene zum Herunterladen ausgewählt werden. Andere konfigurierte Proxys für automatische Software-Updates laden diese Module während einer Aktualisierung standardmäßig herunter. Module können auch auf lokaler Ebene für individuelle Proxy- und Client-Server zum Herunterladen ausgewählt werden. Damit werden globale Einstellungen überschrieben, sodass nur die ausgewählten Module auf den bestimmten Server heruntergeladen werden. 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.

Zum Herunterladen ausgewählte Module

Zeigt die ausgewählten Module im Browser-Dialogfeld "RSS-Feed" an. Der Standard-Proxy für automatische Software-Updates und alle anderen Online-Proxys laden diese Module während des Aktualisierungsprozesses vom CA-Server für automatische Software-Updates herunter. Die aufgelisteten Module können Module sein, die zum Download auf globaler Ebene ausgewählt wurden, oder Module darstellen, die für einen bestimmten Server auf lokaler Ebene ausgewählt wurden.

HTTP-Proxy-Server

Bestimmt, ob dieser Server den CA-Server für automatische Software-Updates bezüglich Aktualisierungen 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.

Ablaufplan

Gibt die Startzeit und die Häufigkeit an, mit der CA Enterprise Log Manager-Server nach automatischen Software-Updates fragen. Online-Proxy für automatische Software-Updates (einschließlich des Standard-Proxy-Servers) kontaktieren den CA-Server für automatische Software-Updates, und Proxy-Clients kontaktieren ihre Proxy-Server entsprechend diesem Ablaufplan. Der Ablaufplan kann global für alle CA Enterprise Log Manager-Server festgelegt werden; er kann auch für einen bestimmten Server lokal überschrieben werden.

Proxy für automatische Software-Updates zur Client-Aktualisierung

Hiermit können Sie mittels Round-Robin 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(s) für automatische Software-Updates für 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: Sie sollten zwecks Redundanz mehr als einen Server auswählen, um als Proxy für automatische Software-Updates für Inhaltsaktualisierungen zu fungieren.

Weitere Informationen:

Freier Speicherplatz für Aktualisierungen (siehe Seite 259)
Info zu öffentlichen Schlüsseln für automatische Software-Updates (siehe Seite 260)

Systemstatus-Service

Sie können den Systemstatus-Service verwenden, um Informationen über einen CA Enterprise Log Manager-Server zu sammeln und diesen zu steuern. Sie zeigen nur den Systemstatus für einzelne CA Enterprise Log Manager-Server an. Alle Einstellungen und Optionen werden auf lokaler Ebene angewendet.

Der Systemstatus-Service enthält die folgenden Registerkarten:

- Verwaltung: Kontrollieren der Dienste und Hostserver und Erstellen einer Diagnosedatei für den Support
- Status: Überprüfen von Status und Version des System-Services und der Prozesse
- Selbstüberwachende Ereignisse: Überprüfen von Ereignissen, die sich auf den System- und Komponentenstatus

Weitere Informationen

Systemstatus-Aufgaben (siehe Seite 194)
Erstellen einer Diagnosedatei für den Support (siehe Seite 195)
Neustart eines Hostservers (siehe Seite 196)
Starten Sie die ELM-Services neu. (siehe Seite 196)
Überprüfen von Service-Status und Version (siehe Seite 197)
Überprüfen von selbstüberwachenden Systemsstatus-Ereignissen (siehe Seite 197)

Aufgaben für die Konfiguration von CA-Adaptern

Lokale Listener empfangen und erfassen mit Hilfe von verschiedenen Typen von CA-Adaptern native Ereignisse von bestimmten Quelltypen.

Sie können zwei Arten von individuellen Adapterkonfigurationen anzeigen und bearbeiten.

- Eine globale Konfiguration gilt für alle Instanzen eines einzelnen Adapters in Ihrer Umgebung, beispielsweise für alle SAPI-Collector-Instanzen.
- Eine lokale Konfiguration gilt nur für einen ausgewählten einzelnen Adapter-Host, beispielsweise für einen einzelnen SAPI-Collector.

Sie können auch selbstüberwachende Ereignisse für jeden Adapter-Service oder Adapter-Host aus den globalen oder lokalen Konfigurationsbereichen des einzelnen Adapters anzeigen.

Weitere Informationen

Bearbeiten globaler Adapterkonfigurationen (siehe Seite 186)
Bearbeiten lokaler Adapterkonfigurationen (siehe Seite 187)
Anzeigen von selbstüberwachenden Adapterereignissen (siehe Seite 189)
Anzeigen des Adapterstatus (siehe Seite 190)
Hinweise zum SAPI-Service (siehe Seite 191)
Hinweise zu iTechnology Event Service (siehe Seite 193)

Bearbeiten globaler Adapterkonfigurationen

Globale Adapterkonfigurationen sind Einstellungen, die für alle Instanzen eines bestimmten CA-Adapters in Ihrer Umgebung gelten. Diese können Sie bearbeiten. Sie können beispielsweise Konfigurationsänderungen vornehmen, die für alle in Ihrer Umgebung ausgeführten SAPI-Collectors gelten. Durch eine globale Adapterkonfiguration werden lokale Adaptereinstellungen, die von der globalen Einstellung abweichen, *nicht* außer Kraft gesetzt.

So bearbeiten Sie eine globale Adapterkonfiguration:

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

   Die Ordnerliste "Protokollerfassung" wird angezeigt.

2. Klicken Sie auf den Ordner "CA-Adapter".

   Der Ordner wird eingeblendet, so dass Unterordner für jeden Adapter angezeigt werden.

3. Wählen Sie den Ordner für den Adapter aus, dessen Konfiguration Sie bearbeiten möchten.

   Im Detailbereich wird die globale Service-Konfiguration angezeigt.

4. Ändern Sie die Konfiguration wie gewünscht.

   Hinweis: Wenn Sie auf "Zurücksetzen" klicken, werden die Konfigurationswerte auf den zuletzt gespeicherten Status zurückgesetzt. Sie können eine einzelne Änderung oder mehrere Änderungen zurücksetzen, bis Sie auf "Speichern" klicken. Nach dem Speichern von Änderungen können Sie diese nur noch einzeln zurücksetzen.

5. Klicken Sie auf "Speichern", wenn Sie die Änderungen abgeschlossen haben.

   Sämtliche von Ihnen durchgeführten Konfigurationsänderungen werden für alle Hosts des ausgewählten Adapters übernommen, es sei denn, die lokalen Einstellungen stimmen nicht überein.

Bearbeiten lokaler Adapterkonfigurationen

Sie können lokale Adapterkonfigurationen anzeigen oder bearbeiten. Mit lokalen Adapterkonfigurationen können Sie Einstellungen steuern, die möglicherweise nicht für die gesamte Umgebung gelten oder erforderlich sind. Sie setzen globale Einstellungen nur für bestimmte Adapter-Hosts außer Kraft. Möglicherweise möchten Sie festlegen, dass ein bestimmter SAPI-Adapter einen anderen Port abhört. Dieses Verhalten können Sie mit Hilfe einer lokalen Konfiguration festlegen.

So bearbeiten Sie eine lokale Adapterkonfiguration:

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

   Die Ordnerliste "Protokollerfassung" wird angezeigt.

2. Klicken Sie auf den Ordner "CA-Adapter".

   Der Ordner wird eingeblendet, so dass Unterordner für jeden Adapter angezeigt werden.

3. Wählen Sie den Ordner für den Adapter aus, dessen Konfiguration Sie bearbeiten möchten.

   Die Service-Anzeige wird eingeblendet, so dass Adapter-Hosts angezeigt werden.

4. Klicken Sie auf den gewünschten Adapter-Host.

   Die von Ihnen ausgewählte Host-Konfiguration wird im Detailbereich angezeigt.

5. Ändern Sie die Konfiguration wie gewünscht. Für jedes Feld, Menü oder Steuerelement zur Eingabe von Werten in der lokalen Konfiguration wird eine Schaltfläche für die lokale/globale Konfiguration angezeigt, mit der zwischen den beiden Status hin- und hergeschaltet werden kann.

   Globale Konfiguration: 

   Lokale Konfiguration: 

   Wenn Sie auf die Schaltfläche klicken, wird von der globalen zur lokalen Einstellung gewechselt, und das zugehörige Eingabefeld wird zur Bearbeitung verfügbar. Das Eingabefeld muss auf die lokale Konfiguration eingestellt bleiben, damit die Einstellung wirksam wird: Falls es auf die globale Konfiguration eingestellt ist, so ist die globale Einstellung für diesen Adapter wirksam.

Hinweis: Wenn Sie auf "Zurücksetzen" klicken, werden die zuletzt gespeicherten Konfigurationswerte für alle verfügbaren Konfigurationen angezeigt. Sie können eine einzelne Änderung oder mehrere Änderungen zurücksetzen, bis Sie auf "Speichern" klicken. Nach dem Speichern von Änderungen können Sie diese nur noch einzeln zurücksetzen.

6. Klicken Sie auf "Speichern", wenn Sie die Änderungen abgeschlossen haben.

   Sämtliche von Ihnen durchgeführten Änderungen werden nur für den ausgewählten Adapter-Host übernommen.

Anzeigen von selbstüberwachenden Adapterereignissen

Sie können die Aktivität von Service-Adaptern überwachen und zur Problembehebung selbstüberwachende Ereignisse für jeden Adapter-Service-Host anzeigen. Darüber hinaus können Sie vorab überwachte Ereignisse aus den globalen oder lokalen Konfigurationsbereichen einzelner Adapter anzeigen.

So zeigen Sie selbstüberwachende Adapterereignisse an:

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

   Die Ordnerliste "Protokollerfassung" wird angezeigt.

2. Klicken Sie auf den Ordner "CA-Adapter".

   Der Ordner wird eingeblendet, so dass Unterordner für jeden Adapter-Service angezeigt werden.

3. Wählen Sie den Ordner für einen Adpater-Service aus, um selbstüberwachende Ereignisse für diesen Service anzuzeigen, oder blenden Sie die Ordner ein, und wählen Sie einen Adapter-Host aus, um nur selbstüberwachende Ereignisse für diesen einzelnen Adapter-Host anzuzeigen.

   Die Adapterkonfiguration wird im Detailbereich angezeigt.

4. Klicken Sie auf die Registerkarte "Selbstüberwachende Ereignisse".

   Ein Ereignisanzeigefenster wird mit entsprechend gefilterten Ereignissen angezeigt. Wenn Sie im dritten Schritt beispielsweise den Ordner für das Ereignis-Plug-In von iTechnology ausgewählt haben, werden alle Instanzen für das Ereignis-Plug-In von iTechnology angezeigt. Wählen Sie im Ordner für das Ereignis-Plug-In von iTechnology einen bestimmten Host aus, werden nur Ereignisse angezeigt, die zu diesem spezifischen iTechnology-Host gehören.

   Hinweis: Ihre Föderationsstruktur steuert, welche Ereignisse sichtbar sind. Falls keine Föderation eingerichtet wurde, werden Ihnen unabhängig davon, welchen Host Sie auswählen, nur lokale Ereignisse angezeigt.

Weitere Informationen

Anzeigen des Adapterstatus (siehe Seite 190)
Bearbeiten globaler Adapterkonfigurationen (siehe Seite 186)
Bearbeiten lokaler Adapterkonfigurationen (siehe Seite 187)

Anzeigen des Adapterstatus

Sie können den aktuellen Status bestimmter CA-Adapter-Services anzeigen, darunter Startzeit, Ausführungsstatus sowie Ereignisübermittlungsinformationen und Statistiken. Der Status des Ereignis-Plug-In-Service von iTechnology kann nicht angezeigt werden.

So zeigen Sie den Status eines Adapters an:

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

   Die Ordnerliste "Protokollerfassung" wird angezeigt.

2. Klicken Sie auf den Ordner "CA-Adapter".

   Der Ordner wird eingeblendet, so dass Unterordner für jeden Adapter-Service angezeigt werden.

3. Wählen Sie den Ordner für den Adapter aus, dessen Status Sie anzeigen möchten.

   Die Service-Anzeige wird eingeblendet, so dass einzelne Adapter-Hosts angezeigt werden.

4. Klicken Sie auf den gewünschten Adapter-Host.

   Die von Ihnen ausgewählte Host-Konfiguration wird im Detailbereich angezeigt.

5. Klicken Sie auf die Registerkarte "Status".

   Die Statusinformationen werden angezeigt.

   Hinweis: Statusinformationen werden nur im Fensterbereich für die lokale Konfiguration angezeigt.

Hinweise zum SAPI-Service

In CA Enterprise Log Manager werden zwei Instanzen eines CA Audit Submit Application Programming Interface (SAPI)-Service verwendet; einer ist als SAPI-Collector installiert, der andere als SAPI-Router. Die SAPI-Services dienen im Allgemeinen dem Eingang von Ereignissen bestehender CA Audit-Clients und integrierter Produkte. Mit folgenden Einstellungen können Sie die SAPI-Adapter konfigurieren:

Listener aktivieren

Startet den ausgewählten Service. Diese Einstellung ist standardmäßig aktiviert.

SAPI-Port

Legt eine bestimmte Portnummer für den ausgewählten Service fest, wenn dieser nicht beim Portmapper registriert ist. Ist das Kontrollkästchen "Registrieren" aktiviert, verwendet der Service bei Auswahl des Standardwerts 0 einen zufällig bestimmten Port.

Hinweis: Die Portnummern für den SAPI-Collector und den SAPI-Router dürfen nicht gleich sein. Werden für beide Services dieselben Ports verwendet, funktioniert der als zweites festgelegte Port nicht.

Registrieren

Bestimmt, ob der Service beim Portmapper des Systems registriert wird. Wenn Sie "Registrieren" aktivieren und in das Feld für den SAPI-Port eine 0 eingeben, wird bei Aktivierung des Service immer ein Port per Zufallsgenerator bestimmt. Für beide Felder ist dies die Standardeinstellung. Wird "Registrieren" nicht aktiviert, muss ein SAPI-Port angegeben werden.

Verschlüsselungsschlüssel

Legt den Verschlüsselungsschlüssel fest, wenn Sie in der CA Audit-Umgebung einen nicht standardmäßigen Verschlüsselungsschlüssel verwenden. Mit diesem liest der SAPI-Adapter eingehende SAPI-Ereignisse.

Ereignisreihenfolge

Stellt sicher, dass die Ereignisse in derselben Reihenfolge zum Ereignisprotokollspeicher gesendet werden, wie sie empfangen wurden. Wird die Ereignisreihenfolge deaktiviert, kann sie dann geändert werden, wenn einige Ereignisse schneller als andere analysiert und weitergeleitet werden. Das Aktivieren der Option für die Ereignisreihenfolge kann sich auf die Leistung auswirken, da die Größe der Warteschlange für Ereignisse zunimmt.

Ereignisbeschränkung

Bestimmt die Höchstzahl der Ereignisse in der Ereigniswarteschlange und erlaubt so die Regulierung von Verarbeitungsressourcen. Wird der Wert 0 in das Feld eingegeben, findet keine Ereignisbeschränkung statt. Ereignisse, die diesen Schwellenwert überschreiten, werden an der Quelle verzögert.

Thread-Anzahl pro Warteschlange

Bestimmt die Anzahl der Verarbeitungs-Threads der einzelnen Protokolle. Bei deaktivierter Ereignisreihenfolge kann die Verarbeitung mit Hilfe vieler Verarbeitungs-Threads beschleunigt werden. Wird die Ereignisreihenfolge aktiviert, hat die Anzahl der Threads keine Auswirkungen. Die Verwendung vieler Threads kann die Leistung negativ beeinflussen.

Chiffre- und Datenzuordnung

- Die Wechselsteuerung für Chiffre bestimmt, welche der verfügbaren Chiffremöglichkeiten der Service zum Entschlüsseln eingehender Nachrichten heranzieht.
- Mit der Wechselsteuerung für die Datenzuordnungsdatei wird festgelegt, welche der verfügbaren DM-Dateien der Service bei der Ereigniszuordnung nutzt.

Anhand von Protokolleinstellungen wird geregelt, wie einzelne CA Enterprise Log Manager-Module interne Nachrichten erfassen. Diese Einstellungen sind nur als lokale Einstellungen verfügbar. Üblicherweise dienen Protokolleinstellungen zur Fehlerbehebung. Im Allgemeinen müssen diese Einstellungen nicht geändert werden. Bevor Sie Änderungen daran vornehmen, machen Sie sich mit den Protokolldateien und dem Protokollierungsverfahren vertraut.

Protokollebene

Bestimmt Typ und Ebene der Informationen, die in der Protokolldatei aufgezeichnet werden. Die Optionen in der Dropdown-Liste sind nach Detailgenauigkeit angeordnet. Die erste Option bietet den niedrigsten Detailgrad, die letzte den höchsten.

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 zu iTechnology Event Service

Der Service von iTechnology steuert die über den iGateway-Daemon übermittelten Ereignisse. Sie können den Service konfigurieren, indem Sie mit Hilfe der Wechselsteuerung für die DM-Datei festlegen, welche der verfügbaren (DM-)Datenzuordnungsdateien der Service für die Zuordnung von Ereignissen nutzt.

Der Plugin-Ereignis-Service umfasst bereits die meisten gängigen Datenzuordnungsdateien.

Anhand von Protokolleinstellungen wird geregelt, wie einzelne CA Enterprise Log Manager-Module interne Nachrichten erfassen. Diese Einstellungen sind nur als lokale Einstellungen verfügbar. Üblicherweise dienen Protokolleinstellungen zur Fehlerbehebung. Im Allgemeinen müssen diese Einstellungen nicht geändert werden. Bevor Sie Änderungen daran vornehmen, machen Sie sich mit den Protokolldateien und dem Protokollierungsverfahren vertraut.

Protokollebene

Bestimmt Typ und Ebene der Informationen, die in der Protokolldatei aufgezeichnet werden. Die Optionen in der Dropdown-Liste sind nach Detailgenauigkeit angeordnet. Die erste Option bietet den niedrigsten Detailgrad, die letzte den höchsten.

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.

Systemstatus-Aufgaben

Im Systemstatus-Service haben Sie folgende Möglichkeiten:

- Überprüfen von Status und Version des System-Services
- Überprüfen von selbstüberwachenden Ereignissen, die sich auf Systemkomponenten und Nutzung beziehen
- Erstellen einer Diagnosedatei für den Support
- Starten Sie die ELM-Services neu.
- Starten Sie den Hostserver neu, auf dem ein CA Enterprise Log Manager-Server ausgeführt wird.
- Aktivieren des Betriebs im FIPS-Modus und Nicht-FIPS-Modus

Weitere Informationen:

Erstellen einer Diagnosedatei für den Support (siehe Seite 195)
Neustart eines Hostservers (siehe Seite 196)
Starten Sie die ELM-Services neu. (siehe Seite 196)
Überprüfen von Service-Status und Version (siehe Seite 197)
Überprüfen von selbstüberwachenden Systemsstatus-Ereignissen (siehe Seite 197)

Erstellen einer Diagnosedatei für den Support

Sie können den Status und die Version für Dienste überprüfen, die auf einem ausgewählten CA Enterprise Log Manager-Server ausgeführt werden. Klicken Sie auf "Support-Diagnose", um das Skript "LmDiag.sh script" auszuführen, das mit CA Enterprise Log Manager geliefert wird.

Dieses Dienstprogramm packt Systeminformationen und Protokolldateien in eine komprimierte .tar-Datei, die an die Support-Mitarbeiter von CA gesendet werden kann. Sie können diese Datei über FTP oder eine andere Übertragungsmethode senden.

Hinweis: Diese Datei kann vertrauliche Informationen enthalten, z. B. IP-Adressen, Systemkonfigurationen, Hardwareprotokolle und Prozessprotokolle. Verwenden Sie eine sichere Methode, um diese Datei zu speichern und zu übermitteln/transportieren.

So erstellen Sie eine Diagnosedatei:

1. Klicken Sie auf die Registerkarte "Verwaltung" und dann auf die Unterregisterkarte "Services".
2. Erweitern Sie den Eintrag "Systemstatus".
3. Wählen Sie einen bestimmten CA Enterprise Log Manager-Server aus.

   In der Service-Konfiguration des Systemstatus wird die Registerkarte "Verwaltung" angezeigt.
4. Klicken Sie auf "Support-Diagnose".
5. Wählen Sie für den Download der generierten Diagnosedatei einen Speicherort aus.

   Das Dienstprogramm erstellt die Datei und lädt sie in den angegebenen Ordner herunter. Das Dienstprogramm wird automatisch beendet, sobald die Datei kopiert worden ist.

Neustart eines Hostservers

Sie können den Status und die Version für Dienste überprüfen, die auf einem ausgewählten CA Enterprise Log Manager-Server ausgeführt werden.

Wichtig! Verwenden Sie diese Funktion nur, wenn dies unbedingt erforderlich ist, oder wenn Sie vom CA-Support dazu aufgefordert werden. Beim Neustart eines CA Enterprise Log Manager-Servers kann dieser solange keine Ereignisprotokolle empfangen, analysieren und speichern, bis der Neustart abgeschlossen ist. Wenn Sie den Management-Server neu starten, müssen die verwalteten CA Enterprise Log Manager-Sitzungen auf anderen, verbundenen Servern ab- und erneut angemeldet werden.

So starten Sie einen Hostserver neu:

1. Klicken Sie auf der Registerkarte "Verwaltung" auf die Unterregisterkarte "Services".
2. Erweitern Sie den Eintrag "Systemstatus".
3. Wählen Sie einen bestimmten CA Enterprise Log Manager-Server aus.

   In der Service-Konfiguration des Systemstatus wird die Registerkarte "Verwaltung" angezeigt.
4. Klicken Sie auf "Host neu starten".

Starten Sie die ELM-Services neu.

Sie können die ELM-Services neu starten, die auf einem ausgewählten CA Enterprise Log Manager-Server ausgeführt werden.

Wichtig! Verwenden Sie diese Funktion nur, wenn dies unbedingt erforderlich ist, oder wenn Sie vom CA-Support dazu aufgefordert werden. Durch den Neustart der ELM-Services wird der betroffene CA Enterprise Log Manager-Server veranlasst, das Empfangen, Analysieren und Speichern von Ereignisprotokollen zu stoppen, bis der Neustart abgeschlossen ist. Wenn Sie den Management-Server neu starten, müssen die aktuelle Sitzung und alle anderen CA Enterprise Log Manager-Sitzungen auf anderen Servern ab- und wieder angemeldet werden.

So starten Sie die ELM-Services neu

1. Klicken Sie auf die Registerkarte "Verwaltung" und dann auf die Unterregisterkarte "Services".
2. Erweitern Sie den Eintrag "Systemstatus".
3. Wählen Sie einen bestimmten CA Enterprise Log Manager-Server aus.

   In der Service-Konfiguration des Systemstatus wird die Registerkarte "Verwaltung" angezeigt.
4. Klicken Sie auf "ELM-Services neu starten"

Überprüfen von Service-Status und Version

Sie können den Status und die Version für Dienste überprüfen, die auf einem ausgewählten CA Enterprise Log Manager-Server ausgeführt werden.

So überprüfen Sie den Status:

1. Klicken Sie auf die Registerkarte "Verwaltung" und dann auf die Unterregisterkarte "Services".
2. Erweitern Sie den Eintrag "Systemstatus".
3. Wählen Sie einen bestimmten CA Enterprise Log Manager-Server aus.
4. Klicken Sie auf die Registerkarte "Status".

Überprüfen von selbstüberwachenden Systemsstatus-Ereignissen

Sie können den Status und die Version für Dienste überprüfen, die auf einem ausgewählten CA Enterprise Log Manager-Server ausgeführt werden. Die Statusmeldungen beziehen sich auf Ereignisse, die die Prozessor- und Speicherplatzauslastung, durchschnittliche CPU-Auslastung, Arbeitsspeicherverwendung, Hardware-Zugriffe und -nutzung sowie andere Ereignisse betreffen.

So überprüfen Sie selbstüberwachende Systemstatus-Ereignisse:

1. Klicken Sie auf die Registerkarte "Verwaltung" und dann auf die Unterregisterkarte "Services".
2. Erweitern Sie den Eintrag "Systemstatus".
3. Wählen Sie einen bestimmten CA Enterprise Log Manager-Server aus.
4. Klicken Sie auf die Registerkarte "Selbstüberwachende Ereignisse".

Kapitel 6: Protokollspeicherung

Dieses Kapitel enthält folgende Themen:

Info zur Protokollspeicherung

Sie können über CA Enterprise Log Manager zwei Aspekte der Protokollspeicherung verwalten:

- Sicherung der Datenbanken, die die Protokolldateien im Archivverzeichnis jedes Berichtsservers enthalten, in einem Archivverzeichnis, das Sie auf dem Remote-Speicherserver erstellen. Der Remote-Speicherserver ist ein Zwischenspeicherort für archivierte Datenbanken, bis diese an einen Offsite-Speicherort verschoben werden können.
- Wiederherstellung der Datenbanken mit den Protokolldateien aus dem Archivverzeichnis auf einem Remote-Speicherserver auf den ursprünglichen Berichterstellungsserver oder eine CA Enterprise Log Manager-Ressource, die Sie speziell als Wiederherstellungspunkt-Server festgelegt haben. Nach der Wiederherstellung können Sie den Inhalt mit Abfragen und Berichten überprüfen.

Sie können Sicherungen von Ereignisprotokoll-Datenbanken auf zwei Arten verwalten:

- (Bevorzugt) Konfigurieren Sie CA Enterprise Log Manager so, dass warme Datenbanken mit Hilfe von automatischer Archivierung nach einem festgelegten Plan von einem CA Enterprise Log Manager-Berichtsserver auf einen Remote-Speicherserver verschoben werden. Bei der automatischen Archivierung wird der Berichtsserver über die erfolgte Sicherung der Datenbanken benachrichtigt.

  Hinweis: Weitere Informationen finden Sie im *CA Enterprise Log Manager-Implementierungshandbuch* unter "Info zur automatischen Archivierung".

- Sichern Sie die Datenbanken auf dem CA Enterprise Log Manager-Server von Hand und kopieren Sie sie in einen Onsite-Speicherort. Verwenden Sie das Hilfsprogramm "LMArchive", um dem CA Enterprise Log Manager-Server mitzuteilen, dass diese Datenbanken als gesichert markiert werden sollen.

  Die Verschiebung von gesicherten Dateien an einen Offsite-Speicherort ist eine Aufgabe, die Sie außerhalb von CA Enterprise Log Manager ausführen. Dies gilt auch für ihre Verschiebung zurück in das Netzwerk, wenn sie für die Wiederherstellung benötigt werden.

Sie können den Archivkatalog abfragen, um Datenbankdateien für die Wiederherstellung zu ermitteln. Sie haben die Möglichkeit, Datenbanken nach Bedarf auf eine der beiden folgenden Arten wiederherzustellen:

- Sie können sie mit Hilfe einer der folgenden Methoden auf dem ursprünglichen Berichterstellungsserver wiederherstellen:
  - Wenn Sie zwischen dem Remote-Speicherserver und dem ursprünglichen Berichtsserver nicht interaktive Authentifizierung konfigurieren, führen Sie das restore-ca-elm.sh-Skript aus, um die archivierten Datenbanken am ursprünglichen Berichtsserver wiederherzustellen.

    Nach der Wiederherstellung der Dateien fragen Sie diese ab und erstellen Berichte zur Länge des Zeitraums in Tagen, der als Lebensdauer von warmen Dateien konfiguriert ist.
  - Falls Sie die Archivdatenbanken manuell gesichert haben, kopieren Sie die Dateien wieder in dasselbe Archivverzeichnis zurück und benachrichtigen die betreffende CA Enterprise Log Manager-Ressource über die Wiederherstellung. Informieren Sie CA Enterprise Log Manager mit Hilfe einer Option des Befehlszeilen-Hilfsprogramms "LMArchive" über die wiederhergestellten Datenbanken.

    Nach der Wiederherstellung der Dateien fragen Sie diese ab und erstellen Berichte zur Länge des Zeitraums in Stunden, der als Lebensdauer von verfügbar gemachten Dateien konfiguriert ist.
- Sie können mit einer der beiden folgenden Methoden archivierte Datenbanken an einem Wiederherstellungspunktserver wiederherstellen, der dafür vorgesehen ist, wiederhergestellte Ereignisprotokolle zu überprüfen.
  - Wenn Sie vom Remote-Speicherserver zum CA Enterprise Log Manager-Wiederherstellungspunkt nicht interaktive Authentifizierung konfigurieren, können Sie das restore-ca-elm.sh-Skript ausführen, um archivierte Datenbanken am Wiederherstellungspunkt wiederherzustellen.
  - Kopieren Sie, wenn Sie die nicht interaktive Authentifizierung nicht konfiguriert haben, die archivierten Datenbanken manuell vom Remote-Speicherserver in das Archivverzeichnis des Wiederherstellungspunktservers. Benachrichtigen Sie anschließend diese CA Enterprise Log Manager-Ressource mit einer Neukatalogisierung aus der Archivkatalogabfrage im Protokollerfassungs-Explorer über die Wiederherstellung.

Diese Benachrichtigung führt dazu, dass der Katalog neu erstellt wird, wodurch die Datenbankdateien für Abfragen und Berichterstellung verfügbar werden. Diese Verfügbarkeit ist abhängig von dem für warme Dateien konfigurierten Alter in Tagen vor dem Löschen, das auf einen Wert festgelegt ist, der das Alter der wiederhergestellten Dateien überschreitet. Daher ist es wichtig, das maximale Alter für warme Dateien entsprechend auf einen beliebigen dedizierten Wiederherstellungspunkt festzulegen.

Status von Ereignisprotokoll-Datenbanken

Bei der Konfiguration der Autoarchivierung auf drei Servern (Erfassung, Berichterstellung und Remote-Speicherung) durchlaufen alle Ereignisprotokoll-Datenbanken drei Status: heiß, warm und kalt. Bei dieser Architektur gibt es nur auf dem Erfassungsserver eine heiße Datenbank mit nicht komprimierten Protokollen. Auf dem Berichterstellungsserver werden komprimierte warme Datenbanken gespeichert, während sich auf dem Remote-Speicherungsserver nur kalte Datenbanken befinden. Wenn eine kalte Datenbank mit dem Wiederherstellungs-Shellskript wiederhergestellt wird, wird sie als warme Datenbank wiederhergestellt. Wenn sie mit dem Hilfsprogramm "LMArchive" manuell wiederhergestellt wird, wird sie als verfügbar gemachte Datenbank wiederhergestellt.

Die folgenden vier Status des Ereignisprotokollspeichers beschreiben jeweils nicht komprimierte, komprimierte, gesicherte und verschobene und wiederhergestellte Datenbanken:

Heiß

Ein *heißer Datenbankstatus* ist der Status der nicht komprimierten Datenbank im Ereignisprotokollspeicher eines Erfassungsservers, in dem neu verarbeitete Ereignisse eingefügt werden. Sie können die maximale Anzahl neuer Datensätze in einer heißen Datenbank ("Maximale Zeilenanzahl") konfigurieren, bevor die Datenbank als warme Datenbank komprimiert wird. Sie können die Autoarchivierung planen, so dass warme Datenbanken stündlich vom Erfassungsserver zum konfigurierten Berichterstellungsserver verschoben werden. (Auf dem Berichterstellungsserver ist ebenfalls eine heiße Datenbank zum Einfügen selbstüberwachender Ereignisse vorhanden.)

Warm

Der *warme Datenbankstatus* ist der Status der Datenbanken im Ereignisprotokollspeicher des Berichterstellungsordners. Wenn Sie zwischen dem Berichterstellungsserver und einem Remote-Speicherserver die tägliche Autoarchivierung konfigurieren, bleiben die Datenbanken warm, bis sie auf den Remote-Speicherserver verschoben werden. Danach werden sie auf dem Berichterstellungsserver automatisch gelöscht. Wenn Sie zwischen dem Berichterstellungsserver und einem Remote-Speicherserver keine Autoarchivierung konfigurieren, bleiben warme Datenbanken auf dem Berichterstellungsserver, bis ihr Alter in Tagen den für "Maximale Anzahl an Archivtagen" konfigurierten Wert erreicht oder bis der für "Festplattenspeicher für Archiv" konfigurierte Schwellenwert erreicht wird, je nachdem, welcher Wert zuerst erreicht wird. Sobald einer dieser Schwellenwerte erreicht wird, wird die Datenbank gelöscht und der Datenbank wird der Status "kalt" zugewiesen. Ohne Autoarchivierung müssen Sie warme Datenbanken mit einem Tool eines Drittanbieters manuell sichern, bevor diese gelöscht werden, und anschließend das Hilfsprogramm "LMArchive" ausführen, um CA Enterprise Log Manager die Namen der Datenbanken mitzuteilen, die Sie gesichert und verschoben haben. Der warme Status wird auch zugewiesen, wenn nach der Wiederherstellung einer kalten Datenbank mit dem Skript "restore-ca-elm.sh" oder über die Schaltfläche "Neukatalogisieren" eine Neukatalogisierung durchgeführt wird.

Kalt

Der *kalte Datenbankstatus* wird Datenbanken auf dem Remote-Speicherserver zugewiesen. Auf dem Berichterstellungsserver wird ein Datensatz für eine kalte Datenbank erstellt, wenn die Datenbank auf dem Remote-Management-Server automatisch archiviert und auf dem Berichterstellungsserver gelöscht wird. Bei der manuellen Archivierung wird ein Datensatz der kalten Datenbank erstellt, wenn das Hilfsprogramm "LMArchive" mit der Option "-notify arch" ausgeführt wird. Sie können den Archivkatalog eines Berichterstellungsservers abfragen, um kalte Datenbanken für die Wiederherstellung zu ermitteln.

Verfügbar gemacht

Der *Status für verfügbar gemachte Datenbanken* ist der Status, der einer physisch kalten Datenbank zugewiesen wird, die im Archivverzeichnis wiederhergestellt wurde, nachdem der Administrator das Hilfsprogramm "LMArchive" mit der Option "-notify rest" 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.

Datenbanken können in jedem Status abgefragt werden. Eine normale Abfrage gibt Ereignisdaten von den heißen und warmen Datenbanken auf dem Berichterstellungsserver und, sofern vorhanden, verfügbar gemachte Datenbanken zurück. Eine föderierte Abfrage gibt Ereignisdaten von allen Servern in der Föderation zurück, wie etwa von föderierten Erfassungsservern, die heiße Datenbanken enthalten. Eine Archivabfrage gibt eine Liste mit Datenbanken zurück, die auf dem Berichterstellungsserver nicht mehr vorhanden sind, d. h. von Datenbanken im kalten Status. Die in einer Archivabfrage angegebenen physischen Datenbanken können auf dem Remote-Speicherserver vorhanden sein, der für die Onsite- oder Offsite-Speicherung verwendet wird.

Weitere Informationen

Automatisierung der Sicherung und Wiederherstellung (siehe Seite 205)
Manuelles Sichern von archivierten Datenbanken (siehe Seite 225)
Manuelles Wiederherstellen von Archiven im ursprünglichen Ereignisprotokollspeicher (siehe Seite 229)
Manuelles Wiederherstellen von Archiven in neuem Ereignisprotokollspeicher (siehe Seite 236)

Automatisierung der Sicherung und Wiederherstellung

Ein Sicherungsvorgang stellt sicher, dass durch die Löschung alter Datenbanken keine Daten verloren gehen. Die bevorzugte Methode, archivierte Datenbanken zu sichern, ist die "Automatische Archivierung". Automatische Archivierung ist eine geplante, automatisierte Übertragung von archivierten Datenbanken zwischen Serverpaaren. Automatische Archivierung zwischen einem Ausgangsserver und einem Zielserver benötigt nicht interaktive Authentifizierung. Bei der nicht interaktiven Authentifizierung wird eine Authentifizierung mit öffentlichem RSA-Schlüssel ohne Passphrase durchgeführt. Sie können nicht interaktive Authentifizierung und automatische Archivierung konfigurieren:

- Von jedem Ausgansserver zu seinem Berichtsserver.
- Von jedem Berichtsserver zu seinem Remote-Speicherserver.

Hinweis: Weitere Informationen finden Sie im *Implementierungshandbuch*.

Eine Wiederherstellung verschiebt archivierte Datenbanken vom Remote-Speicherserver in einen CA Enterprise Log Manager-Server zur Untersuchung. Die bevorzugte Methode, um archivierte Datenbanken wiederherzustellen, besteht darin, das restore-ca-elm.sh-Skript zu verwenden. Dieses Hilfsprogramm für die Wiederherstellung automatisiert die Übertragung von archivierten Datenbanken. Wie die automatische Archivierung verwendet auch das restore-ca-elm.sh-Skript nicht interaktive Authentifizierung. Sie können nicht interaktive Authentifizierung konfigurieren und das Wiederherstellungsskript ausführen:

- vom Remote-Speicherserver zum ursprünglichen Berichtsserver,
- vom Remote-Speicherserver zu einem Server mit einem einzelnen Wiederherstellungspunkt.

Sie konfigurieren automatische Archivierung so, dass sie in regelmäßigen Abständen stattfindet. Sie rufen das Wiederherstellen nach Bedarf auf.

Datenintegritätsüberprüfungen

Sie können archivierte oder neu katalogisierte Daten daraufhin überprüfen, ob sie manipuliert wurden, falls Sie als Benutzer mit Administratorrechten angemeldet sind. Durch diese Überprüfungen können Sie Ihre archivierten Daten sichern und dadurch gesetzliche Vorschriften einhalten. CA Enterprise Log Manager verwendet digitale Signaturen, um die Datenbanken zu validieren. Wenn die Datenbank beschädigt ist oder die Signatur fehlt oder beschädigt ist, betrachtet die Datenintegritätsüberprüfung die Datenbank als manipuliert.

Sie können Datenintegritätsüberprüfungen folgendermaßen festlegen:

- Automatisch, wenn Sie Daten wieder herstellen und neu katalogisieren
- Zu geplanten Zeiten auf ausgewählten Servern
- Nach Bedarf, wann Sie wollen

Sie können die Ergebnisse aller dieser Überprüfungen über die Datenintegritätsschnittstelle anzeigen. Manipulierte Datenbanken werden in Quarantäne gestellt und in den Listen der in Quarantäne gestellten Datenbanken angezeigt.

Weitere Informationen:

Automatische Integritätsüberprüfung aktivieren (siehe Seite 207)
Planen Sie eine Datenintegritätsüberprüfung (siehe Seite 207)
Datenintegrität nach Bedarf prüfen (siehe Seite 208)
In Quarantäne gestellte Datenbanken signieren (siehe Seite 208)

Automatische Integritätsüberprüfung aktivieren

Sie können eine Datenintegritätsüberprüfung festlegen, die immer dann automatisch auftritt, wenn Sie Daten wieder herstellen oder neu katalogisieren.

So aktivieren Sie eine automatische Datenintegritätsüberprüfung

1. Klicken Sie auf die Registerkarte "Verwaltung" und erweitern Sie die Unterregisterkarte "Services".
2. Wählen Sie den Knoten für den Ereignisprotokollspeicher aus, um globale automatische Überprüfungen zu aktivieren, oder erweitern Sie den Knoten für den Ereignisprotokollspeicher und wählen Sie einen CA Enterprise Log Manager-Server aus, um eine lokale automatische Überprüfung zu aktivieren.
3. Wählen Sie die Option "Integrität bei Neukatalogisierung und Wiederherstellung validieren" aus.

Planen Sie eine Datenintegritätsüberprüfung

Sie können tägliche Datenintegritätsüberprüfungen planen, um zu festgelegten Zeiten und auf ausgewählten CA Enterprise Log Manager-Servern stattzufinden. Jede bei einer geplanten Integritätsüberprüfung erkannte manipulierte Datenbank wird automatisch unter Quarantäne gestellt.

So planen Sie eine Datenintegritätsüberprüfung

1. Klicken Sie auf die Registerkarte "Verwaltung" und erweitern Sie die Unterregisterkarte "Services".
2. Wählen Sie den Knoten für den Ereignisprotokollspeicher aus, um globale automatische Überprüfungen zu planen, oder erweitern Sie den Knoten für den Ereignisprotokollspeicher und wählen Sie einen CA Enterprise Log Manager-Server aus, um eine lokale Überprüfung festzulegen.
3. Wählen Sie "Aktiviert".
4. (Optional) Wählen Sie "Föderiert" aus, um die geplante Überprüfung auf allen föderierten Servern auszuführen, die vom ausgewählten Server aus sichtbar sind.
5. Legen Sie die tägliche Startzeit fest.

Datenintegrität nach Bedarf prüfen

Sie können jederzeit eine Datenintegritätsüberprüfung auf einem ausgewählten CA Enterprise Log Manager-Server ausführen.

So führen Sie eine Datenintegritätsüberprüfung nach Bedarf durch

1. Klicken Sie auf die Registerkarte "Verwaltung" und auf die Unterregisterkarte "Archiv-Verwaltung".
2. Erweitern Sie den Ordner "Datenintegrität" und wählen Sie den CA Enterprise Log Manager-Server aus, auf dem Sie eine Überprüfung ausführen möchten.
3. Wählen Sie einen Zeitbereich für Ihre Überprüfung aus.
4. (Optional) Wählen Sie "Föderiert" aus, um die geplante Überprüfung auf allen föderierten Servern auszuführen, die für den ausgewählten Server sichtbar sind.
5. Klicken Sie auf "Jetzt validieren".

   Eine Liste der überprüften Datenbanken wird angezeigt. Als manipuliert erkannte Datenbanken werden mit einem roten Symbol angezeigt. Sie werden auch in der Liste der in Quarantäne gestellten Datenbanken angezeigt.

In Quarantäne gestellte Datenbanken signieren

Sie können die digitale Signatur auf einer in Quarantäne gestellten Datenbanken regenerieren, und sie somit für Abfragen verfügbar machen.

So regenerieren Sie die Signatur einer in Quarantäne gestellten Datenbank

1. Klicken Sie auf die Registerkarte "Verwaltung" und auf die Unterregisterkarte "Archiv-Verwaltung".
2. Erweitern Sie den Ordner "Datenintegrität" und wählen Sie den CA Enterprise Log Manager-Server aus, auf dem sich die in Quarantäne gestellten Datenbanken befinden.
3. Klicken Sie im rechten Fensterbereich auf die Registerkarte "Datenbanken in Quarantäne".
4. Wählen Sie die Datenbank aus, für die Sie eine Signatur regenerieren wollen.
5. Klicken Sie auf "Signatur generieren".

   Eine Bestätigungsmeldung wird angezeigt.

Schlüsselrotationen durchführen

Sie können die Registrierungsschlüssel, die dazu verwendet werden, hinsichtlich archivierter Datenbanken für erhöhte Sicherheit zu sorgen, rotieren.

Registrierungsschlüssel verwenden eine Kombination aus einem öffentlichen und privaten Verschlüsselungscode, um die Datenbankdateien zu sichern. Wenn Sie Schlüsselrotationen durchführen, wird der vorherige öffentliche Schlüssel beibehalten, sodass CA Enterprise Log Manager die Dateien überprüfen kann, die den vorherigen privaten Schlüssel verwendet haben.

So rotieren Sie Registrierungsschlüssel

1. Klicken Sie auf die Registerkarte "Verwaltung" und erweitern Sie die Unterregisterkarte "Services".
2. Wählen Sie den Ordner "Datenintegrität" aus und klicken Sie auf "Schlüsselrotationen durchführen".

   Eine Bestätigungsmeldung wird angezeigt.

Schlüssel importieren

Sie können öffentliche Registrierungsschlüssel importieren, die verwendet werden, um archivierte Datenbanken vor einer äußeren Quelle zu schützen. Durch den Import können Sie Schlüssel beibehalten, die von anderen älteren CA Enterprise Log Manager-Servern oder sonstigen früheren Servern verwendet wurden. Wenn Sie beispielsweise eine Sicherungsliste der öffentlichen Schlüssel führen, könnten Sie einen Import durchführen, um alte Datenbanksignaturen auf einem neu erstellten CA Enterprise Log Manager-Server überprüfen zu können.

So importieren Sie Registrierungsschlüssel

1. Klicken Sie auf die Registerkarte "Verwaltung" und erweitern Sie die Unterregisterkarte "Services".
2. Wählen Sie den Ordner "Datenintegrität" aus und klicken Sie auf "Schlüssel importieren".

   Ein Dialogfeld für den Import von Dateien wird angezeigt.
3. Suchen Sie die XML-Schlüsseldatei, die importiert werden soll, und klicken Sie auf "OK".

   Eine Bestätigungsmeldung wird angezeigt.

   Hinweis: Sie können Schlüssel nur im XML-Format importieren.

Schlüssel exportieren

Sie können die öffentlichen Registrierungsschlüssel exportieren, die dazu verwendet werden, archivierte Datenbanken zu sichern. Durch das Exportieren können Sie die Schlüssel für einen späteren Import in andere CA Enterprise Log Manager-Server sichern.

So exportieren Sie Registrierungsschlüssel

1. Klicken Sie auf die Registerkarte "Verwaltung" und erweitern Sie die Unterregisterkarte "Services".
2. Wählen Sie den Ordner "Datenintegrität" aus und klicken Sie auf "Schlüssel exportieren".

   Das Dialogfeld "Exportieren" wird angezeigt.
3. Wählen Sie den gewünschten Speicherort aus, und klicken Sie auf "Speichern".

Konfigurieren der nicht-interaktiven Authentifizierung für die Wiederherstellung

Nach dem Konfigurieren nicht interaktiver ssh-Authentifizierung zwischen dem Remote-Speicherserver und dem Zielserver können Sie das Shell-Skript "restore-ca-elm" verwenden, um die archivierten Datenbanken nach Bedarf wiederherzustellen. Für die Wiederherstellung ist der Remote-Speicherserver die Quelle und der Berichts-CA Enterprise Log Manager oder Wiederherstellungspunkt-CA Enterprise Log Manager ist das Ziel.

Die Prozesse unterscheiden sich geringfügig, je nach dem, ob das Ziel ein Berichtsserver oder ein dedizierter Wiederherstellungspunkt ist.

- Wenn Sie einen dedizierten Wiederherstellungspunkt verwenden, stellen Sie die nicht interaktive Authentifizierung einmal ein und verwenden Sie sie für jede darauf folgende Wiederherstellung. Das Verfahren richtet das .ssh-Verzeichnis auf dem Wiederherstellungspunkt mit der erforderlichen Eigentümerschaft ein und legt für die Schlüsseldatei Berechtigungen fest.
- Wenn Sie archivierte Datenbanken vom Remote-Speicherserver auf mehreren Berichtsservern wiederherstellen, richten Sie zwischen jedem Serverpaar die nicht interaktive Authentifizierung ein. Sie erstellen das Schlüsselpaar einmal, aber Sie kopieren den gleichen öffentlichen Schlüssel des Schlüsselpaares in jeden Zielberichtsserver. Kopieren Sie zum Beispiel den öffentlichen Schlüssel als "authorized_keys_RSS" vom Remote-Speicherserver in jeden Berichtsserver. Auf jedem Berichtsserver verbinden Sie die Datei "authorized_keys_RSS" mit der vorhandenen Datei "authorized_keys". Die vorhandene Datei enthält die von jedem Sammelserver kopierten öffentlichen Schlüssel.

Beide Prozesse gehen davon aus, dass Sie zuvor den Remote-Speicherserver dafür vorbereitet haben, als Zielserver für die automatische Archivierung zu dienen, wozu die nicht interaktive Authentifizierung erforderlich ist. Wenn die Vorbereitung nicht erfolgt ist, sehen Sie nach unter dem Abschnitt "Erstellen einer Verzeichnisstruktur mit Eigentumsrechten auf dem Remote-Speicherserver" im *Implementierungshandbuch*.

Beispiel: Authentifizierung vom Remote-Speicher zu einem Wiederherstellungspunkt konfigurieren

Einen CA Enterprise Log Manager-Server als Wiederherstellungspunkt zu verwenden, macht die Einstellung der nicht interaktiven Authentifizierung einfach. Sobald Sie zwischen dem Remote-Speicherserver und dem Wiederherstellungspunkt Authentifizierung einrichten, können Sie das Skript "restore-ca-elm.sh" für jede Wiederherstellung verwenden, ohne zusätzliche Schritte für Authentifizierung vorzunehmen.

Der Prozess für das Konfigurieren der nicht interaktiven Authentifizierung von einem Speicherserver zu einem Wiederherstellungspunkt CA Enterprise Log Manager beinhaltet die folgenden Prozeduren:

1. Generieren Sie vom Remote-Speicherserver das öffentliche/private RSA-Schlüsselpaar. Kopieren Sie den öffentlichen Schlüssel als "authorized_keys" in das Verzeichnis "/tmp" auf dem Wiederherstellungspunkt.
2. Erstellen Sie vom Wiederherstellpunkt aus das .ssh-Verzeichnis in /opt/CA/LogManager und legen Sie die Eigentümerschaft auf "caelmservice" fest. Kopieren Sie "authorized_keys" aus dem Verzeichnis "/tmp" in das Verzeichnis ".ssh". Wechseln Sie die Eigentümerschaft und legen Sie Berechtigungen auf "authorized_keys" fest.
3. Validieren Sie erfolgreiche nicht interaktive Authentifizierung zwischen dem Remote-Speicherserver und dem Wiederherstellungspunkt.

Generieren Sie Schlüssel und kopieren Sie den öffentlichen Schlüssel in den Wiederherstellungspunkt.

Generieren Sie vom Remote-Speicherserver ein RSA-Schlüsselpaar als "caelmservice"-Benutzer. Kopieren Sie dann die öffentliche Schlüsseldatei "id_rsa.pub" als "authorized_keys" in das Verzeichnis "/temp" auf dem Wiederherstellungspunkt CA Enterprise Log Manager. Ein Wiederherstellungspunkt ist ein Server, der dazu dient, wiederhergestellte Daten zu untersuchen.

Es wird angenommen, dass die Verzeichnisstruktur /opt/CA/LogManager/.ssh auf dem Speicherserver vorhanden und die Eigentümerschaft auf "caelmservice"-Benutzer und -Gruppe festgelegt ist. Sie enthält aus Berichtsservern kopierte "authorized_keys". Wenn Sie das Schlüsselpaar generieren, speichern Sie "id_rsa.pub" im Verzeichnis /opt/CA/LogManager/ssh.

So generieren Sie ein öffentliches/privates RSA-Schlüsselpaar für den Remote-Speicher zur Wiederherstellungspunktserver-Authentifizierung.

1. Melden Sie sich über "ssh" als "caelmservice"-Benutzer an dem Remote-Server an, der zum Speichern verwendet wird.
2. Schalten Sie Benutzer auf das "root"-Konto um.

   ```
   su –
   ```

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

   ```
   su – caelmservice
   ```

4. Erstellen Sie als "caelmservice"-Benutzer ein RSA-Schlüsselpaar.

   ```
   ssh-keygen –t rsa
   ```

5. Drücken Sie die Eingabetaste, um für jede der folgenden Eingabeaufforderungen den Standard zu akzeptieren:
   - 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 zur Datei .ssh, in der der "id_rsa.pub"-Schlüssel gespeichert ist.

   ```
   cd .ssh
   ```

9. Kopieren Sie den öffentlichen Schlüssel als "authorized_keys" in das Verzeichnis "/tmp" auf dem Wiederherstellungspunktserver.

   ```
   scp id_rsa.pub caelmadmin@<restore_point>:/tmp/authorized_keys
   ```

Bereiten Sie die Datei des öffentlichen Schlüssels zur Verwendung vor.

Sie erstellen das .ssh-Verzeichnis auf dem Wiederherstellungspunktserver und setzen die Eigentümerschaft auf "caelmservice" fest. Danach kopieren Sie "authorized_keys" aus dem Verzeichnis "/tmp" in das Verzeichnis ".ssh". Zuletzt legen Sie die Eigentümerschaft und Berechtigungen auf die Datei des öffentlichen Schlüssels fest.

So bereiten Sie den öffentlichen Schlüssel auf dem Wiederherstellungspunktserver für nicht interaktive Authentifizierung vor

1. Melden Sie sich mittels ssh als "caelmadmin" auf dem Wiederherstellungspunkt-CA Enterprise Log Manager-Server an.
2. Wechseln Sie die Benutzer zu "root".
3. Wechseln Sie Verzeichnisse zum CA Enterprise Log Manager-Verzeichnis.

   ```
   cd /opt/CA/LogManager
   ```

4. Erstellen Sie das .ssh-Verzeichnis:

   ```
   mkdir .ssh
   ```

5. Wechseln Sie die Eigentümerschaft von .ssh zu "caelmservice"-Benutzer und -Gruppe:

   ```
   chown caelmservice:caelmservice .ssh
   ```

6. Wechseln Sie zu folgendem Verzeichnis: /opt/CA/LogManager/.ssh.
7. Kopieren Sie die Datei "authorized_keys" von "/temp" nach ".ssh":

   ```
   cp /tmp/authorized_keys .
   ```

8. Wechseln Sie die Eigentümerschaft der Datei "authorized_keys" auf "caelmservice":

   ```
   chown caelmservice:caelmservice authorized_keys
   ```

9. Ändern Sie Berechtigungen auf der Datei "authorized_keys":

   ```
   chmod 755 authorized_keys
   ```

Beispiel: Authentifizierung von einem Speicherserver zu einem Berichtsserver konfigurieren

Sie können archivierte Datenbanken von einem Remote-Speicherserver auf ihrem ursprünglichen Berichtsserver wiederherstellen, das heißt auf dem Server, von dem aus sie automatisch archiviert wurden. Der Vorteil dieser Methode ist, dass Sie die CA Enterprise Log Manager-Archivdatenbank nicht neu katalogisieren müssen. Die Datenbanken von Protokolldateien, die Sie wiederherstellen, sind dem Berichtsserver bereits bekannt. Wenn Sie mehrere Berichtsserver haben, konfigurieren Sie die nicht interaktive Authentifizierung zwischen dem Remote-Speicherserver und jedem Berichtsserver. Die Datei "authorized_keys" ist im ".ssh"-Verzeichnis des Berichtsservers vorhanden. Diese Datei "authorized_keys" besitzt die öffentlichen Schlüssel jedes Schlüsselpaares, das auf einem Sammelserver generiert wurde, der automatisch auf diesen Berichtsserver archiviert. Deswegen erstellen Sie eine autorisierte Schlüsseldatei mit einem Suffix und verbinden diese Datei dann mit der ursprünglichen "authorized_keys"-Datei.

Der Prozess für das Konfigurieren der nicht interaktiven Authentifizierung von einem Remote-Speicherserver zu einem CA Enterprise Log Manager-Berichtsserver beinhaltet die folgenden Prozeduren:

1. Vom Remote-Speicherserver:
   a. Konfigurieren Sie den öffentlichen/privaten RSA-Schlüssel für den Remote-Speicher für Berichtsserverauthentifizierung.
   b. Kopieren Sie den öffentlichen Schlüssel als "authorized_keys_RSS" vom Speicherserver zum "/tmp"-Verzeichnis auf dem Berichtsserver.
2. Vom Berichtsserver:
   a. Kopieren Sie die aktuelle Datei "authorized_keys" aus ".ssh" in "/tmp".
   b. Verbinden Sie "authorized_keys_RSS" im Verzeichnis "/tmp" mit der Datei "authorized_keys".
   c. Kopieren Sie die angehängte Datei "authorized_keys" zurück ins Verzeichnis ".ssh".
3. Validieren Sie vom Remote-Speicherserver aus erfolgreiche nicht interaktive Authentifizierung zwischen Servern.
4. Wiederholen Sie diese Schritte für jede Kombination von Remote-Speicherserver zu Berichtsserver.

Generieren Sie Schlüssel und kopieren Sie den öffentlichen Schlüssel auf einen Berichtsserver.

Generieren Sie vom Remote-Speicherserver aus ein RSA-Schlüsselpaar als "caelmservice"-Benutzer und kopieren Sie den öffentlichen Schlüssel dann als "authorized_keys_RSS" ins "/tmp"-Verzeichnis auf einem CA Enterprise Log Manager-Berichtsserver. Der Berichtsserver hat normalerweise eine "authorized_keys"-Datei im ".ssh"-Verzeichnis, die eine Verbindung von öffentlichen Schlüsseln aus verschiedenen Sammelservern enthält. Senden Sie den Schlüssel mit einem eindeutigen Namen, so dass er an die vorhandene "authorized_keys"-Datei angehängt werden kann.

So generieren Sie das öffentliche/private RSA-Schlüsselpaar und kopieren den öffentlichen Schlüssel vom Remote-Speicher auf einen Berichtsserver.

1. Melden Sie sich beim Remote-Speicherserver über "ssh" als "caelmadmin"-Benutzer an.
2. Wechseln Sie die Benutzer zu "root".
3. Schalten Sie Benutzer auf das "caelmservice"-Konto um.

   ```
   su – caelmservice
   ```

4. Erstellen Sie als "caelmservice"-Benutzer ein RSA-Schlüsselpaar.

   ```
   ssh-keygen –t rsa
   ```

5. Drücken Sie die Eingabetaste, um für jede der folgenden Eingabeaufforderungen den Standard zu akzeptieren:
   - 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. Ändern Sie die Berechtigungen für das Verzeichnis ".ssh" mit folgendem Befehl:

   ```
   chmod 755 .ssh
   ```

7. Navigieren Sie zu dem Verzeichnis ".ssh".
8. Kopieren Sie "id_rsa.pub als authorized_keys_RSS" in das Verzeichnis "/tmp" auf dem Berichtsserver.

   ```
   scp id_rsa.pub caelmadmin@<reporting_server>:/tmp/authorized_keys_RSS
   ```

Aktualisieren der vorhandenen öffentlichen Schlüsseldatei

Sie haben den öffentlichen Schlüssel "authorized_keys_RSS" in das Verzeichnis "/tmp" auf dem Berichtsserver kopiert. Nun bereiten Sie den vorhandenen öffentlichen Schlüssel zur Verwendung vor. Vorbereiten bedeutet, "authorized_keys_RSS" an "authorized_keys" anzuhängen. Die korrekte Eigentümerschaft und richtigen Berechtigungen sind bereits auf der vorhandenen "authorized_keys"-Datei festgelegt.

So hängen Sie "authorized_keys_RSS" an "authorized_keys" an und kopieren die Datei in den richtigen Speicherort

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 "/tmp", das "authorized_keys_RSS" enthält.
4. Kopieren Sie die vorhandene "authorized_keys"-Datei von ".ssh" ins aktuelle Verzeichnis "/tmp".

   ```
   cp /opt/CA/LogManager/.ssh/authorized_keys .
   ```

5. Fügen Sie die Inhalte des öffentlichen Schlüssels aus dem Remote-Speicherserver zur "authorized_keys"-Datei hinzu, die öffentliche Schlüssel von Sammelservern enthält.

   ```
   cat authorized_keys_RSS >> authorized_keys
   ```

6. Wechseln Sie zu folgendem Verzeichnis: /opt/CA/LogManager/.ssh.
7. Kopieren Sie die "authorized_keys"-Datei von "/tmp" in ".ssh", das aktuelle Verzeichnis:

   ```
   cp /tmp/authorized_keys .
   ```

Abfragen des Archivkatalogs

Sie können Abfragen erstellen, um mithilfe von Schnellfiltern oder erweiterten Filtern den lokalen Archivkatalog nach ausgelagerten (ferngespeicherten) Datenbanken zu durchsuchen. Die Abfrageergebnisse können Ihnen dabei helfen, die gesicherten Datenbankdateien zu ermitteln, die zur Durchführung einer Untersuchung wiederhergestellt werden müssen.

So fragen Sie den Archivkatalog ab:

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

   Der Ordner "Archiv-Explorer" wird angezeigt.

2. Klicken Sie auf den Ordner "Archivabfrage und Neukatalogisierung".

   Im Fenster "Details" wird das Dialogfeld "Archivabfrage" angezeigt.

3. Wählen Sie den Zeitraum für Ihre Abfrage aus, oder geben Sie ihn ein.

4. Klicken Sie auf "Filter hinzufügen", wählen Sie eine Spalte aus, und geben Sie den Suchwert für die Spalte ein. Sie können mehrere Filter hinzufügen.

5. Wählen Sie "Ausschließen", um nach allen Protokollen zu suchen, *ausgenommen* die Protokolle mit dem von Ihnen eingegebenen Wert.

   Hinweis: Wenn Sie einen Filter mit einer Spalte erstellen, die *nicht* im Katalog enthalten ist, gibt CA Enterprise Log Manager statt eines leeren Satzes alle Datenbanken aus dem angegebenen Zeitraum aus. Dies bedeutet, dass Sie nicht alle katalogisierten Spalten kennen müssen, um eine zweckdienliche Archivabfrage zu erstellen.

6. Optional: Klicken Sie auf die Registerkarte "Erweiterte Filter", um erweiterte Filter hinzuzufügen. Es werden die Ereignisinformationen aufgenommen, deren Spaltenwert dem entsprechenden Vergleich mit dem von Ihnen eingegebenen Wert standhält. Wählen Sie eine Spalte und einen Operator, und wählen Sie dann einen Wert aus, oder geben Sie einen Wert ein. Operatorbeschreibungen folgen:

   Vergleichsoperatoren

   Gleich, Ungleich, Kleiner als, Größer als, Kleiner oder gleich, Größer oder gleich.

   Wie

   Berücksichtigt die Ereignisinformationen, wenn die Spalte ein Muster enthält, das Ihrer Texteingabe unter Verwendung des Platzhalterzeichens "%" entspricht. "L%" berücksichtigt Werte, die mit "L" beginnen. "%L%" berücksichtigt Werte, die "L" enthalten, wobei dieser Buchstabe weder das erste noch das letzte Zeichen ist.

   Nicht wie

   Berücksichtigt die Ereignisinformationen, falls der Spaltenwert nicht dem angegebenen Muster entspricht.

   Enthalten

   Berücksichtigt die Ereignisinformationen, wenn die Spalte einen oder mehrere der Werte enthält, die Sie durch Anführungszeichen getrennt eingegeben haben. Mehrere Werte in der Gruppe müssen durch Kommata voneinander getrennt werden.

   Nicht enthalten

   Berücksichtigt die Ereignisinformationen, wenn die Spalte einen oder mehrere der Werte enthält, die Sie durch Anführungszeichen getrennt eingegeben haben. Mehrere Werte in der Gruppe müssen durch Kommata voneinander getrennt werden.

   Übereinstimmend

   Schließt alle Ereignisinformationen ein, die mit einem oder mehreren der von Ihnen eingegebenen Zeichen übereinstimmen, so dass Sie nach Schlüsselwörtern suchen können.

Mit Schlüssel

Schließt alle Ereignisinformationen ein, die beim Konfigurieren des Berichtsservers als Schlüsselwerte festgelegt wurden. Verwenden Sie Schlüsselwerte, um die Unternehmensrelevanz oder andere organisatorische Gruppen festzulegen.

Ohne Schlüssel

Schließt alle Ereignisinformationen ein, die beim Konfigurieren des Berichtsservers nicht als Schlüsselwerte festgelegt wurden. Verwenden Sie Schlüsselwerte, um die Unternehmensrelevanz oder andere organisatorische Gruppen festzulegen.

7. Klicken Sie auf "Abfrage".

   Die Abfrageergebnisse werden angezeigt. Die Dateien, die mit Ihren Abfragekriterien übereinstimmende Datensätze enthalten, werden mit dem vollständigen relativen Pfad angezeigt, relativ zu $IGW_LOC. Beispiele:

   ../../LogManager/data/archive/<databaseFilename>

   <RemoteHostname>-.../../LogManager/data/archive/<databaseFilename>

Wiederherstellen automatisch archivierter Dateien

Wenn Sie archivierte Dateien von einem externen Speicherort auf den Remote-Server kopieren, der für die automatische Archivierung konfiguriert ist, können Sie sie mit dem Skript "restore-ca-elm.sh" wiederherstellen. Diese Alternative ist der manuellen Verwendung des Hilfsprogramms "LMArchive" vorzuziehen.

So stellen Sie automatisch archivierte Dateien wieder her:

1. Melden Sie sich mit Ihren "caelmadmin"-Berechtigungsnachweisen bei dem CA Enterprise Log Manager-Server mit dem Ereignisprotokollspeicher an, wo Sie die Datenbanken wiederherstellen möchten.
2. Schalten Sie bei der Befehls-Eingabeaufforderung von "Benutzer" auf "Root" um, i. e.:

   ```
   su - root
   ```

3. Wechseln Sie mit dem folgenden Befehl zum Verzeichnis "/opt/CA/SharedComponents/iTechnology":

   ```
   cd $IGW_LOC
   ```

4. Schalten Sie bei der Befehls-Eingabeaufforderung von "Benutzer" zum "caelmservice"-Konto um.

   ```
   su - caelmservice
   ```

5. Führen Sie den folgenden Befehl aus, wobei *userid* und *pwd* die Berechtigungsnachweise für ein CA Enterprise Log Manager-Benutzerkonto mit Administratorrolle sind.

   ```
   restore-ca-elm.sh -euser userid -epasswd pwd -rhost hostname -ruser userid -rlocation path -files file1,file2,file3...
   ```

   Note: Um einem Nicht-Administrator zu gestatten, das Skript "restore-ca-elm shell" auszuführen, erstellen Sie eine benutzerdefinierte Rolle und eine benutzerdefinierte Richtlinie. Dann können Benutzer, denen Sie diese Rolle zuweisen, ihre userid- und pwd-Berechtigungsnachweise angeben.

Weitere Informationen:

Wiederherstellungs–Skript für die Wiederherstellung archivierter Datenbanken (siehe Seite 222)
Beispiel: Einem Nicht-Administrator gestatten, Archive zu verwalten (siehe Seite 122)
Automatisierung der Sicherung und Wiederherstellung (siehe Seite 205)

Wiederherstellungs-Skript für die Wiederherstellung archivierter Datenbanken

Daten, die in einer kalten Datenbank auf einem Remote-Speicherserver enthalten sind, können nicht abgefragt und in Berichten ausgegeben werden. Wenn Sie solche Daten abfragen und in Berichten verwenden möchten, müssen sie sich auf einem CA Enterprise Log Manager-Server befinden und den Status "warm" aufweisen. Das Shell-Skript zur Wiederherstellung "restore-ca-elm.sh" ist ein Befehlszeilen-Hilfsprogramm, das eine festgelegte kalte Datenbank und die entsprechende digitale Signatur auf einen festgelegten CA Enterprise Log Manager-Server verschiebt und als warme Datenbank wiederherstellt. Sie können das Hilfsprogramm für die Wiederherstellung verwenden, um eine Datenbank wieder auf den ursprünglichen Berichtsserver oder an einen bestimmten Wiederherstellungspunkt zurück zu verschieben. Nicht interaktive Authentifizierung zu konfigurieren ist eine Voraussetzung für die Ausführung des Wiederherstellskripts.

Sie führen das Wiederherstellungsskript auf dem CA Enterprise Log Manager-Server aus, auf dem Sie die Dateien wiederherstellen möchten. Der Remote-Host, den Sie in dem Befehl angeben, bezieht sich auf den Remote-Speicherserver. Kalte Datenbanken befinden sich im Archivverzeichnis des Remote-Speicherservers.

Für das Wiederherstellen von Datenbankdateien auf entweder dem ursprünglichen Berichtsserver oder einem Wiederherstellungspunktserver gelten folgende Anforderungen:

- Auf dem Remote-Server wurden die Eigentumsrechte an der RSA-Schlüsseldatei festgelegt.
- "caelmservice" verfügt auf dem Remote-Server über Zugriffsberechtigung auf den Ordner "/opt/CA/LogManager".

Wenn Sie Dateien auf einem Wiederherstellungspunktserver wiederherstellen, führen Sie außerdem folgende Aktionen aus:

1. Kopieren Sie den RSA-Schlüssel vom Remote-Speicherserver auf den Wiederherstellungspunktserver.
2. Legen Sie die Eigentumsrechte an der RSA-Schlüsseldatei auf dem Wiederherstellungspunktserver fest.

Der Befehl besitzt das folgende Format:

```
restore-ca-elm.sh -euser userid -epasswd pwd -rhost hostname -ruser userid -
rlocation path -files file1,file2,file3...
```

-euser *Benutzername*

Gibt den Benutzernamen eines CA Enterprise Log Manager-Benutzerkontos an, dem die Administratorrolle zugewiesen ist.

-epasswd *pwd*

Gibt das CA Enterprise Log Manager-Kennwort an, das dem Benutzernamen zugewiesen ist.

-rhost *host*

Gibt den Hostnamen oder die IP-Adresse des Remote-Hosts an, auf dem sich die kalten Datenbankdateien im Archivverzeichnis befinden. Der Remote-Host ist kein CA Enterprise Log Manager-Server.

-ruser remote *user*

Gibt das Benutzerkonto mit Berechtigungen für den Pfad "/opt/CA/LogManager" und Eigentumsrechten am Ordner".ssh" an, der die autorisierten Schlüsseldateien enthält. Normalerweise handelt es sich bei diesem Konto um das "caelmservice"-Benutzerkonto.

-rlocation *path*

Gibt den Pfad der Datenbankdateien auf dem Remote-Speicherserver an. Wenn es sich bei diesem Server um einen UNIX-Server handelt, lautet der Pfad "/opt/CA/LogManager/data/archive".

files *file1,file2,file3...*

Gibt eine kommagetrennte Liste (ohne Leerzeichen) der wiederherzustellenden Datenbankdateien an.

Beispiel: Shell-Skript zur Wiederherstellung

Der folgende Beispielbefehl wird von dem CA Enterprise Log Manager aus ausgeführt, auf dem die archivierten Datenbanken wiederhergestellt werden sollen. Er wird von einem Benutzer durchgeführt, der über Berechtigungsnachweise des "Administrator1", "calm_r12" verfügt. Der Remote-Server, auf den die archivierten Datenbanken aus dem externen Speicherserver "NY-Speicherserver" verschoben worden sind. Dieser Remote-Server ist mit einem "caelmservice"-Konto konfiguriert worden, das Eigentumsrechte am Ordner ".ssh" hat, in den die öffentlichen RSA-Schlüssel kopiert worden sind. Dieses Konto verfügt außerdem über sämtliche Berechtigungen für die Verzeichnisstruktur "/opt/CA/LogManager". Dieser Befehl gibt an, dass sich die wiederherzustellenden Dateien im Verzeichnispfad "data/archive" des NY--Storage-Svr-Servers befinden, und identifiziert die Datenbankdateien, die als NY--Storage- "Svr_20081206192014.db.cerod" wiederherzustellen sind.

```
restore-ca-elm.sh -euser Administrator1 -epasswd calm_r12 -rhost NY-Storage-Svr -
ruser caelmservice -rlocation /opt/CA/LogManager/data/archive -files
NY-Storage-Svr_20081206192014.db.cerod
```

Weitere Informationen:

Wiederherstellen automatisch archivierter Dateien (siehe Seite 220)
Konfigurieren der nicht-interaktiven Authentifizierung für die Wiederherstellung (siehe Seite 211)
Beispiel: Authentifizierung vom Remote-Speicher zu einem Wiederherstellungspunkt konfigurieren (siehe Seite 212)
Beispiel: Authentifizierung von einem Speicherserver zu einem Berichtsserver konfigurieren (siehe Seite 215)

Manuelles Sichern von archivierten Datenbanken

CA Enterprise Log Manager erstellt jedes Mal, wenn Daten von einem heißen Speicher in einen warmen Speicher verschoben werden, gemäß den von Ihnen festgelegten Einstellungen automatisch eine neue archivierte Datenbank. Es wird zwar empfohlen, zum Verschieben von warmen Datenbanken auf einen Remote-Server die Autoarchivierung zu konfigurieren. Dennoch können Sie Ihre eigenen Tools zum Durchführen von Sicherungen der Archivdatenbanken verwenden und anschließend das Hilfsprogramm "LMArchive" ausführen, um das System über die durchgeführte Sicherung zu benachrichtigen.

Es wird empfohlen, warme Datenbanken täglich entweder automatisch oder wie im Folgenden beschrieben manuell zu sichern. Das ist wichtig, da Archivdateien aus warmen Speichern automatisch gelöscht werden, wenn die von Ihnen festgelegte Zeit überschritten wird oder wenn der Festplattenspeicher den von Ihnen festgelegten Wert erreicht.

Gehen Sie wie folgt vor, um warme Datenbanken manuell zu sichern:

1. Ermitteln Sie, welche Datenbanken noch nicht gesichert wurden.
2. Führen Sie die Sicherungen durch.
3. Zeichnen Sie die Sicherungen auf.

Weitere Informationen

Ermitteln von nicht gesicherten Datenbanken (siehe Seite 225)
Durchführen von Sicherungen (siehe Seite 227)
Aufzeichnen der Sicherungen (siehe Seite 227)

Ermitteln von nicht gesicherten Datenbanken

Sie können eine Liste mit archivierten Datenbanken anzeigen, die noch nicht als mit dem Hilfsprogramm LMArchive gesichert markiert sind. Um zuverlässige Ergebnisse zu erhalten, wird vorausgesetzt, dass dieses Hilfsprogramm jedes Mal mit der Option *-notify arch* ausgeführt wird, wenn eine archivierte Datenbank gesichert wird.

Wichtig! Um Verwirrung zu vermeiden, informieren Sie CA Enterprise Log Manager am besten immer gleich über abgeschlossene Sicherungen.

So zeigen Sie die Namen aller aktuellen archivierten Datenbankdateien an, die nicht als gesichert markiert sind:

1. Melden Sie sich mit den **caelmadmin**-Anmeldeinformationen beim CA Enterprise Log Manager-Server mit dem Ereignisprotokollspeicher an, der die Datenbanken enthält, die zur Archivierung gesichert werden müssen.
2. Lassen Sie die Benutzer an der Eingabeaufforderung folgendermaßen zum Root-Verzeichnis wechseln:

   ```
   su - root
   ```

3. Wechseln Sie mit dem folgenden Befehl zum Verzeichnis "/opt/CA/SharedComponents/iTechnology":

   ```
   cd $IGW_LOC
   ```

4. Führen Sie den folgenden Befehl aus, wobei *Benutzername* und *Kennwort* für die Anmeldeinformationen eines CA Enterprise Log Manager-Benutzerkontos mit der Administratorrolle stehen.

   ```
   LMArchive -euser Benutzername -epassword Kennwort –list inc
   ```

Beispiel: Zeigen Sie alle aktuellen archivierten CA Enterprise Log Manager-Dateien an, die nicht als gesichert markiert sind

Mit dem folgenden, von einem Administrator ausgegebenen Befehl wird die Liste aller warmen Datenbanken abgefragt, die nicht als gesichert markiert sind.

```
LMArchive -euser Administrator1 -epassword calmr12 -list inc
```

Eine Liste mit Archivdateien, die nicht als gesichert markiert sind, wird in einem Format angezeigt, das mit dem folgenden vergleichbar ist:

```
Archivierte CAELM-Dateien (nicht gesichert):
    calm04_20091206192014.db.cerod
    calm04_20091206192014.db.sig
```

Durchführen von Sicherungen

Wenn Sie das System nicht so konfiguriert haben, dass die Dateien eines CA Enterprise Log Manager-Berichtsservers automatisch auf einem Offline-Server archiviert werden, der kein CA Enterprise Log Manager-Server ist, müssen die archivierten Datenbanken manuell gesichert und an einem sicheren Ort (Festplatte oder Server) gespeichert werden.

Wichtig! Sichern und verschieben Sie die Datenbanken, bevor sie vom CA Enterprise Log Manager-Berichtsserver *gelöscht* werden.

Warme Datenbanken werden automatisch gelöscht, wenn der festgelegte maximale Archivierungszeitraum erreicht wurde oder wenn der Anteil an Speicher unter den für den Archivfestplattenspeicher festgelegten Wert fällt. Um Datenverluste aufgrund der Löschung von Dateien zu vermeiden, sichern Sie Ihre Daten regelmäßig.

So sichern Sie warme Datenbanken manuell:

1. Melden Sie sich mit Ihren caelmadmin-Anmeldeinformationen an dem CA Enterprise Log Manager-Berichtsserver an, auf dem sich der Ereignisprotokollspeicher mit den gewünschten Datenbanken befindet.
2. Wechseln Sie vom Benutzer- in das Stammverzeichnis:

   ```
   su - root
   ```

3. Wechseln Sie zu folgendem Verzeichnis: /opt/CA/LogManager/data/archive.
4. Sichern Sie die warmen Datenbanken mit Hilfe des Sicherungsverfahrens Ihrer Wahl, und verschieben Sie die Datenbanken gemäß Ihren Anforderungen zur zwischenzeitlichen Aufbewahrung auf einen anderen Server oder zur langfristigen Aufbewahrung auf einen Offline-Server.

Aufzeichnen der Sicherungen

Zeichnen Sie jedes Mal, wenn Sie für eine oder mehrere archivierte Datenbanken eine Sicherung durchführen, diesen Vorgang in dem CA Enterprise Log Manager auf, in dem die Sicherung durchgeführt wurde.

Hinweis: Wenn Sie nicht jede Sicherung aufzeichnen, werden beim Auflisten von gesicherten Datenbanken mit Hilfe des Hilfsprogramms "LMArchive" falsche Daten gemeldet.

So zeichnen Sie die Sicherungen von bestimmten archivierten Datenbanken auf:

1. Melden Sie sich mit den "caelmadmin"-Anmeldeinformationen beim CA Enterprise Log Manager-Server mit dem Ereignisprotokollspeicher an, der die Datenbanken enthält, die Sie gesichert haben.
2. Lassen Sie die Benutzer an der Eingabeaufforderung folgendermaßen zum Root-Verzeichnis wechseln:

   ```
   su - root
   ```

3. Wechseln Sie mit dem folgenden Befehl zum Verzeichnis "/opt/CA/SharedComponents/iTechnology":

   ```
   cd $IGW_LOC
   ```

4. Führen Sie den folgenden Befehl aus, wobei *Benutzername* und *Kennwort* für die Anmeldeinformationen eines CA Enterprise Log Manager-Benutzerkontos mit der Administratorrolle stehen.

   ```
   LMArchive -euser Benutzername -epassword Kennwort –notify arch –files
   Datei1,Datei2,Datei3...
   ```

Beispiel: Benachrichtigen Sie CA Enterprise Log Manager, dass bestimmte Dateien gesichert wurden

Mit dem folgenden, vom Administrator mit dem Namen "Administrator1" ausgegebenen Befehl wird der CA Enterprise Log Manager-Ereignisprotokollspeicher benachrichtigt, dass die warme Datenbank "calm04_20091206192014.db.cerod" gesichert wurde. Gesicherte Datenbanken können zur langfristigen Aufbewahrung manuell in externe Speicher verschoben werden.

```
LMArchive -euser Administrator1 -epassword calmr12 -notify arch
-files calm04_20091206192014.db.cerod
```

Die Benachrichtigung über die Archivdatei wird in einem Format angezeigt, das dem folgenden gleicht:

```
Archivbenachrichtigung gesendet für Datei calm04_20091206192014.db.cerod...
```

Manuelles Wiederherstellen von Archiven im ursprünglichen Ereignisprotokollspeicher

Gelegentlich kann es vorkommen, dass Sie kalte Datenbankdateien zum Abfragen oder zum Erstellen eines Berichts im Archivverzeichnis auf einem CA Enterprise Log Manager-Server wiederherstellen müssen. Dies kann erforderlich sein, um eine Sicherheitslücke zu untersuchen oder um eine jährliche oder halbjährliche Prüfung der Einhaltung von Richtlinien durchzuführen. Die verwendeten Vorgehensweisen hängen von den folgenden beiden Fragen ab:

- Wurden die Dateien, die jetzt wiederhergestellt werden sollen, mit Hilfe der Autoarchivierung gesichert?
- Sollen die Dateien auf dem ursprünglichen Berichterstellungsserver oder auf einem anderen Server, wie etwa auf einem speziellen Wiederherstellungspunkt-Server, wiederhergestellt werden?

  Wenn die Dateien auf einem anderen Server wiederhergestellt werden sollen, lesen Sie den Abschnitt "Wiederherstellen von Archiven in einem neuen Ereignisprotokollspeicher".

Gehen Sie wie folgt vor, wenn die Dateien auf dem ursprünglichen Berichterstellungsserver wiederhergestellt werden sollen:

1. Bereiten Sie die Wiederherstellung von archivierten Datenbanken vor, indem Sie die wiederherzustellenden Dateien ermitteln und das Archivverzeichnis angeben.
2. Verschieben Sie die Datenbanken vom externen Speicher in das Archivverzeichnis auf dem für die Autoarchivierung konfigurierten Remote-Server oder auf den ursprünglichen Berichterstellungsserver.
3. Wenn Sie die archivierten Dateien auf den für die Autoarchivierung konfigurierten Remote-Speicherserver verschoben haben, melden Sie sich beim berichterstellenden CA Enterprise Log Manager an, und stellen Sie die automatisch archivierten Dateien vom Remote-Speicherserver mit dem Skript "restore-ca-elm.sh" wieder her.
4. Wenn Sie die archivierten Dateien in das Archivverzeichnis auf dem ursprünglichen berichterstellenden CA Enterprise Log Manager-Server verschoben haben, stellen Sie die manuell archivierten Dateien mit dem Hilfsprogramm "LMArchive" wieder her.
5. Überprüfen Sie, ob die verfügbar gemachte Datenbank abgefragt werden kann, indem eine Abfrage, bei der das Enddatum auf das Datum der wiederhergestellten Datenbank festgelegt ist, ausgeführt wird und die Abfrageergebnisse überprüft werden.

Weitere Informationen

Vorbereitung für die Wiederherstellung archivierter Datenbanken (siehe Seite 231)
Verschieben von archivierten Datenbanken in ein Archivverzeichnis (siehe Seite 233)
Wiederherstellen automatisch archivierter Dateien (siehe Seite 220)
Manuell archivierte Dateien wiederherstellen (siehe Seite 234)
Überprüfen der Wiederherstellung (siehe Seite 236)

Vorbereitung für die Wiederherstellung archivierter Datenbanken

Bevor Sie archivierte Datenbanken wiederherstellen, müssen Sie Folgendes wissen:

- die Namen der wiederherzustellenden Dateien;
- den Pfad des Archivverzeichnisses, in das Sie die vom externen Speicherort abgerufenen Dateien kopieren möchten. Der standardmäßige Pfad ist "/opt/CA/LogManager/data/archive".

Sie können den Archivkatalog über die CA Enterprise Log Manager-Verwaltungsregisterkarte "Protokollerfassungs-Explorer" abfragen, wo Sie einfache oder erweiterte Filter festlegen können. Sie können auch das Hilfsprogramm "Befehlszeile" verwenden wie hier beschrieben.

Wenn Sie die erforderlichen Informationen schon zur Hand haben, überspringen Sie dieses Verfahren.

So bereiten Sie die Wiederherstellung archivierter Datenbanken vor:

1. Melden Sie sich mit Ihren "caelmadmin"-Berechtigungsnachweisen bei dem CA Enterprise Log Manager-Server mit dem Ereignisprotokollspeicher an, wo Sie die Datenbanken wiederherstellen möchten.
2. Lassen Sie die Benutzer an der Eingabeaufforderung folgendermaßen zum Root-Verzeichnis wechseln:

   ```
   su - root
   ```

3. Wechseln Sie mit dem folgenden Befehl zum Verzeichnis "/opt/CA/SharedComponents/iTechnology":

   ```
   cd $IGW_LOC
   ```

4. Geben Sie aus einer Liste mit den Dateien, die gesichert und zu einem externen Speicherort verschoben worden sind, diejenigen Datenbanken an, die Sie wiederherstellen möchten. Um die Liste aller archivierten Dateien in diesem Archivkatalog anzuzeigen, führen Sie den folgenden Befehl aus, wobei "userid" und "pwd" die Berechtigungsnachweise für ein CA Enterprise Log Manager-Benutzerkonto mit Administratorrolle sind.

   ```
   LMArchive -euser userid -epassword pwd -list all
   ```

   Die Liste aller archivierten Dateien wird angezeigt.

5. (Optional) Wenn Sie die Wiederherstellung anhand manueller Sicherungen vornehmen, bestimmen Sie den Ablageort des Archivverzeichnisses, in das die identifizierten kalten Archivdateien kopiert werden sollen. Führen Sie den folgenden Befehl aus, wobei "userid" und "pwd" die Berechtigungsnachweise für ein CA Enterprise Log Manager-Benutzerkonto mit Administratorrolle sind.

   ```
   LMArchive -euser userid -epassword pwd -list loc
   ```

   Das Archivverzeichnis wird angezeigt.

Beispiel: Anzeigen aller aktuellen CA Enterprise Log Manager-Archivdateien

Durch den folgenden, vom CA Enterprise Log Manager-Administrator "Administrator1" herausgegebenen Befehl wird eine Liste aller Datenbanken angefordert, die im Archivverzeichnis des Ereignisprotokollspeichers vorhanden sind.

```
LMArchive -euser Administrator1 -epassword calmr12 -list all
```

Eine List der aktuellen Archivdateien wird angezeigt in einem Format, das dem folgenden ähnelt:

```
CAELM-Archivdateien:
    calm04_20091206191941.db.cerod
    calm04_20091206191958.db.cerod
    calm04_20091206192014.db.cerod
    calm04_20091206191941.db.sig
    calm04_20091206191958.db.sig
    calm04_20091206192014.db.sig
```

Beispiel: Anzeigen des CA Enterprise Log Manager-Archivverzeichnisses

Der folgende, von einem CA Enterprise Log Manager-Administrator, Administrator1, Befehl fordert den Verzeichnis-Ablageort der archivierten Datenbanken an:

```
LMArchive -euser Administrator1 -epassword calmr12 -list loc
```

Folgendes ist eine typische Antwort:

```
CAELM Archive Location (localhost) :
../../LogManager/data/archive
```

Weitere Informationen:

Abfragen des Archivkatalogs (siehe Seite 218)

Verschieben von archivierten Datenbanken in ein Archivverzeichnis

Wenn Sie die archivierten Dateien an einen Offsite-Speicherort verschoben haben, verwenden Sie die Verfahren Ihrer Site, um die Dateien abzurufen und wieder onsite zu bringen.

Verschieben Sie die archivierten Datenbanken wieder in das Archivverzeichnis des ursprünglichen CA Enterprise Log Manager-Servers oder in das Archivverzeichnis eines für die nicht interaktive Authentifizierung konfigurierten Remote-Servers. Das Archivverzeichnis lautet wie folgt: "/opt/ca/LogManager/data/archive".

So verschieben Sie eine archivierte Datenbank von einem externen Speicher in Ihr Netzwerk:

1. Sie haben eine der folgenden Möglichkeiten, die Datenbankdateien zum Wiederherstellen von einem externen Speicher wieder in Ihr Netzwerk zu verschieben:
   - Wenn Sie Ihre archivierten Dateien mit Hilfe der Autoarchivierung automatisch auf den Remote-Server verschieben, kopieren Sie sie wieder in das Archivverzeichnis auf diesem Remote-Server. (Dieser Remote-Server ist bereits für die nicht interaktive Authentifizierung bei dem CA Enterprise Log Manager-Server konfiguriert, auf dem die archivierten Datenbanken wiederhergestellt werden sollen.)
   - Wenn Sie die Autoarchivierung nicht verwenden, kopieren Sie Ihre archivierten Dateien wieder in das Archivverzeichnis auf dem ursprünglichen CA Enterprise Log Manager-Server.
2. Führen Sie je nach dem Speicherort der archivierten Dateien eines der folgenden Verfahren durch.
   - Wenn sich die archivierten Dateien auf dem Remote-Server befinden, der für die Autoarchivierung konfiguriert wurde, stellen Sie automatisch archivierte Dateien mit dem Skript "restore-ca-elm.sh" wieder her.
   - Wenn sich die archivierten Dateien im Archivverzeichnis auf dem ursprünglichen CA Enterprise Log Manager-Server befinden, benachrichtigen Sie CA Enterprise Log Manager, dass die archivierten Dateien mit dem Hilfsprogramm "LMArchive" wiederhergestellt wurden. Nach der Benachrichtigung werden die wiederhergestellten Dateien verfügbar gemacht.

Weitere Informationen:

Wiederherstellen automatisch archivierter Dateien (siehe Seite 220)
Manuell archivierte Dateien wiederherstellen (siehe Seite 234)

Manuell archivierte Dateien wiederherstellen

Nachdem Sie eine oder mehrere Datenbanken aus einem langfristigen Speicher im Archivverzeichnis wiederhergestellt haben, müssen Sie für den Besitzer des Archivverzeichnisses den Benutzer "caelmservice" angeben, bevor Sie CA Enterprise Log Manager benachrichtigen, dass die Datenbank mit dem Hilfsprogramm "LMArchive" wiederhergestellt wurde. Archivierte Dateien, die sich im Besitz von "root" befinden, werden vom Hilfsprogramm "LMArchive" nicht erkannt.

Wenn das Hilfsprogramm "LMArchive" mit der Option "-notify rest" ausgeführt wird, wird der Status der archivierten Datenbankdateien von "kalt" in "verfügbar gemacht" geändert, so dass diese Dateien für Abfragen und für die Berichterstellung verfügbar sind.

Der Administrator konfiguriert die Anzahl der Stunden, für die eine verfügbar gemachte archivierte Datenbank aufbewahrt wird, bevor sie automatisch aus dem archivierten Verzeichnis gelöscht wird. Hierzu verwendet er die Einstellung "Exportrichtlinie" in der Konfiguration des Services für den Ereignisprotokollspeicher.

So stellen Sie manuell archivierte Datenbankdateien wieder her:

1. Melden Sie sich mit den **caelmadmin**-Anmeldeinformationen beim CA Enterprise Log Manager-Server mit dem Ereignisprotokollspeicher an, der die wiederhergestellten Datenbanken enthält.
2. Lassen Sie die Benutzer an der Eingabeaufforderung folgendermaßen zum Root-Verzeichnis wechseln:

   ```
   su - root
   ```

3. Wechseln Sie zum Verzeichnis "/data". Beispiel:

   ```
   cd /opt/CA/LogManager/data
   ```

4. Weisen Sie dem Konto "caelmservice" die Besitzrechte des Archivverzeichnisses (/opt/CA/LogManager/data/archive) zu.

   ```
   chown -R caelmservice:caelmservice archive
   ```

   Der Besitz der Archivdateien wird auf "caelmservice", den internen Betriebssystembenutzer, übertragen, ein Konto, mit dem keine Anmeldung durchgeführt werden kann.

5. Wechseln Sie mit dem folgenden Befehl zum Verzeichnis "/opt/CA/SharedComponents/iTechnology":

   ```
   cd $IGW_LOC
   ```

6. Führen Sie den folgenden Befehl aus, wobei *Benutzername* und *Kennwort* für die Anmeldeinformationen eines CA Enterprise Log Manager-Benutzerkontos mit der Administratorrolle stehen.

   ```
   LMArchive -euser Benutzername -epassword Kennwort –notify rest –files
   Datei1,Datei2,Datei3
   ```

   Die Bestätigung der Wiederherstellung wird angezeigt. CA Enterprise Log Manager macht die angegebenen Dateien verfügbar. Verfügbar gemachte Dateien werden für die konfigurierte Anzahl an Stunden aufbewahrt, wobei eine Aufbewahrung von bis zu sieben Tagen konfiguriert werden kann.

Hinweis: Sie können nun die Ereignisdaten in den wiederhergestellten Archivdateien abfragen und mit diesen Daten Berichte erstellen.

Beispiel: Benachrichtigen Sie CA Enterprise Log Manager, dass bestimmte Datenbanken wiederhergestellt wurden

Mit dem folgenden Befehl, der von einem CA Enterprise Log Manager-Benutzer mit der Administratorrolle ausgegeben wird, wird der CA Enterprise Log Manager-Ereignisprotokollspeicher benachrichtigt, dass die angegebene kalte Datenbank, calm04_20091206192014.db, in das Archivverzeichnis kopiert wurde.

```
LMArchive -euser Administrator1 -epassword calmr12 -notify rest
-files calm04_20091206192014.db.cerod
```

Die Bestätigung der Wiederherstellung wird ein einem Format vergleichbar mit dem folgenden angezeigt:

```
Archivbenachrichtigung gesendet für Datei calm04_20091206192014.db.cerod
```

Überprüfen der Wiederherstellung

Sie können schnell überprüfen, ob die wiederhergestellte Datenbank für eine Untersuchung verfügbar ist. Dazu führen Sie eine schnelle Abfrage aus. Durch normale Abfragen werden Daten aus wiederhergestellten Datenbanken als warme und verfügbar gemachte Daten angezeigt.

Betrachten Sie folgenden Prozess:

1. Kopieren Sie eine Software-Update-Abfrage zur Anzeige des Typs von Ereignisdetails, der in der wiederhergestellten Datenbank gespeichert ist.
2. Fahren Sie mit dem Schritt des Assistenten für das Abfragedesign fort, in dem Sie Ergebnisbedingungen festlegen und einen Datumsbereich eingeben, der den gerade verfügbar gemachten Datenbankdateien entspricht.
3. Speichern Sie die Abfrage.
4. Führen Sie die Abfrage aus.

Manuelles Wiederherstellen von Archiven in neuem Ereignisprotokollspeicher

Gelegentlich kann es vorkommen, dass Sie kalte gespeicherte Dateien zum Abfragen oder zum Erstellen eines Berichts für eine jährliche oder halbjährliche Prüfung der Einhaltung von Richtlinien wiederherstellen müssen. Wenn Sie einen CA Enterprise Log Manager als Wiederherstellungspunkt für Untersuchungen von kalten Daten bestimmen, müssen Sie erzwingen, dass der Katalog jedes Mal neu erstellt wird, wenn Sie auf diesem CA Enterprise Log Manager eine neue Datenbank wiederherstellen. Die Neuerstellung des Katalogs oder Neukatalogisierung ist nur erforderlich, wenn Daten auf einem anderen Server wiederhergestellt werden als auf dem Server, auf dem sie erstellt wurden.

Wichtig! Stellen Sie sicher, dass die Einstellung "Maximale Anzahl an Archivtagen" für den Ereignisprotokollspeicher dieses Servers ausreichend ist. Andernfalls werden wiederhergestellte Dateien sofort gelöscht.

Eine Neukatalogisierung wird ggf. automatisch durchgeführt, wenn iGateway erneut gestartet wird. Wenn Datenbanken vor dem Herunterfahren von iGateway unvollständig katalogisiert wurden, wird die Neukatalogisierung beim Neustart von iGateway durchgeführt. Wenn eine oder mehrere Datenbanken zum Archivdatenbankverzeichnis hinzugefügt werden, während iGateway heruntergefahren ist, wird die Neukatalogisierung beim nächsten Start von iGateway durchgeführt.

Zum Wiederherstellen von archivierten Dateien von einem externen Speicher auf einem anderen CA Enterprise Log Manager als auf dem Server, auf dem sie gesichert wurden, sind folgende Schritte erforderlich:

1. Ermitteln der Datenbanken, die wiederhergestellt werden sollen. Unterstützung erhalten Sie, indem Sie den Archivkatalog mit Filtern abfragen.
2. Verschieben der ermittelten kalten Archivdateien aus dem externen Speicher in das eigene Netzwerk.
3. Kopieren der verschobenen Datenbanken in das Archivverzeichnis. Um das Archivverzeichnis anzuzeigen, führen Sie das Hilfsprogramm "LMArchive" mit der Option "-list loc" aus.
4. Erneutes Erstellen des Archivkatalogs (Neukatalogisieren).

   Das erneute Erstellen des Archivkatalogs zum Hinzufügen einer einzelnen Datenbank kann mehrere Stunden in Anspruch nehmen. Wenn Sie lange genug gewartet haben, bis die Neukatalogisierung abgeschlossen ist, können Sie die Untersuchung beginnen, indem Sie die Ereignisprotokolle aus den wiederhergestellten Datenbanken abfragen oder mit diesen Protokollen Berichte erstellen.
5. Überprüfen Sie die Wiederherstellung, indem Sie eine Abfrage ausgeben.

Hinweis: Wenn Sie einen CA Enterprise Log Manager als Wiederherstellungspunkt bestimmen, müssen Sie ihn aus der Föderation ausschließen.

Weitere Informationen:

Verschieben von archivierten Datenbanken in ein Archivverzeichnis (siehe Seite 233)
Konfigurieren der maximalen Anzahl an Archivtagen für wiederhergestellte Archive (siehe Seite 238)
Hinzufügen von wiederhergestellten Datenbanken zum Katalog (siehe Seite 239)
Überprüfen der Wiederherstellung (siehe Seite 236)
Beispiel: Einem Nicht-Administrator gestatten, Archive zu verwalten (siehe Seite 122)

Konfigurieren der maximalen Anzahl an Archivtagen für wiederhergestellte Archive

Wenn Sie den Ereignisprotokollspeicher für eine als Wiederherstellungspunkt genutzte CA Enterprise Log Manager-Ressource konfigurieren, empfiehlt es sich, die globale Einstellung für "Maximale Anzahl an Archivtagen" außer Kraft zu setzen und auf den maximalen Wert (28000) einzustellen. Falls die Anzahl von Tagen, für die archivierte Datenbankdateien gespeichert werden sollen, bevor sie gelöscht werden, auf einen niedrigeren Wert als das Alter der wiederhergestellten Datenbankdateien festgelegt ist, werden diese Dateien vom System sofort gelöscht, nachdem sie als warme Dateien wiederhergestellt wurden.

Hinweis: Diese Vorgehensweise gilt nur für Dateien, die in einem neuen Ereignisprotokollspeicher wiederhergestellt werden.

So legen Sie die maximale Anzahl an Archivtagen fest, um das Alter der wiederhergestellten Dateien zu berücksichtigen:

1. Klicken Sie auf die Registerkarte "Verwaltung" und auf die Unterregisterkarte "Services".
2. Blenden Sie in der Service-Liste den Ordner "Ereignisprotokollspeicher" ein, und wählen Sie die CA Enterprise Log Manager-Ressource aus, die als dedizierter Wiederherstellungspunkt dient.
3. Klicken Sie neben "Maximale Anzahl an Archivtagen" auf die Taste zum Umschalten, um zur lokalen Konfiguration zu wechseln und das Eingabefeld zu aktivieren.
4. Stellen Sie das Feld für die Anzahl von Tagen auf einen Wert ein, bei dem die älteste wiederherzustellende Datei berücksichtigt wird. Der maximale Wert ist 28000.
5. Klicken Sie auf "Speichern".

Hinzufügen von wiederhergestellten Datenbanken zum Katalog

Wenn Sie die wiederhergestellte Datenbank direkt in das Archivverzeichnis auf einem anderen Server kopieren – also nicht auf dem Server, auf dem die Datenbank erstellt wurde –, erstellen Sie den Archivkatalog neu, um die wiederhergestellte Datenbank hinzuzufügen.

Verwenden Sie in den folgenden Fällen *nicht* die Funktion "Neukatalogisieren":

- Wenn Sie eine archivierte Datenbank mithilfe des Skripts "restore-ca-elm.sh" wiederherstellen. Das Wiederherstellungs-Shellskript führt die Neukatalogisierung für Sie aus.
- Wenn Sie die wiederhergestellte Datenbank direkt in das Archivverzeichnis auf dem Server kopieren, auf dem sie auch generiert wurde, und CA Enterprise Log Manager dann mit dem Hilfsprogramm "LMArchive" mit der Option "-notify rest" darüber informieren, dass die Datenbank wiederhergestellt wurde.

Durch den Neukatalogisierungsprozess wird die wiederhergestellte Datenbank zu einer "warmen" Datenbank – und nicht, wie bei der Option "-notify rest" des Hilfsprogramms "LMArchive", zu einer "verfügbar gemachten" Datenbank. Daher gelten hier die üblichen Archivierungsregeln und nicht die in der Konfiguration des Ereignisprotokollspeichers festgelegte Exportrichtlinie.

So erstellen Sie den Archivkatalog neu, um die wiederhergestellte Datenbank hinzuzufügen:

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

   Der Ordner "Archiv-Verwaltung" wird angezeigt.

2. Klicken Sie auf den Ordner "Archivabfrage und Neukatalogisierung".

   Über den Registerkarten "Schnellfilter" und "Erweiterte Filter" werden drei Schaltflächen angezeigt, darunter die Schaltfläche "Neukatalogisieren".

3. Klicken Sie auf "Neukatalogisieren".

   Es wird eine Meldung angezeigt, dass die Bestätigung erfolgreich war. Die wiederhergestellte Datenbank wird dem Katalog als warme Datenbank hinzugefügt.

Weitere Informationen:

Beispiel: Einem Nicht-Administrator gestatten, Archive zu verwalten (siehe Seite 122)

LMArchive – Verfolgung der Sicherung/Wiederherstellung

LMArchive ist das Befehlszeilentool, das die Sicherung und Wiederherstellung von warmen Datenbanken im Ereignisprotokollspeicher auf einem CA Enterprise Log Manager-Server verfolgt. Mit "LMArchive" können Sie die Liste der warmen Datenbankdateien abfragen, die für die Archivierung bereit sind. Nachdem Sie die aufgelistete Datenbank gesichert und in den langfristigen (kalten) Speicher verschoben haben, erstellen Sie mit "LMArchive" einen Datensatz auf dem CA Enterprise Log Manager-Server, auf dem diese Datenbank gesichert wurde. Nach der Wiederherstellung einer kalten Datenbank auf dem ursprünglichen CA Enterprise Log Manager-Server benachrichtigen Sie CA Enterprise Log Manager mit Hilfe von "LMArchive". Hierdurch werden die Dateien der kalten Datenbank verfügbar gemacht und so in einen Zustand versetzt, in dem sie abgefragt werden können.

Der Befehl besitzt das folgende Format:

```
LMArchive -euser Benutzername -epassword pwd {-list [loc|all|inc] | -notify
[arch|rest] -files Datei1,Datei2,Datei3...}
```

-euser *Benutzername*

Gibt den Benutzernamen eines CA Enterprise Log Manager-Benutzerkontos an, dem die Administratorrolle zugewiesen ist

-epassword *Kennwort*

Gibt das CA Enterprise Log Manager-Kennwort an, das dem Benutzernamen zugewiesen ist

-list [loc | all | inc]

Fordert eine Liste folgender Elemente an: Speicherorte der Archivverzeichnisse, Namen aller warmen und kalten Datenbanken oder Namen nur der warmen Datenbanken.

-loc

Fordert den Speicherort des Archivverzeichnisses an.

all

Fordert eine Liste aller Dateinamen an, die sich im Archivverzeichnis des Ereignisprotokollspeichers befinden.

inc

Fordert eine inkrementelle Liste der Namen der aktuellen Dateien in der warmen Datenbank an, die nicht archiviert wurden. Die Anforderung gibt die Namen der Dateien zurück, die nicht gesichert, in externen Speicher verschoben und in den kalten Status versetzt wurden. Dateien werden in den kalten Status versetzt, wenn die Benachrichtigung über die Verschiebung durch den Benachrichtigungsbefehl dieses Hilfsprogramms eingeht.

-notify [arch | rest]

Benachrichtigt den CA Enterprise Log Manager-Ereignisprotokollspeicher, dass die angegebenen Dateien erfolgreich gesichert beziehungsweise wiederhergestellt wurden.

arch

Benachrichtigt den CA Enterprise Log Manager-Ereignisprotokollspeicher, dass die angegebenen Dateien erfolgreich gesichert wurden.

rest

Benachrichtigt den CA Enterprise Log Manager-Ereignisprotokollspeicher, dass die angegebenen Dateien erfolgreich wiederhergestellt wurden.

-files *Datei1*,*Datei2*,*Datei3* ...

Gibt die Namen der Datenbankdateien an, die gesichert beziehungsweise wiederhergestellt wurden

Weitere Informationen

Info zur Protokollspeicherung (siehe Seite 200)
Ermitteln von nicht gesicherten Datenbanken (siehe Seite 225)
Aufzeichnen der Sicherungen (siehe Seite 227)
Vorbereitung für die Wiederherstellung archivierter Datenbanken (siehe Seite 231)
Manuell archivierte Dateien wiederherstellen (siehe Seite 234)

Kapitel 7: Abonnement

Dieses Kapitel enthält folgende Themen:

Aktualisierung auf CA Enterprise Log Manager-Version 12.5 durch Software-Update

Um CA Enterprise Log Manager auf Version 12.5 zu aktualisieren, führen Sie zuerst eine Aktualisierung auf die Version 12.5 des Log Manager-Produkts durch, und aktualisieren Sie dann alle anderen CA Enterprise Log Manager-Module, wie Inhalts-, Integrations- und Agent-Module. Sie führen alle Aktualisierungstasks über das automatische Software-Update durch.

Wichtig! Führen Sie ein Upgrade für den CA Enterprise Log Manager-Verwaltungsserver durch, bevor Sie andere CA Enterprise Log Manager-Server in Ihrem Netzwerk installieren. Dies ermöglicht es den neuen Servern, sich richtig zu registrieren.

So aktualisieren Sie auf CA Enterprise Log Manager-Version 12.5

1. Aktualisieren Sie auf Log Manager-Version 12.5

   Hinweis: Die aktualisierte CA Enterprise Log Manager-12.5-Benutzeroberfläche listet unter der Unterregisterkarte "Services" der Registerkarte "Verwaltung" sowohl das Modul als auch den Service für automatische Software-Updates auf. "Modul für automatische Software-Updates" bezieht sich auf die Schnittstelle und Funktionalität vor der Aktualisierung auf 12.5, und dient dazu, während der Aktualisierung auf 12.5 für einwandfreie Kommunikation zwischen allen CA Enterprise Log Manager-Servern zu sorgen. Sobald Sie das Log Manager-Produkt auf einem bestimmten CA Enterprise Log Manager-Server auf Version 12.5 aktualisiert haben, verwenden Sie nur den Service für automatische Software-Updates, um alle weiteren Aktualisierungsaufgaben und Konfigurationsänderungen durchzuführen.

2. Aktualisieren Sie alle anderen CA Enterprise Log Manager-Module.

   Wichtig! Nachdem Sie Schritt 1 ausgeführt haben, listet die aktualisierte CA Enterprise Log Manager-12.5-Benutzeroberfläche sowohl das Modul als auch den Service für automatische Software-Updates auf. Verwenden Sie nur den Service für automatische Software-Updates, nicht das Modul, um alle weiteren Software-Update-Aufgaben einschließlich dieses Schrittes durchzuführen. Das Modul für automatische Software-Updates dient nur dazu, während des Upgrades auf 12.5 für einwandfreie Kommunikation zwischen allen CA Enterprise Log Manager-Servern zu sorgen; verwenden Sie es nicht zur Ausführung von Post-Upgrades an Software-Update-Funktionen.

3. Wenn sich unter den Aktualisierungen Agent- oder Connector-Module befanden, installieren Sie die aktualisierten Agents oder Connectors.

4. Registrieren Sie Produkte von Drittanbietern und andere CA-Produkte wie z. B. CA Access Control, die auf ihren systemeigenen Benutzeroberflächen CA Enterprise Log Manager-Berichte durch Aufrufe über offene Schnittstellen anzeigen, erneut.

   Nach diesem Schritt werden die Zertifikate aktualisiert, die sich in dieser Version geändert haben. Weitere Informationen finden Sie im *CA Enterprise Log Manager - API-Programmierhandbuch*.

Hinweis: Weitere Informationen über die Ausführung dieser Schritte finden Sie unter *Aktualisierung auf CA Enterprise Log Manager-Version 12.5 durch Software-Update* in den *Versionshinweisen für CA Enterprise Log Manager 12.5*. Überprüfen Sie die Versionshinweise auch auf bekannte Probleme im Zusammenhang mit automatischen Software-Updates.

Weitere Informationen:

Automatische Software-Updates auf Agenten und Connectors anwenden (siehe Seite 266)

Globalen Status automatischer Software-Updates anzeigen

Der Service für automatische Software-Updates lädt ausgewählte Aktualisierungsmodule herunter und verteilt sie entweder entsprechend einem Ablaufplan, den Sie konfigurieren, oder als Folge eines Updates nach Bedarf an Ihre CA Enterprise Log Manager-Server. Sie können den aktuellen Status automatischer Software-Updates Ihrer CA Enterprise Log Manager-Server über das Dashboard für automatische Software-Updates anzeigen.

Das Dashboard für automatische Software-Updates zeigt den Fortschritt aller Aktualisierungen an, die ein CA Enterprise Log Manager-Server derzeit herunterlädt oder installiert. Sie können auch den Status aller Inhaltsaktualisierungen, die derzeit ausgeführt werden, sowie eine Liste aller zu einem früheren Zeitpunkt installierten Inhaltsaktualisierungen anzeigen.

So zeigen Sie den globalen Status von Software-Updates an

1. Klicken Sie auf die Registerkarte "Verwaltung" und auf die Unterregisterkarte "Services".
2. Klicken Sie auf "Automatisches Software-Update - Service".

   Die Globale Service-Konfiguration für den Service automatischer Software-Updates wird angezeigt und die Registerkarte "Dashboard für automatische Software-Updates" ist ausgewählt.
3. Um den Status von Inhaltsaktualisierungen anzuzeigen, prüfen Sie das Fenster "Inhaltsstatus des automatischen Software-Updates".

   Wenn derzeit eine Inhaltsaktualisierung durchgeführt wird, zeigen eine Statusanzeige und Statusmeldungen den Status der Aktualisierung an. Klicken Sie auf die Schaltfläche "Aktualisieren", um den jüngsten Fortschritt der Aktualisierung anzuzeigen.
4. Um eine Liste aller bis zum derzeitigen Zeitpunkt installierten Inhaltsaktualisierungen anzusehen, klicken Sie auf "Katalog durchsuchen".

   Das Fenster "Inhalt" wird angezeigt. Klicken Sie auf einen Inhaltstyp, um von allen bis zum derzeitigen Zeitpunkt installierten zugehörigen Aktualisierungen den Namen, das Datum und die Version anzuzeigen.

5. Um den Status automatischer Software-Updates eines beliebigen CA Enterprise Log Manager-Servers anzuzeigen, prüfen Sie das Fenster "Server".

   Wenn auf einem beliebigen CA Enterprise Log Manager-Server eine Aktualisierung in Bearbeitung ist, wird für den jeweiligen Server eine Statusanzeige in der Spalte "Fortschritt" angezeigt. Klicken Sie auf die Schaltfläche "Aktualisieren", um den jüngsten Fortschritt der Aktualisierung anzuzeigen.

   Das Server-Fenster zeigt auch Informationen über jeden CA Enterprise Log Manager-Server an, wie:

   Status

   Zeigt den Status automatischer Software-Updates eines bestimmten CA Enterprise Log Manager-Servers an. Vorhandene Status automatischer Software-Updates sind "Leerlauf", "Im Wartezustand", "Wird heruntergeladen", "Wird installiert", "Abgeschlossen" und "Fehlgeschlagen".

   Meldung

   Zeigt jede Meldung über den Status automatischer Software-Updates eines bestimmten CA Enterprise Log Manager-Servers an.

   Datum

   Zeigt das Datum der letzten Aktualisierung an, die von einem bestimmten CA Enterprise Log Manager-Server ausgeführt wurde.

Anzeigen des Status für automatische Software-Updates eines Servers

Der Service für automatische Software-Updates lädt ausgewählte Aktualisierungsmodule herunter und verteilt sie entweder entsprechend einem Ablaufplan, den Sie konfigurieren, oder als Folge eines Updates nach Bedarf an Ihre CA Enterprise Log Manager-Server. Sie können den aktuellen Status der automatischen Software-Updates eines bestimmten CA Enterprise Log Manager-Servers über das globale Dashboard für automatische Software-Updates, oder durch das lokale Statusfenster des Servers anzeigen.

So zeigen Sie den Status für automatische Software-Updates eines CA Enterprise Log Manager-Servers an

1. Klicken Sie auf die Registerkarte "Verwaltung" und auf die Unterregisterkarte "Services".
2. Klicken Sie auf "Automatisches Software-Update - Service".

   Die Globale Service-Konfiguration für den Service automatischer Software-Updates wird angezeigt und die Registerkarte "Dashboard für automatische Software-Updates" ist ausgewählt.
3. Führen Sie einen der folgenden Schritte aus:

   - Prüfen Sie im Fenster "Server" die Statusinformation für den gewünschten Server. Wenn eine Aktualisierung in Bearbeitung ist, wird für den jeweiligen Server eine Statusanzeige in der Spalte "Fortschritt" angezeigt. Klicken Sie auf die Schaltfläche "Aktualisieren", um den aktuellen Fortschritt anzuzeigen. Das Fenster "Server" zeigt auch Zusatzinformationen für jeden CA Enterprise Log Manager-Server, einschließlich Status, Nachricht und Datum an.

   oder

   - Ausführlichere Informationen erhalten Sie, wenn Sie im Fenster "Server" auf den Namen des gewünschten Servers klicken, um das lokale Statusfenster dieses Servers zu öffnen. Wenn eine Aktualisierung in Bearbeitung ist, öffnen sich im Status-Fenster eine Statusanzeige und Statusmeldungen, die den Fortschritt der Aktualisierung anzeigen. Klicken Sie auf die Schaltfläche "Aktualisieren", um den aktuellen Fortschritt anzuzeigen. Das Server-Fenster zeigt auch Informationen über jeden CA Enterprise Log Manager-Server an, wie:

Status

Zeigt den Status automatischer Software-Updates eines bestimmten CA Enterprise Log Manager-Servers an. Vorhandene Status automatischer Software-Updates sind "Leerlauf", "Im Wartezustand", "Wird heruntergeladen", "Wird installiert", "Abgeschlossen" und "Fehlgeschlagen".

Meldung

Zeigt jede Meldung über den Status automatischer Software-Updates eines bestimmten CA Enterprise Log Manager-Servers an.

Datum

Zeigt das Datum der letzten Aktualisierung an, die von einem bestimmten CA Enterprise Log Manager-Server ausgeführt wurde.

Bearbeiten der globalen Konfiguration für automatische Software-Updates

Während der Implementierungsphase können Sie globale Einstellungen für automatische Software-Updates in Ihrer Umgebung konfigurieren. Alle CA Enterprise Log Manager-Server übernehmen und verwenden diese globalen Einstellungen, außer wenn Sie eine globale Einstellung durch das Konfigurieren lokaler Einstellungen für einen individuellen Server überschreiben.

Der erste installierte Server ist standardmäßig der Proxy für automatische Software-Updates. Alle danach installierten Server werden als Clients für automatische Software-Updates konfiguriert. Wenn kein anderer Proxy konfiguriert wird oder verfügbar ist, lädt der Standard-Proxy Aktualisierungen auf Clients für automatische Software-Updates herunter.

Sie können die globalen Einstellungen jederzeit ändern. Alle Server übernehmen eventuelle Änderungen, außer wenn ein bestimmter Server lokal konfiguriert wird, um jene Einstellungen zu überspringen.

Folgende Einstellungen können nur auf globaler Ebene festgelegt und bearbeitet werden:

- Standard-Proxy für automatische Software-Updates
- Öffentlicher Schlüssel – Version
- Proxy(s) für automatische Software-Updates für Inhaltsaktualisierungen

So bearbeiten Sie die globale Konfiguration für automatische Software-Updates:

1. Klicken Sie auf die Registerkarte "Verwaltung" und auf die Unterregisterkarte "Services".
2. Klicken Sie auf "Service automatischer Software-Updates".

   Die globale Service-Konfiguration für den Service automatischer Software-Updates wird angezeigt.
3. Klicken Sie auf die Registerkarte "Verwaltung".
4. Prüfen Sie die Einstellungen unter "Globale Service-Konfiguration: Service automatischer Software-Updates" im rechten Fensterbereich. Überprüfen Sie die Einstellungen und nehmen Sie gegebenenfalls Änderungen vor.

   Hinweis: Details zu den einzelnen Feldern finden Sie in der Online-Hilfe.
5. Klicken Sie auf "Speichern".

Weitere Informationen:

Anwenden automatischer Software-Updates (siehe Seite 711)

Bearbeiten der lokalen Konfiguration automatischer Software-Updates eines Servers

Bei der Implementierung automatischer Software-Updates können Sie globale Einstellungen für automatische Software-Updates, wie einen Ablaufplan und eine Proxy-Liste, für Ihre Umgebung konfigurieren. Die einzelnen CA Enterprise Log Manager-Server übernehmen diese globalen Einstellungen.

Sie können globale Einstellungen jederzeit durch das Konfigurieren lokaler Einstellungen für einen individuellen Server überschreiben. Berücksichtigen Sie die Rolle eines Servers im Rahmen der automatischen Software-Updates, wenn Sie planen, globale Einstellungen außer Kraft zu setzen.

So bearbeiten Sie die Konfiguration automatischer Software-Updates eines Servers

1. Klicken Sie auf die Registerkarte "Verwaltung" und auf die Unterregisterkarte "Services".
2. Erweitern Sie den Service für automatische Software-Updates und wählen Sie den zu konfigurierenden Server aus.

   Die Konfiguration des Services automatischer Software-Updates wird für den ausgewählten CA Enterprise Log Manager-Server angezeigt.
3. Klicken Sie auf die Registerkarte "Verwaltung".

4. Wenn Sie die Rolle des Servers für automatische Software-Updates ändern möchten, führen Sie einen der folgenden Schritte aus:

   - Um den Server als Client für automatische Software-Updates festzulegen, deaktivieren Sie das Kontrollkästchen "Proxy für automatische Software-Updates".
   - Um ihn als Online-Proxy für automatische Software-Updates festzulegen, aktivieren Sie das Kontrollkästchen "Proxy für automatische Software-Updates", und wählen Sie "Online-Proxy für automatische Software-Updates" aus.
   - Um ihn als Offline-Proxy für automatische Software-Updates festzulegen, aktivieren Sie das Kontrollkästchen "Proxy für automatische Software-Updates", und wählen Sie "Offline-Proxy für automatische Software-Updates" aus.

   Hinweis: Bevor Sie die Rolle eines Servers von "Proxy für automatische Software-Updates" auf "Client für automatische Software-Updates" abändern, berücksichtigen Sie die Konfigurationen der Clients für automatische Software-Updates, die diesen Proxy verwenden. Wenn Sie einen Server von Proxy auf Client ändern, entfernen Sie den Server sofort aus der globalen und lokalen Liste "Proxy(s) für automatische Software-Updates zur Client-Aktualisierung".

   Wichtig! Bevor Sie die Rolle eines Servers auf Offline-Proxy für automatische Software-Updates ändern, überlegen Sie, ob der Server in irgendeiner Proxy-Liste enthalten ist. In einer gemischten Umgebung automatischer Software-Updates, in der sowohl Offline- als auch Online-Proxys konfiguriert sind, nehmen Sie keine Offline-Proxys in die Proxy-Liste für Online-Clients auf.

5. Um eine übernommene globale Einstellung zu überschreiben, klicken Sie auf die Schaltfläche zur globalen/lokalen Konfiguration, um für das ausgewählte Feld auf lokale Servicekonfiguration umzuschalten.

   Hinweis: Zum Wiederherstellen der globalen Einstellung klicken Sie erneut auf die Schaltfläche. Die globale Einstellung wird zur Startzeit der nächsten Aktualisierung wiederhergestellt.

6. Wenn sich die Module, die Sie für diesen Server herunterladen möchten, von den Einstellungen unterscheiden, die von den globalen Einstellungen übernommen wurden, schalten Sie zur lokalen Konfiguration, klicken Sie auf "Durchsuchen" und wählen Sie die gewünschten Module aus.

   Hinweis: Stellen Sie sicher, dass die für diesen Proxy ausgewählten Module mindestens alle diejenigen Module einschließen, die in den Download-Listen der Clients enthalten sind, die von diesem Proxy Aktualisierungen erhalten.

7. Falls dieser Server Software-Updates über einen HTTP-Proxy-Server herunterladen soll, der nicht dem übernommenen Server entspricht, wechseln Sie zur lokalen Konfiguration und konfigurieren Sie den gewünschten HTTP-Proxy-Server.
8. Wenn dieser Server nach einem anderen Ablaufplan, als dem übernommenen, Aktualisierungen herunterladen soll, wechseln Sie auf die lokale Konfiguration und bearbeiten Sie den Ablaufplan.
9. Wenn dieser Server Aktualisierungen von einem anderen CA Enterprise Log Manager-Proxy für automatische Software-Updates herunterladen soll, wechseln Sie zur lokalen Konfiguration und fügen Sie die gewünschten CA Enterprise Log Manager-Proxy-Server zur Liste der Proxy(s) für Client-Aktualisierungen hinzu.

   Dieser Server nimmt Verbindung mit den festgelegten Proxy-Servern auf, um automatische Software-Updates herunterzuladen und eine abgestufte Proxy-Struktur erstellen.
10. Klicken Sie auf "Speichern".

Herunterladen und Auswählen von Modulen für automatische Software-Updates im Offline-Modus

Dateien der automatischen Software-Updates im Offline-Modus sind auf der CA-FTP-Seite für automatische Software-Updates im Offline-Modus, in ZIP-Dateien verpackt, verfügbar. Sobald neue Module verfügbar sind, werden sie auf der FTP-Seite angezeigt. Überwachen Sie die Liste der verfügbaren Module in regelmäßigen Abständen, um sicherzustellen, dass Sie die letzten Aktualisierungen heruntergeladen haben. Sie können auch unter http://ca.com/de/support die CA Support-Website aufrufen, um zu erfahren, wann neue Log Manager Service Packs und Versionen verfügbar sind.

Bevor Sie Module auswählen können, um Offline-Proxys für automatische Software-Updates herunterzuladen, laden Sie das Paket der Dateien der automatischen Software-Updates von der CA-FTP-Seite herunter und kopieren Sie es manuell für Ihre Offline-Proxys. Anschließend können Sie auswählen, welche Module heruntergeladen und installiert werden. Clients für automatische Software-Updates im Offline-Modus erhalten, im Gegensatz dazu, automatisch alle Aktualisierungen, die auf ihren Offline-Proxys manuell installiert sind. Dabei spielen die ausgewählten Module für den Client auf der lokalen Ebene keine Rolle.

So laden Sie automatische Software-Updates im Offline-Modus herunter und wählen sie aus

1. Navigieren Sie auf einem System mit Internet- oder FTP-Zugriff zum Speicherort des automatischen Software-Updates im Offline-Modus:

   ftp://ftp.ca.com/pub/elm/connectors/ftp/outgoing/pub/elm/ELM_Offline_Subscription

   Der Verzeichnisindex zeigt einen Ordner für jede größere CA Enterprise Log Manager-Version an.

2. Laden Sie die entsprechende ZIP-Datei, die Sie ausführen möchten, für die Aktualisierung herunter.

   Hinweis: Der Ordner für die CA Enterprise Log Manager-Version r12.5 enthält einen Unterordner sowie eine ZIP-Datei. Der Unterordner enthält Module zum Durchführen von Upgrades von Vorgängerversionen auf die Version r12.5. Die ZIP-Datei enthält die Module für die Ausführung routinemäßiger, periodischer Aktualisierungen auf die Version r12.5. Wenn Sie mithilfe eines automatischen Software-Updates im Offline-Modus ein Upgrade von einer Vorgängerversion auf r12.5 durchführen möchten, finden Sie weitere Informationen dazu im Abschnitt "Upgrade auf CA Enterprise Log Manager" in den *Versionshinweisen*. Wenn Sie eine routinemäßige Aktualisierung ausführen, wählen Sie die ZIP-Datei aus.

3. Wenn Sie physische Datenträger wie eine Festplatte oder scp verwenden, kopieren Sie die ZIP-Datei manuell in den folgenden Dateipfad auf Ihren Offline-Proxys:

   /opt/CA/LogManager/data/subscription/offline

4. Melden Sie sich in Ihrer CA Enterprise Log Manager-Umgebung beim System an.

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

6. Erweitern Sie den Service für automatische Software-Updates, und wählen Sie den zu konfigurierenden Offline-Proxy-Server aus.

   Die Konfiguration des Services automatischer Software-Updates wird für den ausgewählten CA Enterprise Log Manager-Server angezeigt.

   Hinweis: Clients für automatische Software-Updates im Offline-Modus erhalten alle Module, die manuell auf ihren Offline-Proxys installiert sind. Die Inhalte des Proxy-Servers steuern, welche Aktualisierungen der Client für automatische Software-Updates erhält. Auf lokaler Ebene für einen Offline-Client ausgewählte Module haben keine Auswirkung.

7. Klicken Sie auf die Registerkarte "Verwaltung".
8. Wählen Sie im Drop-down-Menü "Datei" die ZIP-Datei der Offline-Aktualisierung aus, die Sie auf den Server kopiert haben, und klicken Sie auf "Durchsuchen".

   Das Dialogfeld "Zum Download verfügbare Module" wird angezeigt.
9. Wählen Sie die Module aus, die Sie aktivieren möchten.
10. Klicken Sie auf "OK".

    Das Dialogfeld "Zum Download verfügbare Module" schließt sich, und die Module, die Sie auswählen, werden in der Liste "Zum Download ausgewählte Module" angezeigt.
11. Klicken Sie auf "Speichern".

    Clients für automatische Software-Updates im Offline-Modus können diese Module jetzt automatisch entsprechend dem festgelegten Ablaufplan für automatische Software-Updates herunterladen, oder sie je nach Bedarf herunterladen, wenn Sie eine manuelle Aktualisierung beginnen.
12. (Optional) Klicken Sie auf "Jetzt aktualisieren".

    Der Offline-Proxy-Server aktualisiert sich selbst mit den ausgewählten Modulen.

    Hinweis: Obwohl Sie zulassen können, dass der Offline-Proxy sich entsprechend dem festgelegten Ablaufplan für automatische Software-Updates selbst aktualisiert, wird es empfohlen, immer eine manuelle Aktualisierung durchzuführen, wenn Sie neue Dateien übertragen. Damit stellen Sie sicher, dass die Aktualisierungen verfügbar sind, wenn sie von Clients für automatische Software-Updates im Offline-Modus abgefragt werden.

Info zu On-Demand-Aktualisierungen

Eine On-Demand-Aktualisierung unterscheidet sich von einer geplanten Aktualisierung, da es sofort ausgeführt wird und nur den ausgewählten Server aktualisiert. Eine On-Demand-Aktualisierung kann nicht für mehrere CA Enterprise Log Manager-Server gleichzeitig ausgeführt werden. Bevor Sie auf einem Client für automatische Software-Updates eine On Demand-Aktualisierung ausführen, aktualisieren Sie zuerst den entsprechenden Proxy-Server.

Normalerweise sind die Binärdateien Ihrer Server und die Konfigurations- und Inhaltsdateien Ihres Verwaltungsservers im Rahmen der automatischen Software-Updates immer auf dem neuesten Stand. Manchmal kann es sinnvoll sein, eine außerplanmäßige Aktualisierung für einen einzelnen Server auszuführen.

In den folgenden Fällen wird eine On-Demand-Aktualisierung empfohlen:

- Für den Verwaltungsserver wird ein Fehler oder eine Warnung für das automatische Software-Update berichtet. Beispiel:

  ```
  Verbindung zu EEM-Server konnte nicht hergestellt werden
  ```

  ```
  Fehler beim Installieren von Inhalt in EEM
  ```

  Wählen Sie den Verwaltungsserver aus, und klicken Sie auf "Aktualisieren". Wenn der Verwaltungsserver als Proxy für Inhaltsaktualisierungen konfiguriert wird, importiert der Server neue Aktualisierungen vom CA-Server für automatische Software-Updates. Dann überträgt der Server die Inhaltsaktualisierungen an das Inhalts-Repository. Wenn dieser Server als Proxy für Clients konfiguriert wird, werden die binären Aktualisierungen für seine Clients nach dem Prinzip "First Come, First Served" verfügbar.

  Hinweis: Alternativ können Sie bis zur nächsten geplanten Aktualisierungssitzung warten, wenn eine unvollständige Verarbeitung wieder aktiv wird und sich vervollständigt.

- Ein Fehler bei automatischen Software-Updates weist darauf hin, dass der Download abgebrochen wurde. Wenn der Download nur auf einem Proxy-Server abgebrochen wurde, kann er durch eine On-Demand-Aktualisierung neu versucht werden. Eine On-Demand-Aktualisierung ist sinnvoll, wenn Sie den Fehler kurz nach dessen Auftreten entdecken. Wenn die Startzeit zwischen Proxy und Client ausreicht, kann eine On-Demand-Aktualisierung des Proxy abgeschlossen werden, bevor die geplante Aktualisierung durch die Clients beginnt, die Aktualisierungen von diesem Proxy erhalten.

- Sie installieren einen neuen CA Enterprise Log Manager, konfigurieren ihn als Proxy und möchten sicherstellen, dass die aktuellen Aktualisierungen angewendet werden, bevor Sie ihn verwenden.
- Sie stellen fest, dass ein Modul, das von einem Client benötigt wird, nicht als herunterzuladendes Modul ausgewählt war. Jedoch wurde dieses Modul als ein Modul ausgewählt, das vom Proxy heruntergeladen werden soll. Durch "Jetzt aktualisieren" auf dem Client werden die fehlenden Updates installiert.
- Sie haben ein Offline-Paket für automatische Software-Updates heruntergeladen und es auf einen Offline-Proxy kopiert. Mithilfe einer manuellen Aktualisierung auf dem Offline-Proxy bei jedem Transfer neuer Dateien, stellen Sie sicher, dass die Aktualisierungen verfügbar sind, wenn Offline-Clients für automatische Software-Updates sie anfordern.

Starten eines Updates nach Bedarf

Mit der Funktion "Jetzt aktualisieren" können Sie Server nach Bedarf aktualisieren. Wenn Sie zwei oder mehr Server nacheinander aktualisieren, stellen Sie sicher, dass der Vorgang auf einem Server abgeschlossen ist, bevor Sie mit dem Vorgang auf dem nächsten Server fortfahren. Überprüfen Sie zur Bestätigung selbstüberwachende Ereignisse.

Wenn Sie kürzlich konfigurierte Werte für automatische Software-Updates ändern, müssen Sie warten, bis das Aktualisierungsintervall (standardmäßig 300 Sekunden) vergangen ist, bevor Sie eine On-Demand-Aktualisierung ausführen. CA Enterprise Log Manager generiert nach Abschluss des Updates ein sich selbst überwachendes Ereignis.

Hinweis: Wenn ein geplantes Update ausgeführt wird, hat das Klicken auf "Jetzt aktualisieren" keine Auswirkung. Wenn ein geplantes Update gestartet werden soll, während ein Update nach Bedarf ausgeführt wird, wird das geplante Update nicht ausgeführt. Wenn die On-Demand-Aktualisierung abgeschlossen ist, wird der geplante Aktualisierungszyklus wieder aufgenommen.

Wichtig! Wenn die herunterzuladenden Module Inhaltsaktualisierungen enthalten, aktualisieren Sie den Inhalts-Proxy bevor Sie eine andere On-Demand-Aktualisierung durchführen.

So aktualisieren Sie Server nach Bedarf

1. Klicken Sie auf die Registerkarte "Verwaltung" und dann auf die Unterregisterkarte "Services".
2. Erweitern Sie den Service für automatische Software-Updates in der Service-Liste.
3. Wählen Sie den Server aus, der als Proxy für Inhaltsaktualisierungen dient, und untersuchen Sie die zum Herunterladen ausgewählten Module. Wenn Inhaltsaktualisierungen enthalten sind, klicken Sie auf "Jetzt Aktualisieren".

   Der Server ruft Aktualisierungen vom CA-Server für automatische Software-Updates ab. Als Proxy für Inhaltsaktualisierungen verschiebt er Inhaltsaktualisierungen ins Inhalts-Repository. Als Online-Proxy lädt er auch binäre Aktualisierungen herunter.
4. Wählen Sie den Server, der aktualisiert werden soll, und überprüfen Sie seine Rolle.

5. Wenn es sich um einen Proxy für automatische Software-Updates zur Client-Aktualisierung handelt, klicken Sie auf "Jetzt aktualisieren".

   Der Server wird mit den Modulen aktualisiert, die für den Download ausgewählt wurden.

6. Wenn es sich um einen Client mit einem Online-Proxy handelt, gehen Sie folgendermaßen vor:

   a. Wählen Sie aus den ausgewählten Elementen der Liste "Proxy für automatische Software-Updates für Client" einen Proxy für diesen Client aus.

   b. Wählen Sie den Proxy für den Client aus, und klicken Sie auf "Jetzt Aktualisieren".

   c. Wählen Sie den Client aus, und klicken Sie auf "Jetzt aktualisieren".

   Der Server wird mit den Modulen aktualisiert, die für den Download ausgewählt wurden.

7. Wenn es sich um einen Offline-Proxy für automatische Software-Updates handelt, gehen Sie folgendermaßen vor:

   a. Laden Sie das Paket der Offline-Aktualisierung von der CA-FTP-Seite für automatische Software-Updates im Offline-Modus herunter.

   b. Kopieren Sie die Aktualisierungen manuell in den Download-Pfad des Offline-Proxys.

      .../data/subscription/offline

   c. Wählen Sie den Offline-Proxy und anschließend die ZIP-Datei der Offline-Aktualisierung aus, klicken Sie auf "Durchsuchen" und wählen Sie die gewünschten Module aus.

   d. Klicken Sie auf "Jetzt aktualisieren".

   Der Server wird mit den Modulen aktualisiert, die für den Download ausgewählt wurden.

8. Wenn es sich um einen Client mit einem Offline-Proxy handelt, gehen Sie folgendermaßen vor:

   a. Aktualisieren Sie den Offline-Proxy wie in Schritt 7 beschrieben.

   b. Wählen Sie den Client aus, und klicken Sie auf "Jetzt aktualisieren".

   Der Server wird mit allen Modulen aktualisiert, die auf seinen Offline-Proxys installiert sind.

   Hinweis: Clients für automatische Software-Updates im Offline-Modus erhalten alle Module, die manuell auf ihren Offline-Proxys installiert sind. Auf lokaler Ebene für einen Offline-Client ausgewählte Module haben keine Auswirkung.

Freier Speicherplatz für Aktualisierungen

Durch eine regelmäßige Bereinigung des Datenträgers können Sie dazu beitragen, dass automatische Software-Updates auf CA Enterprise Log Manager-Servern erfolgreich verlaufen. Wenn der verfügbare Speicherplatz bei Beginn des automatischen Software-Updates auf einen Wert unter 5 GB sinkt, gibt der Service für automatische Software-Updates ein Selbstüberwachungsereignis aus und unterbricht den Download-Prozess.

So stellen Sie sicher, dass genügend Speicherplatz für automatische Software-Updates vorhanden ist

1. Überwachen Sie den verfügbaren Speicherplatz in regelmäßigen Abständen. Alternativ können Sie einen Aktionsalarm einrichten, durch den Sie benachrichtigt werden, wenn der verfügbare Speicherplatz unter den entsprechenden Wert sinkt.
2. Geben Sie in diesem Fall Speicherplatz mit einem Bereinigungstool frei.
3. Falls Sie durch ein Selbstüberwachungsereignis eine Warnung erhalten, dass eine Bereinigung erforderlich ist, geben Sie genügend Speicherplatz frei, damit der Download erfolgreich durchgeführt werden kann.

Weitere Informationen:

Beispiel: Einen Aktionsalarm für "Wenig Speicherplatz verfügbar" erstellen.
(siehe Seite 503)

Info zu öffentlichen Schlüsseln für automatische Software-Updates

Der Proxy für automatische Software-Updates verwaltet eine Gruppe von öffentlichen Schlüsseln, die mit den vom CA-Software-Update-Server verwendeten privaten Schlüsseln korrespondieren. Der Proxy für automatische Software-Updates lädt die Software-Updates als ZIP-Datei herunter, die mit einem privaten Schlüssel digital signiert ist. Das Update ermittelt den öffentlichen Schlüssel, mit dem die Signatur des Updates überprüft werden soll. Durch die Überprüfung der Signatur stellt der Proxy für automatische Software-Updates sicher, dass das Update vom CA-Software-Update-Server stammt. Für ein automatisches Software-Update wird nur ein Schlüsselpaar aus privatem und öffentlichem Schlüssel verwendet. Mit einem privaten Schlüssel wird das Update signiert. Mit dem öffentlichen Schlüssel wird die Signatur verifiziert. Der öffentliche Schlüssel ist auf jedem CA Enterprise Log Manager-Server gespeichert und kann aktualisiert werden.

CA Enterprise Log Manager speichert die anfängliche Version des öffentlichen Schlüssels während der Installation in der Konfigurationsdatei des automatischen Software-Updates. Falls ein neuer privater Schlüssel erforderlich ist, wird der zugehörige öffentliche Schlüssel vor dem Update-Zyklus heruntergeladen, in dem der neue Schlüssel benötigt wird.

Wichtig! Aktualisieren Sie das Feld "Öffentlicher Schlüssel" für das automatische Software-Update nicht manuell, es sei denn, Sie werden vom Technischen Support von CA ausdrücklich dazu angewiesen.

Selbstüberwachung von Ereignissen für automatische Software-Updates

Sie können erfolgreiche und fehlgeschlagene automatische Software-Updates überwachen, an denen folgendermaßen konfigurierte CA Enterprise Log Manager-Server beteiligt sind:

- Standard-Proxy für automatische Software-Updates
- Ggf. weitere Online-Proxys für automatische Software-Updates
- Ggf. Offline-Proxys für automatische Software-Updates
- Clients für automatische Software-Updates

Hinweis: Bei den hier beschriebenen Ereignissen werden automatische Software-Updates für Agenten nicht nachverfolgt.

Erfolgreiche Updates werden in den folgenden Fällen berichtet:

- Hoch- und Herunterfahren von CA Enterprise Log Manager-Servern, von beiden Software-Proxys für automatische Software-Updates sowie von Clients für automatische Software-Updates.
- Erfolgreiches Herunterladen einer Komponente von einem Online- oder Offline-Update-Proxy
- Erfolgreiche Installation einer Komponente durch einen Client für automatische Software-Updates

Misslingen und Fehler werden in den folgenden Fällen berichtet:

- Fehlgeschlagenes Herunterladen einer Komponente von einem Online- oder Offline-Update-Proxy
- Fehlgeschlagene Installation einer Komponente durch einen Client für automatische Software-Updates
- Fehlerbedingungen

Überwachen von Software-Update-Ereignissen

Sie können den Erfolg und Misserfolg der Prozesse für automatische Software-Updates überwachen, indem Sie selbstüberwachende Ereignisse für die automatischen Software-Updates anzeigen.

So überwachen Sie Ereignisse zur Verarbeitung von automatischen Software-Updates:

1. Klicken Sie auf die Registerkarte "Verwaltung" und auf die Unterregisterkarte "Services".
2. Klicken Sie in der Service-Liste auf den Service für automatisches Software-Update.
3. Klicken Sie auf die Registerkarte "Selbstüberwachende Ereignisse", um entweder auf "Automatisches Software-Update - Service" oder unter "Automatisches Software-Update - Service" auf einen Host zuzugreifen.

4. Überprüfen Sie die angezeigten Ereignisdetails.

   Einige der für selbstüberwachende Ereignisse angezeigten Felder spiegeln die CEG-Standardmethode wider, mit der herstellerübergreifend auf allgemeine Aktionen verwiesen wird. Das Idealmodell basiert auf dieser Hierarchie: "event_category", "event_class" (innerhalb der Kategorie), "event_action" (innerhalb der Klasse), "event_result" und "event_severity". Bei dem in diesem Bericht angezeigten CA-Schweregrad handelt es sich um die CA-Interpretation des Schweregrades.

   CA - Schweregrad

   Schweregrad des Ereignisses, wobei gilt:

   - "Unbekannt" – unbekannte Ereignisse, Ereignisse, die nicht CEG zugeordnet sind, oder unklassifizierte Ereignisse
   - "Informationen" – allgemeine Informationen zum Systembetrieb, sicherheitsrelevante Informationen oder ein Hinweis
   - "Warnung" – ungewöhnliche Änderungen, eine normale, aber signifikante Bedingung, fehlgeschlagene Vorgänge oder Leistungsabfälle
   - "Geringfügige Auswirkung" – geringfügige Auswirkung auf ein System, eine Funktion oder die Sicherheit
   - "Schwerwiegende Auswirkung" – schwerwiegende Auswirkung auf ein System, eine Funktion oder die Sicherheit
   - "Kritisch" – sofortige Maßnahmen sind erforderlich; wahrscheinlich liegt eine Sicherheitslücke vor.

   Datum

   Zeitpunkt, zu dem das Ereignis aufgetreten ist

   Empfänger

   Die Komponente konnte den aktuellen Prozess nicht erfolgreich abschließen. Dies könnte entweder ein Proxy oder Client für automatische Software-Updates sein. Falls es sich um einen Proxy für automatische Software-Updates handelt, könnte dies ein Standard-Proxy, ein Online-Proxy oder ein Offline-Proxy sein.

   Empfängerhost

   Hostname des CA Enterprise Log Manager-Servers, der der Empfänger ist

Kategorie

Kategorie des Ereignisses. Die Konfigurationsverwaltung für Ereignisse des Services automatischer Software-Updates lautet "event_category".

Benutzer

Benutzername oder die Identität, der/die die in den Ereignisinformationen angegebene Aktion initiiert hat Hierbei handelt es sich um das Feld "source_username" in CEG.

Aktion

Aktion, die zur Generierung des Ereignisses geführt hat. Hierbei handelt es sich um das Feld "event_action" in CEG.

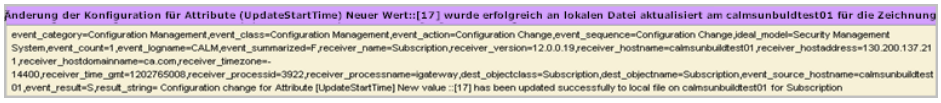
Ergebnis

"S" für "Success" (Erfolgreich); "F" für "Failure" (Fehler). Beim Ergebnis der Ereignisaktion handelt es sich um das Feld "event_result" in CEG. Andere Aktionen sind "Accept" (Akzeptiert), "Reject" (Zurückgewiesen), "Drop" (Verworfen) und "Unknown" (Unbekannt).

Ergebnisbeschreibung

Meldungstext. Wenn in der Spalte "Ergebnis" der Wert "Failure" (Fehler) angezeigt wird, sehen Sie sich den Text unter "Ergebnisbeschreibung" an.

5. Zeigen Sie Details in der Ereignisanzeige an. Hier können Sie Änderungen anzeigen, die beispielsweise an einem Konfigurationswert wie der Startzeit vorgenommen wurden.



Anzeigen von Ereignisdetails bei Automatischen Software-Updates

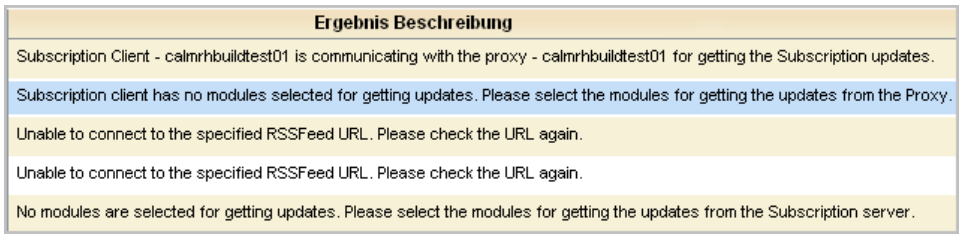
Nach dem Konfigurieren der automatischen Software-Updates können Sie die selbstüberwachenden Ereignisse anzeigen. Nach einem automatischen Software-Update können Sie überprüfen, ob die Aktualisierung auf allen Servern erfolgreich abgelaufen ist. Wenn die Aktualisierungen abgeschlossen sind, dann prüfen Sie auf allen betroffenen Servern auf die folgenden selbstüberwachenden Ereignisse:

- <Komponente> wurde erfolgreich auf Proxy <Proxyname> heruntergeladen und in EEM installiert.
- <Komponente> wurde erfolgreich auf Proxy <Proxyname> heruntergeladen.
- <Komponente> wurde erfolgreich auf Client <Clientname> installiert.

Sie können selbstüberwachende Ereignisse für automatische Software-Updates auch zum Zweck der Fehlerbehebung anzeigen.

So können Sie Details zu automatischen Software-Updates in der Ereignisanzeige anzeigen:

1. Klicken Sie auf die Registerkarte "Verwaltung" und auf die Unterregisterkarte "Services".
2. Klicken Sie in der Service-Liste auf den Service für automatisches Software-Update.
3. Klicken Sie auf die Registerkarte "Selbstüberwachende Ereignisse", um entweder auf "Automatisches Software-Update - Service" oder unter "Automatisches Software-Update - Service" auf einen Host zuzugreifen.
4. Prüfen Sie die Spalte "Ergebnisbeschreibung". In dieser Spalte können z. B. Ereignisse wie "Für den Client für automatische Software-Updates sind keine Module zum Abrufen von Aktualisierungen ausgewählt" angezeigt werden.

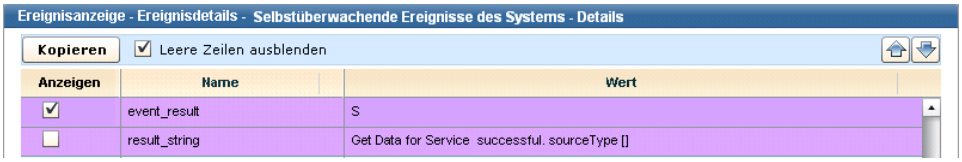


Ergebnis Beschreibung
Subscription Client - calmrhbuildtest01 is communicating with the proxy - calmrhbuildtest01 for getting the Subscription updates.
Subscription client has no modules selected for getting updates. Please select the modules for getting the updates from the Proxy.
Unable to connect to the specified RSSFeed URL. Please check the URL again.
Unable to connect to the specified RSSFeed URL. Please check the URL again.
No modules are selected for getting updates. Please select the modules for getting the updates from the Subscription server.

5. Doppelklicken Sie auf die Ereignisbeschreibung, für die Sie Details anzeigen möchten.

   Die "Ereignisanzeige" wird geöffnet.

6. Scrollen Sie zum Abschnitt "Ergebnisse", und prüfen Sie den Text, der für "Ergebnis_Zeichenkette" angezeigt wird.



Automatische Software-Updates auf Agenten und Connectors anwenden

Regelmäßige Updates, Service-Packs und punktuelle Aktualisierungen werden durch automatische Software-Updates übermittelt. Oft schließen die herunterzuladenden Module Agenten und Integrationen ein. Wenn diese Module auf einen Software-Update-Client heruntergeladen werden, der Agenten verwaltet, müssen Sie die Updates auf die Agenten anwenden, nachdem Sie überprüft haben, ob der Software-Update-Client, der die Agenten verwaltet, erfolgreich aktualisiert wurde. Aktualisierungen für Agenten müssen vor Aktualisierungen für Connectors angewendet werden.

So aktualisieren Sie CA Enterprise Log Manager-Agenten mit "Automatischen Software-Updates":

1. Wenn die Aktualisierung das Agenten-Modul einschließt, aktualisieren Sie Ihre Agenten nach Plattform wie folgt:
   a. Klicken Sie auf die Registerkarte "Verwaltung" und auf die Unter-Registerkarte "Protokollerfassung".
   b. Legen Sie fest, ob Agenten-Aktualisierungen auf alle Agenten gleichzeitig, auf eine ausgewählte Gruppe von Agenten oder einen einzelnen Agenten angewendet werden sollen, abhängig vom Umfang, der für eine einzelne Plattform zutrifft.
      - Wenn alle Ihre Agenten auf derselben Plattform installiert sind, wählen Sie "Agenten-Explorer", und klicken Sie dann auf "Automatisches Software-Update".
      - Wenn Ihre Agentengruppen aus Agenten bestehen, die auf derselben Plattform installiert sind, erweitern Sie den Agenten-Explorer, wählen Sie eine Agentengruppe und klicken Sie auf "Automatisches Software-Update".
      - Andernfalls erweitern Sie zunächst den "Agenten-Explorer", dann eine Agentengruppe, wählen Sie einen Agenten aus, und klicken Sie dann auf "Automatisches Software-Update".

      Der Assistent "Automatisches Software-Update" wird angezeigt.
   c. Wenn Sie "Agenten-Explorer" oder eine Agentengruppe ausgewählt haben, wählen Sie "Agenten-Aktualisierungen", wählen Sie die Plattform aus der Dropdown-Liste "Plattform" aus, klicken Sie auf "Suchen", und klicken Sie auf den Schritt "Versionsauswahl".
   d. Wenn Sie einen Agenten ausgewählt haben, wählen Sie "Agenten-Aktualisierungen", und klicken Sie auf den Schritt "Versionsauswahl".

e. Wählen Sie die Update-Version für jeden aufgelisteten Agenten.

f. Klicken Sie auf "Speichern und schließen".

g. Überprüfen Sie die erfolgreiche Durchführung. Klicken Sie auf "Status und Befehl". Klicken Sie auf "Konfigurationserfolg". Vermerken Sie die Version der angewendeten Konfiguration.

h. Wiederholen Sie dies so oft wie nötig, um alle Agenten zu aktualisieren.

2. Wenn die Aktualisierung das Integrationen-Modul einschließt, aktualisieren Sie Connectors für Ihre Agenten wie folgt:

   a. Klicken Sie auf die Registerkarte "Verwaltung" und auf die Unter-Registerkarte "Protokollerfassung".

   b. Legen Sie fest, ob Connector-Aktualisierungen auf alle Connectors für alle Agenten gleichzeitig, auf Connectors für eine ausgewählte Agentengruppe oder auf Connectors für einen einzelnen Agenten angewendet werden sollen.

   c. Wählen Sie "Agenten-Explorer", eine Agentengruppe oder einen Agenten aus. Klicken Sie dann auf "Automatisches Software-Update".

   d. Wählen Sie "Connector-Aktualisierungen" in der Liste "Aktualisierungsauswahl".

   e. Optional können Sie einen Wert aus einer der folgenden Dropdown-Listen auswählen, um die Standardeinstellungen für "Alle: Agentengruppe, Plattform, Integration" zu ändern. Klicken Sie auf "Suchen".

   f. Klicken Sie auf den Schritt "Versionsauswahl".

   g. Klicken Sie auf "Alle auswählen", um alle Einträge in der Liste auszuwählen, oder wählen Sie einzelne Zeilen, die den Connectors entsprechen, die Sie aktualisieren möchten. Wählen Sie für jede ausgewählte Zeile die anzuwendende Aktualisierungsversion.

   h. Klicken Sie auf "Speichern und schließen".

3. Überprüfen Sie die Aktualisierungen. Führen Sie den Assistenten "Automatisches Software-Update" erneut aus. Wählen Sie den Schritt "Versionsauswahl", um die aktuelle Version anzuzeigen, und überprüfen Sie, ob es sich um die Version handelt, die Sie für die Aktualisierung ausgewählt haben. Klicken Sie auf "Abbrechen".

Weitere Informationen:

Anwenden automatischer Software-Updates (siehe Seite 711)
Öffnen des Assistenten für die Liste der Aktualisierungen (siehe Seite 712)
Auswählen der Agenten oder Connectors für die Aktualisierung (siehe Seite 713)
Aktualisieren der Agenten- oder Connector-Integrationsversionen (siehe Seite 714)

Kapitel 8: Filter und Profile

Dieses Kapitel enthält folgende Themen:

Kapitel 9: Globale und lokale Filter

Sie können Filter festlegen oder bearbeiten, um das angezeigte Ereignis oder die Incidents-Informationen zu verfeinern. Das Dialogfeld "Globale Filter" können Sie über das Hauptfenster von CA Enterprise Log Manager aufrufen. Innerhalb einzelner Abfrage- oder Berichtsanzeigen oder aus dem Incident-Bereich können Sie lokale Filter hinzufügen. Auch anwendungsweite Abfrageeinstellungen lassen sich in der Oberfläche für globale Filter festlegen.

Jeder Filtertyp verfügt über einen eigenen Erstellungsdialog, der mithilfe einer eigenen Schaltfläche gestartet wird.

Globaler Filter 

Ein globaler Filter wird auf alle Berichte und Abfragen angewandt, die Sie in der *aktuellen* Sitzung anzeigen. Er ermöglicht es, eine Vielzahl von Ereignistypen mit gleicher Berechtigung anzuzeigen. Die Schaltfläche "Globale Filter" befindet sich oben im Hauptfenster von CA Enterprise Log Manager neben dem Menü "Protokollmanager-Server". Sie können einen globalen Filter verwenden, um beispielsweise alle in der letzten Woche empfangenen Ereignisse oder solche eines bestimmten Hosts anzuzeigen. Sie können globale Filter auch für Incidents festlegen, die zwar denselben Aufbau haben, die jedoch nur auf Incidents und deren Komponenten-Ereignisinformationen angewendet werden.

Hinweis: Standardmäßig ist ein globaler Filter vorgegeben, der die Daten der letzten sechs Stunden ausgibt.

Lokaler Filter 

Gilt nur für aktuelle Berichte, Abfragen oder Incident-Ansichten. Die Schaltfläche "Lokale Filter" wird in Abfrage- oder Berichtsausgaben oben im Fenster "Details" und im Fenster "Incidents" angezeigt. Wenn Sie einen neuen Bericht anzeigen, wird der lokale Filter nur angewandt oder gespeichert, wenn Sie den Bericht als Favorit mit entsprechend festgelegtem Filter speichern. Mit lokalen Filtern können Sie eine aktuelle Ansicht eingrenzen, um beispielsweise nur einen Host in einer Multi-Host-Berichtsanzeige anzuzeigen, ohne dabei andere Berichtsanzeigen zu ändern.

Dieses Kapitel enthält folgende Themen:

Infos über einfache Filter

Bevor Sie den Assistenten für das Abfragedesign oder Profildesign das erste Mal verwenden, sollten Sie sich mit den einfachen Filtertypen vertraut machen.

Beispiele einfacher Filter

Nachfolgend finden Sie ein Beispiel zu jedem Typ eines einfachen Filters:

Filtertyp	Wert	Beschreibung
Idealmodell	Antivirus	Zeigt nur die Ereignisdaten, die von beispielsweise folgenden Produkten generiert werden: ■ CA Anti-Virus ■ McAfee VirusScan ■ Symantec Antivirus Corporate Edition ■ TrendMicro OfficeScan
Ereigniskategorie/ Ereignisklasse	Systemzugriffs-/Anmeldeaktivität	Zeigt nur die Ereignisdaten für Benutzer an, die sich am System anmelden.
Ereignisprotokollname	Cisco PIX Firewall	Zeigt nur die Ereignisdaten, die von Cisco PIX-Firewall-Geräten generiert werden.

Mit Ausnahme des Ereignisprotokollnamen basieren die Filtertypen auf der ELM-Schemadefinition (CEG).

- Um sich über die technologiebasierten Produktfilter zu informieren, sehen Sie sich die Liste der Idealmodelle an.
- Um sich über die kategorie-/klassen-/aktionsbasierten Produktfilter zu informieren, sehen Sie sich die Liste der Ereigniskategorien und der Ereignisklassen an.

Diese Listen finden Sie in der Online-Hilfe des Abschnitts "ELM-Schemadefinition".

Einrichten eines einfachen Filters

Sie können einfache Filter festlegen, um Kriterien für das Ereignis einzurichten, das Sie anzeigen oder auswerten möchten. Wenn die einfachen Filter im Assistenten für das Abfragedesign eingerichtet werden, können Sie damit die Ereignisdaten begrenzen, die von einer Abfrage oder einem Alarm zurückgegeben werden. Wenn die einfachen Filter im Assistenten für das Profildesign eingerichtet werden, können Sie damit die Daten begrenzen, die bei Anwendung eines Profils in den Berichts- oder Abfrageergebnissen angezeigt werden.

1. Öffnen Sie den Assistenten.
2. Legen Sie den Typ des einzurichtenden einfachen Filters fest:
   - technologiebasiert
   - kategoriebasiert, kategorie- und klassenbasiert, oder kategorie-, klassen- und aktionsbasiert
   - produktbasiert
3. Um einen produktbasierten Filter einzurichten, aktivieren Sie das Kontrollkästchen "Idealmodell ist" und wählen einen Wert aus der Dropdown-Liste "Idealmodell" aus.
4. Um einen Filter auf der Basis einer Sicherheitsereigniskategorie, einer Kategorie und Klasse oder einer Kategorie, Klasse und Aktion einzurichten, führen Sie folgende Schritte aus:
   a. Aktivieren Sie das Kontrollkästchen "Ereigniskategorie ist", und wählen Sie einen Wert aus der entsprechenden Dropdown-Liste aus.
   b. (Optional). Aktivieren Sie das Kontrollkästchen "Ereignisklasse ist", und wählen Sie einen Wert aus der Dropdown-Liste aus.
   c. (Optional). Wenn Sie "Ereignisklasse" ausgewählt haben, aktivieren Sie das Kontrollkästchen "Ereignisaktion ist", und wählen Sie einen Wert aus der Dropdown-Liste aus.

   Hinweis: Sie können diesen Filtertyp auch unter einem technologiebasierten Filter einrichten.
5. Um einen produktbasierten Filter einzurichten, aktivieren Sie das Kontrollkästchen "Protokollname ist" und wählen einen Wert aus der Dropdown-Liste aus.
6. Beenden Sie den Assistenten.

Infos über Profilfilter

Ein Profil besteht aus einem Satz mehrerer Filter. Sie können ein Profil mit Kennungsfiltern, Datenfiltern oder einer Kombination aus beiden erstellen. Der Abfragekennungsfilter begrenzt die Abfragen, die für die Auswahl angezeigt werden, der Berichtskennungsfilter begrenzt die Berichte, die für die Auswahl angezeigt werden. Die Datenfilter begrenzten die Daten, die in einem Bericht oder in Abfrageergebnissen angezeigt werden. Die Profilfilter werden auf Abfragen, geplante Alarme und geplante Berichte angewandt.

Sie können Kennungsfilter für Berichte und Abfragen separat auswählen. Kennungsfilter können folgende Werte enthalten, sind jedoch nicht auf diese beschränkt:

- Standardbasierte Kennungen, wie COBIT, FISMA,GLBA, HIPAA, NERC, PCI, SAS 70, SOX.

  Standardbasierte Kennungsfilter werden auf Berichtskennungen, nicht auf Abfragekennungen angewandt.
- Kategoriekennungen für Sicherheitsereignisse, wie Inhaltssicherheit, Hostsicherheit, Netzwerksicherheit, Betriebssicherheit, Ressourcen- und Systemzugriff.
- Produktkennungen wie CA Access Control, CA Identity Manager und CA SiteMinder.

Sie können einen einfachen Datenfilter auswählen, oder Sie erstellen einen erweiterten Datenfilter. Nachfolgend finden Sie eine kurze Beschreibung der Filter:

- Einfache Datenfilter können auf folgenden Faktoren basieren:
  - Auf einer ausgewählten Technologie (Systemsoftware, Hostanwendungssoftware und -Services, Netzwerkanwendungssoftware und -Services)
  - Auf einer ausgewählten CEG-Ereigniskategorie, einer ausgewählten CEG-Ereigniskategorie und -klasse oder einer ausgewählten CEG-Ereigniskategorie, -klasse und -aktion
  - Auf einem ausgewählten Produkt
- Erweiterte Datenfilter basieren auf einer benutzerdefinierten SQL-Abfrage, die sich aus einer oder mehreren WHERE-Klauseln zusammensetzt. Die Abfrage wählt eine CEG-Spalte mit einer WHERE-Klausel aus, die sich aus dieser CEG-Spalte, einem ausgewählten Operator und einem angegeben Wert zusammensetzt.

Erstellen von Profilen

Sie können Profile erstellen, mit denen Benutzer ihre CA Enterprise Log Manager-Ansichten entsprechend ihrer Umgebungen einschränken können. Beispiel: Sie können ein Profil "CA-Zugriffskontrolle" erstellen, das nur Berichte, Abfragen und Ereignisse anzeigt, die für die Zugriffskontrolle relevant sind.

Die Erstellung eines Profils mit dem Profilassistenten umfasst folgende Schritte:

1. Öffnen des Profilassistenten
2. Eingeben des Profilnamens und einer Beschreibung
3. Feststellen der Informationen, die bei Verwendung von einfachen und erweiterten Filtern angezeigt werden
4. Auswählen, welche Abfragen und Berichte bei Verwendung von Kennungsfiltern angezeigt werden

Weitere Informationen

Hinzufügen von Profildetails (siehe Seite 276)
Erstellen von Datenfiltern (siehe Seite 277)
Erstellen von Kennungsfiltern (siehe Seite 278)

Öffnen des Profilassistenten

Um ein neues Profil zu erstellen oder ein vorhandenes zu bearbeiten, müssen Sie den Profilassistenten öffnen.

So öffnen Sie den Profilassistenten:

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

   Die Liste der Bibliotheks-Ordner wird angezeigt.

2. Wählen Sie den Ordner "Profile".

   Die Schaltfläche "Profile" wird im Fenster "Details" angezeigt.

3. Klicken Sie auf "Neues Profil". 

   Der Profilassistent wird geöffnet.

   Beachten Sie bei Verwendung des Assistenten Folgendes:

   - Klicken Sie auf "Speichern", um die Regeldatei zu speichern, ohne den Assistenten zu schließen.
   - Klicken Sie auf "Speichern und schließen", um die Regel zu speichern und den Assistenten zu schließen.
   - Klicken Sie auf "Zurücksetzen", um die Ansicht im Assistenten auf die zuletzt gespeicherten Einstellungen zurückzusetzen.

Hinzufügen von Profildetails

Sie müssen einen Namen für das Profil eingeben. Sie können auch optional zu Referenzzwecken eine Beschreibung eingeben.

So geben Sie einen Namen für das Profil ein:

1. Öffnen Sie den Profilassistenten.
2. Geben Sie Namen für das neue Profil ein. Der Name darf bis zu 80 Zeichen umfassen und darf Sonderzeichen enthalten.
3. (Optional) Geben Sie eine Beschreibung ein.
4. Gehen Sie weiter zum Schritt "Datenfilter".

Erstellen von Datenfiltern

Sie können die angezeigten Informationen nach Ihrem Profil filtern, indem Sie einfache oder erweiterte Filter verwenden. Jedes Profil muss mindestens einen Filter haben.

So richten Sie Profildatenfilter ein:

1. Öffnen Sie den Profilassistenten.
2. Geben Sie den Profilnamen ein, sofern noch nicht geschehen, und gehen Sie dann weiter zum Schritt "Datenfilter".

   Das Dialogfeld "Filter" wird mit der Registerkarte "Einfache Filter" angezeigt.
3. Erstellen Sie die gewünschten einfachen Filter. Beispielsweise könnten Sie das Kontrollkästchen "Ereignisprotokollname" aktivieren, und für die Suche nach CA-Zugriffssteuerungsereignissen "CA-Zugriffssteuerung" eingeben.
4. (Optional) Klicken Sie auf die Registerkarte "Erweiterte Filter".

   Das Dialogfeld "Erweiterte Filter" wird angezeigt.
5. Fügen Sie bei Bedarf erweiterte Filter hinzu.
6. Klicken Sie auf den entsprechenden Pfeil, um zu dem Schritt des Profilassistenten zu gelangen, den Sie als nächstes ausführen möchten, oder klicken Sie auf "Speichern und schließen".

   Wenn Sie auf "Speichern und schließen" klicken, wird das neue Profil in der Liste angezeigt. Andernfalls wird der von Ihnen ausgewählte Assistentenschritt angezeigt.

Weitere Informationen

Erstellen eines einfachen Ereignisfilters (siehe Seite 618)
Erstellen erweiterter Ereignisfilter (siehe Seite 621)
Verwenden erweiterter Filter (siehe Seite 528)

Erstellen von Kennungsfiltern

Sie können Kennungsfilter für Ihr Profil erstellen, die steuern, welche Abfragen oder Berichtkategoriekennungen in der CA Enterprise Log Manager-Oberfläche angezeigt werden, wenn ein Benutzer das Profil anwendet. Wenn Sie beispielsweise den Kennungsfilter für CA SiteMinder erstellen, zeigt die CA Enterprise Log Manager-Oberfläche nur die Berichte und Abfragen mit der Kennung CA SiteMinder an.

So erstellen Sie einen Kennungsfilter:

1. Öffnen Sie den Profilassistenten.
2. Geben Sie den Profilnamen ein, sofern noch nicht geschehen, und gehen Sie dann weiter zum Schritt "Kennungsfilter".

   Das Dialogfeld "Filter" wird mit der Unterregisterkarte "Berichtskennungsfilter" angezeigt.
3. Klicken Sie auf "Neuer Ereignisfilter".

   Die erste Zeile der Kennungsfiltertabelle wird aktiviert.
4. Klicken Sie auf die Zelle "Kennung", und wählen Sie die Abfrage oder den Namen der Berichtskennung aus, die sie anzeigen möchten, bzw. geben Sie sie ein. Wenn Sie sie eingeben, werden Ihnen während der Eingabe die verfügbaren Kennungsnamen aufgelistet.
5. (Optional) Klicken Sie auf die Registerkarte "Neuer Ereignisfilter", um weitere Filter hinzuzufügen.

   Die zweite Zeile der Kennungsfiltertabelle wird aktiviert und zeigt UND in der Spalte "Logik" an.
6. (Optional) Klicken Sie in die Logikzelle, um entweder den Operator UND oder ODER auszuwählen.
7. (Optional) Klicken Sie auf die Zelle "Kennung", und wählen Sie Namen der Kennung aus, die sie anzeigen möchten, bzw. geben Sie ihn ein. Wenn Sie sie eingeben, werden Ihnen während der Eingabe die verfügbaren Kennungsnamen aufgelistet.
8. (Optional) Klicken Sie auf die Zellen für die öffnenden und schließenden Klammern, und geben Sie die Zahl der benötigten Klammern ein.
9. (Optional) Klicken Sie auf die Unterregisterkarte "Abfragekennungsfilter", und wiederholen Sie die Schritte 3 bis 8, um die weitere von Ihnen benötigte Kennungsfilter zu erstellen.
10. Wenn Sie alle gewünschten Filteranweisungen eingegeben haben, klicken Sie auf "Speichern".

Weitere Informationen

Erstellen von Datenfiltern (siehe Seite 277)

Importieren eines Profils

Sie können ein Profil importieren, mit dem Sie Profile von einer in eine andere Umgebung verschieben können. Beispielsweise könnten Sie ein Profil, das in einer Testumgebung erstellt wurde, in Ihre produktive Umgebung importieren.

So importieren Sie ein Profil:

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

   Die Liste der Bibliotheks-Ordner wird angezeigt.

2. Klicken Sie auf den Pfeil neben dem Ordner "Profile", um ihn zu öffnen.

   Die Schaltfläche "Profile" wird im Fenster "Details" angezeigt.

3. Klicken Sie auf "Profil importieren"

   Das Dialogfeld "Datei importieren" wird angezeigt.

4. Suchen Sie die Datei, die importiert werden soll, und klicken Sie auf "OK".

   Der Profilassistent wird geöffnet und zeigt die Details des ausgewählten Profils an.

5. Nehmen Sie die gewünschten Änderungen vor, und klicken Sie auf "Speichern und schließen". Wenn das importierte Profil denselben Namen hat, wie ein Profil in Ihrer Verwaltungsdatenbank, werden Sie aufgefordert, den Namen zu ändern.

   Das importierte Profil wird im entsprechenden Ordner angezeigt.

Exportieren eines Profils

Sie können ein Profil exportieren. Dadurch können Sie Profile in mehreren Umgebungen gemeinsam nutzen. Beispielsweise könnten Sie ein Profil, das in einer Testumgebung erstellt wurde, in Ihre produktive Umgebung exportieren.

So exportieren Sie ein Profil:

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

   Die Liste der Bibliotheks-Ordner wird angezeigt.

2. Klicken Sie auf den Pfeil neben dem Ordner "Profile", um ihn zu öffnen.

   Der Profilordner wird angezeigt.

3. Klicken Sie auf den Ordner, in dem sich das zu exportierende Profil befindet.

   Der Ordner wird eingeblendet, und die einzelnen Dateien werden angezeigt.

4. Wählen Sie das Profil aus, das Sie exportieren möchten, und klicken Sie auf "Profil exportieren".

   Ein Dialogfeld für den Exportspeicherort wird angezeigt.

5. Geben Sie das Verzeichnis ein, an dem Sie das exportierte Profil speichern möchten, oder navigieren Sie dorthin, und klicken Sie auf "Speichern".

   Ein Dialogfeld über den erfolgreichen Export wird angezeigt.

6. Klicken Sie auf "OK".

   Das Profil wird exportiert.

Einrichten eines Profils

Sie können jedes verfügbare Profil auswählen, um es auf Ihre Umgebung anzuwenden. Abhängig von den Profilbedingungen werden die verfügbaren Abfragen und Berichte beschränkt. Um ein Profil einzurichten, wählen Sie das gewünschte Profil aus dem Dropdown-Menü "Profile" oben im Hauptfenster von CA Enterprise Log Manager aus.

Hinweis: Um das ausgewählte Profil als das Standardprofil Ihrer Umgebung auszuwählen, klicken Sie ganz oben im CA Enterprise Log Manager-Hauptfenster auf die Profiloption "Als Standard festlegen". Das ausgewählte Profil wird als das Standardprofil des angemeldeten Benutzers festgelegt.

Erstellen von globalen Filtern

Sie können globale Filter erstellen. Mit globalen Filtern können Sie Abfragen, Berichte oder alle Incidents mithilfe der gleichen Kriterien anzeigen. Wenn Sie einen globalen Filter erstellen, legen Sie fest, ob der Filter sich auf Ereignisse oder auf Incidents beziehen soll. Ein einzelner globaler Filter kann sich nicht auf beides beziehen. Auch anwendungsweite Abfrageeinstellungen lassen sich in der Oberfläche für globale Filter festlegen.

So erstellen Sie einen globalen Filter:

1. Klicken Sie oben im Hauptfenster auf die Schaltfläche "Globale Filter".

   Das Dialogfeld "Globale Filter und Einstellungen" wird angezeigt.

2. Klicken Sie auf die Registerkarte "Ereignisse" oder "Incidents", um auszuwählen, worauf der globale Filter angewendet soll.

3. Geben Sie mithilfe des Drop-down-Menüs "Zeitraum" den Zeitraum an, der mit dem Filter durchsucht werden soll.

4. Aktivieren Sie das Kontrollkästchen "Übereinstimmung", und geben Sie einen bestimmten Wert ein, nach dem in allen verfügbaren Rohereignissen gesucht werden soll.

   Hinweis: Sie können in den Rohereignissen nach mehreren Werten, Ausdrücken oder Teilen von Werten suchen, indem Sie die entsprechende Syntax der Funktion "Übereinstimmung" verwenden.

5. Klicken Sie auf "Filter hinzufügen", und geben Sie die Ereignisfelder an, die Sie in den Filter aufnehmen möchten.

   Das Drop-down-Menü "Spalte" und das Feld "Wert" werden angezeigt.

6. Wählen Sie das Ereignisfeld aus, das in den Filter aufgenommen werden soll, und geben Sie den Wert ein, den das Feld enthalten muss, um in den gefilterten Berichten angezeigt zu werden. Sie können mehrere Ereignisfeldnamen und -werte eingeben, indem Sie erneut auf "Filter hinzufügen" klicken. Wenn Sie auf die Schaltfläche "Ausschließen" klicken, wird jeder *außer* dem für das ausgewählte Ereignisfeld eingegebene Wert berücksichtigt.

   Hinweis: Wenn Sie einen globalen Filter in einem Zeichenfolgenfeld erstellt haben, wird dieser der Liste "Schnellfilter" hinzugefügt. Haben Sie einen Filter in einem Feld für numerische Werte oder Zeitangaben erstellt haben, wird er der Liste "Erweiterte Filter" hinzugefügt.

7. (Optional) Um weitere komplexe Kriterien anzugeben, klicken Sie auf die Registerkarte "Erweiterte Filter".

8. (Optional) Zur Auswahl globaler Einstellungen klicken Sie auf die Registerkarte "Einstellungen". Die Einstellungen werden für die ganze Anwendung übernommen.
9. (Optional) Um die Filtereinstellungen für zukünftige Sitzungen unter der gleichen Benutzeranmeldung beizubehalten, klicken Sie unten im Dialogfeld auf "Als Standard festlegen".
10. Klicken Sie auf "Speichern".

    Das Dialogfeld "Globale Filter und Einstellungen" wird geschlossen, und der neue Filter wird für die Berichte übernommen.

Weitere Informationen:

Verwenden erweiterter Filter (siehe Seite 528)
Konfigurieren von globalen Abfrageeinstellungen (siehe Seite 283)

Konfigurieren von globalen Abfrageeinstellungen

Mit Hilfe des Dialogfelds für globale Filter können Sie anwendungsweite Bedingungen festlegen, die für alle Berichte und Abfragen in Ihrer Umgebung gelten. Globale Einstellungen sind während der aktuellen Sitzung wirksam, es sei denn, Sie legen sie als Standardeinstellungen fest.

So konfigurieren Sie globale Abfrageeinstellungen:

1. Klicken Sie oben im Hauptfenster auf die Schaltfläche "Globale Filter".

   Das Dialogfeld "Globale Filter und Einstellungen" wird mit der Registerkarte "Schnellfilter" im Vordergrund angezeigt.

2. Klicken Sie auf die Registerkarte "Einstellungen“.

   Die Registerkarte wird mit den folgenden Werten angezeigt.

   Lokale Zeitzone

   Steuert die Zeitzone für alle Datum/Uhrzeit-Felder in Berichten und Abfragen. Anstelle der Zeitzone des CA Enterprise Log Manager-Servers wird in Ihren Berichten und Abfragen die Zeitzone übernommen, die Sie in der Dropdown-Liste ausgewählt haben.

   Abfragen föderierter Daten ausführen

   Damit kann die Abfrage auf alle verfügbaren föderierten Server angewendet werden. Diese Einstellung ist standardmäßig aktiviert. Wenn diese Einstellung deaktiviert wird, werden Abfragen auf die Ereignisdaten beschränkt, die im lokalen Ereignisprotokollspeicher gespeichert sind. Damit können Sie Ihren lokalen Ereignisprotokollspeicher rasch überprüfen, wenn Sie wissen, dass die Zielereignisse lokal sind.

   Automatische Aktualisierung aktivieren

   Damit wird die Anzeige zu dem für die einzelnen Abfragen festgelegten Intervall automatisch aktualisiert.

3. (Optional) Wählen Sie im unteren Bereich des Dialogfelds "Als Standard festlegen" aus, um die Einstellungen als Standardeinstellungen festzulegen, die nach der aktuellen Sitzung erhalten bleiben.

4. Nehmen Sie die gewünschten Änderungen vor, und klicken Sie auf "Speichern".

   Das Dialogfeld "Globale Filter und Einstellungen" wird geschlossen, und der neue Filter wird angewendet.

Bearbeiten globaler Filter

Sie können einen vorhandenen globalen Filter bearbeiten.

So bearbeiten Sie einen globalen Filter:

1. Klicken Sie oben im Hauptfenster auf die Schaltfläche "Globale Filter".

   Das Dialogfeld "Globale Filter und Einstellungen" wird mit der Registerkarte "Schnellfilter" im Vordergrund angezeigt.

2. Ändern Sie die Parameter nach Bedarf, oder fügen Sie Parameter hinzu. Sie können einen einzelnen Schnellfilterparameter entfernen, indem Sie neben ihm auf das Symbol "Löschen" klicken.

3. Klicken Sie auf "Speichern".

   Das Dialogfeld "Globale Filter und Einstellungen" wird geschlossen, und der bearbeitete Filter wird übernommen.

Entfernen globaler Filter

Sie können einen globalen Filter entfernen und dabei alle Berichte auf den Standardstatus zurücksetzen.

Zum Entfernen eines globalen Filters klicken Sie oben im CA Enterprise Log Manager-Hauptfenster auf die Option zum Löschen globaler Filter: 

Erstellen lokaler Filter

Sie können einen lokalen Filter erstellen, um den Gültigkeitsbereich einer Abfrage, eines Berichts oder des Incidents, der im Bereich "Incidents" angezeigt wird, einzuschränken.

So erstellen Sie einen lokalen Filter:

1. Öffnen Sie die Abfrage oder den Bericht, die bzw. den Sie filtern möchten, oder klicken Sie auf die Registerkarte "Incident", und klicken Sie oben im Fenster auf "Lokale Filter".

   Das Dialogfeld "Lokale Filter" wird mit der Registerkarte "Schnellfilter" im Vordergrund angezeigt.

2. (Optional) Klicken Sie auf die Registerkarte "Incidents", wenn Sie statt Ereignisse angezeigte Incidents filtern möchten.

3. (Optional) Aktivieren Sie das Kontrollkästchen "Übereinstimmung", und geben Sie einen bestimmten Wert ein, nach dem gesucht werden soll.

   Hinweis: Sie können nach mehreren Werten, Ausdrücken oder Teilen von Werten suchen, indem Sie die entsprechende Übereinstimmungssyntax verwenden.

4. Klicken Sie auf "Filter hinzufügen".

5. Wählen Sie das Ereignisfeld aus, das in den Filter aufgenommen werden soll, und geben Sie den Wert ein, den das Feld enthalten muss, um in den gefilterten Berichten angezeigt zu werden. Sie können mehrere Spaltenwerte eingeben, indem Sie erneut auf "Filter hinzufügen" klicken. Wenn Sie auf die Schaltfläche "Ausschließen" klicken, wird jeder *außer* dem für das ausgewählte Ereignisfeld eingegebene Wert berücksichtigt.

6. (Optional) Klicken Sie auf die Registerkarte "Erweiterte Filter", um weitere Kriterien anzugeben.

7. Klicken Sie auf "Speichern".

   Der Filter wird auf die Anzeige angewandt. Speichern Sie die Berichtsansicht, indem Sie sie als Favorit festlegen.

Bearbeiten lokaler Filter

Sie können einen vorhandenen lokalen Filter bearbeiten.

So bearbeiten Sie einen lokalen Filter:

1. Klicken Sie oben im Abfrage- oder Berichtsfenster oder oben in der Incident-Ansicht auf "Lokale Filter".

   Das Dialogfeld "Lokale Filter" wird mit der Registerkarte "Schnellfilter" im Vordergrund angezeigt.

2. Ändern Sie die Werte nach Bedarf, oder fügen Sie sie hinzu. Sie können einzelne Filter entfernen, indem Sie daneben auf das Symbol "Löschen" klicken, oder indem Sie einen Übereinstimmungswert durch Deaktivieren des Kontrollkästchens entfernen.

3. Klicken Sie auf "Speichern".

   Der bearbeitete Filter wird auf die Anzeige angewandt.

Entfernen lokaler Filter

Sie können einen lokalen Filter entfernen und eine Abfrage, einen Bericht oder eine Incident-Ansicht so in den ursprünglichen Zustand zurücksetzen.

Klicken Sie dazu oben in der Abfrage, im Bericht oder im Incident auf die Schaltfläche zum Löschen lokaler Filter: 

Kapitel 10: Abfragen und Berichte

Dieses Kapitel enthält folgende Themen:

Info zu Abfragen und Berichten

Sie können Abfragen folgendermaßen verwenden:

- Sie können eine Abfrage ausführen, um Ereignis- oder Incident-Daten nahezu in Echtzeit anzuzeigen.
- Sie können einen vordefinierten Bericht auswählen, um die Ergebnisse mehrerer zugehöriger Abfragen anzuzeigen.
- Sie können einen Bericht erstellen, der sich aus den von Ihnen ausgewählten Abfragen zusammensetzt.
- Sie können mit Hilfe von Eingabeaufforderungsabfragen nach bestimmten vorausgewählten Informationen suchen.
- Sie können die Ausführung von Abfragen der letzten Daten als Aktionsalarme planen, durch die die verantwortlichen Stellen per E-Mail benachrichtigt werden. Aktionsalarme werden auch RSS-Feeds hinzugefügt, die mit Hilfe von RSS-Readern von Drittanbietern gelesen werden können.
- Sie können Ihre eigenen Abfragen zur Anzeige, Berichterstellung oder zum Erstellen von Aktionsalarmen erstellen.

Es gibt zwei Typen von Abfragen und Berichten:

- *Software-Update-Abfragen und -Berichte* sind von CA vordefiniert und werden als Teil der CA Enterprise Log Manager-Anwendung bei der Installation bereitgestellt oder einem automatischen Software-Update hinzugefügt.
- Bei *Benutzerabfragen und -berichten* handelt es sich um die von einem Benutzer erstellten Abfragen und Berichte. Sie können eine Abfrage oder einen Bericht von Grund auf neu erstellen oder aber basierend auf einer Software-Update-Abfrage beziehungsweise einem Software-Update-Bericht, die beziehungsweise den Sie ändern möchten.

CA Enterprise Log Manager bietet eine umfassende Liste von Abfragen und Berichten auf der Basis von automatischen Software-Updates. Falls Ihnen die Rolle "Auditor", "Analyst" oder "Administrator" zugewiesen wurde, können Sie alle Software-Update-Abfragen und -Berichte anzeigen. Darüber hinaus können Sie für alle von Ihnen angezeigten Software-Update-Abfragen oder -Berichte folgende Aktionen ausführen:

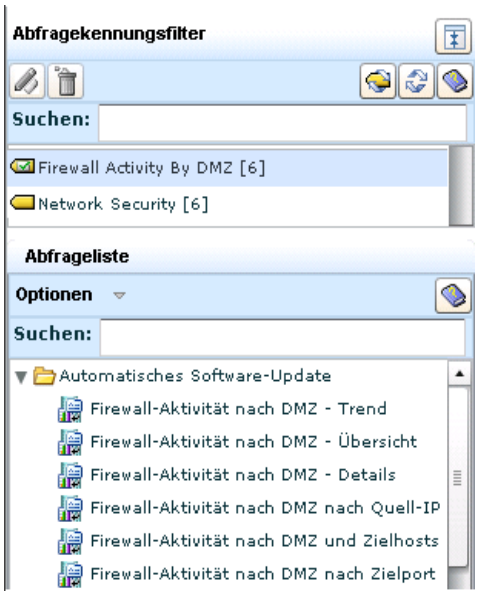
- angezeigte Daten aktualisieren
- lokale Filter bearbeiten, um die Daten auszublenden, die Sie nicht anzeigen möchten
- lokale Filter aufheben, um die Abfrage oder den Bericht erneut ungefiltert anzuzeigen
- angezeigte Abfrage oder angezeigten Bericht Ihrer Favoritenliste hinzufügen
- Abfrage drucken
- Option zur Anzeige der ausgewählten Abfrage oder des ausgewählten Berichts ändern
- angezeigte Abfrage oder angezeigten Bericht schließen

Folgende Aktionen können nur Benutzer mit der Rolle "Analyst" oder "Administrator" ausführen:

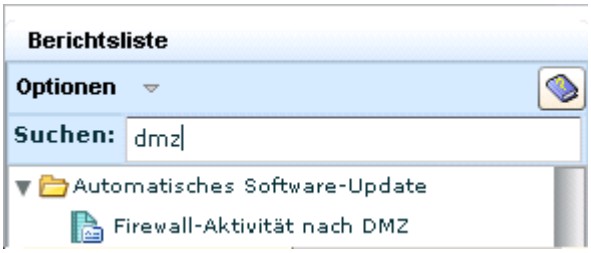
- neue Benutzerabfrage oder neuen Benutzerbericht von Grund auf neu erstellen
- Software-Update-Abfrage oder -Bericht kopieren und als Basis für eine Benutzerabfrage oder einen Benutzerbericht verwenden
- Benutzerabfrage oder Benutzerbericht bearbeiten
- Benutzerabfrage oder Benutzerbericht exportieren
- Benutzerabfrage oder Benutzerbericht löschen
- Änderungen an der ausgewählten Benutzerabfrage oder dem ausgewählten Benutzerbericht speichern
- Definition einer Benutzerabfrage oder eines Benutzerbericht importieren

Beispiel für Abfragen und den zugehörigen Bericht

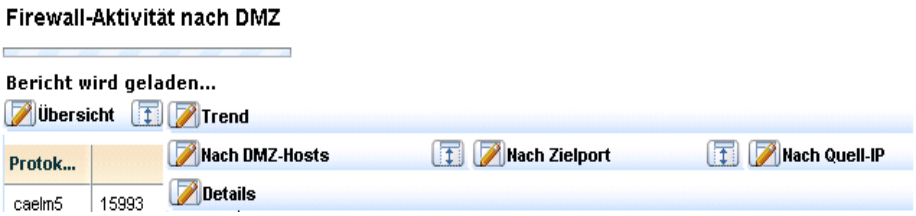
Betrachten Sie die Abfragekennung "Firewall-Aktivität nach DMZ". Beachten Sie, dass sie in diesem Thema sechs separaten Abfragen zugewiesen ist.



Die Abfragen, die Sie in der Abfrageliste sehen, werden in Berichten verwendet. Auf der Registerkarte "Berichte" können Sie einen Bericht namens "Firewall-Aktivität nach DMZ" anzeigen.



In der folgenden Abbildung werden nur die Namen dargestellt. Beachten Sie, dass jeder Name für einen der sechs Abfragen im Bericht steht. Die meisten Berichte umfassen Abfrageergebnisse für Übersichts-, Trend- und Detailangaben.



Aufgaben mit Kennungen

Mit Kennungen können Sie Berichte und Abfragen zu Referenzzwecken Kategorien zuweisen und die Berichterstattung in Ihrer Umgebung strukturiert gestalten. Darüber hinaus können mit Hilfe von Kategoriekennungen Aufgaben nach Rolle oder Ereignistyp verteilt werden.

Sie können die vordefinierten Kennungen verwenden oder eigene, selbst definierte Kennungen für Berichte oder Abfragen erstellen. So können Sie beispielsweise die Kennung "Monatlich" anlegen und sie jedem Bericht hinzufügen, der monatlich ausgeführt wird. Dies erleichtert das Auffinden und die Anzeige von Berichten. Außerdem können Sie auf diese Weise Berichte in Berichtsjobs aufnehmen oder daraus löschen, ohne die Jobs selbst bearbeiten zu müssen. Versehen Sie dazu einfach einen neuen Job mit der Kennung "Monatlich", oder entfernen Sie die Kennung von einem vorhandenen Job.

Einzelne Abfragen oder Berichte können während der Erstellung oder Bearbeitung mit benutzerdefinierten Kennungen versehen werden. Nach Erstellung einer neuen Kennung wird der zugehörige Name in der Liste der Kennungen angezeigt und kann Berichten oder Abfragen zugewiesen werden.

Benutzerdefinierte Kennungen lassen sich umbenennen und löschen. Um benutzerdefinierte Kennungen von einem Bericht oder einer Abfrage zu entfernen, bearbeiten Sie den Bericht oder die Abfrage.

Kapitel 11: Format für Datum/Uhrzeit

CA Enterprise Log Manager verwendet unterschiedliche Gebietsschema-Eigenschaftsdateien, um den Benutzeroberflächeninhalt eines Gebietsschemas anzuzeigen. CA Enterprise Log Manager gibt die folgenden Gebietsschemadateien im Verzeichnis /opt/CA-/LogManager/Gebietsschema an:

- de_ui.properties
- en_ui.properties
- fr_ui.properties
- ja_ui.properties
- es_ui.properties
- it_ui.properties

Diese Gebietsschema-Eigenschaftsdateien werden durch Versionen, Service Packs und automatische Software-Updates aktualisiert. Sie können diese Gebietsschema-Eigenschaftsdateien dazu verwenden, das Standardformat für Datum/Uhrzeit in ein Datums-/Uhrzeitformat Ihrer Wahl zu ändern. Das konfigurierte Format für Datum/Uhrzeit wird auf der Benutzeroberfläche und in den Abfrage- und Berichtsergebnissen angezeigt.

Dieses Kapitel enthält folgende Themen:

Unterstützte Formate für Datum/Uhrzeit

CA Enterprise Log Manager unterstützt folgende Formate für Datum/Uhrzeit:

Buchstabe	Beschreibung
Y	Zeigt ein Jahr an. Folgende Werte stehen zur Verfügung: ■ Zwei ■ Vier Bei zwei Buchstaben wird der Wert als zwei Ziffern interpretiert. Zum Beispiel YY=11 für das Jahr 2011. Bei vier Buchstaben wird der Wert als vier Ziffern interpretiert. Zum Beispiel YYYY=2011.
M	Zeigt einen Monat des Jahres an. Folgende Werte stehen zur Verfügung: ■ Eins ■ Zwei ■ Drei ■ Vier Bei einem Buchstaben wird der Wert als ein oder zwei Ziffern interpretiert. Zum Beispiel M=1 oder 11. Bei zwei Buchstaben wird der Wert als zwei Ziffern interpretiert. Zum Beispiel MM=01. Bei drei Buchstaben wird der Wert als drei Buchstaben interpretiert. Zum Beispiel MMM=Jan. Bei vier Buchstaben wird der Wert als Volltext interpretiert. Zum Beispiel MMMM=Januar.
D	Zeigt einen Tag des Monats an. Folgende Werte stehen zur Verfügung: ■ Eins ■ Zwei Bei einem Buchstaben wird der Wert als ein oder zwei Ziffern interpretiert. Zum Beispiel D=1 oder 11. Bei zwei Buchstaben wird der Wert als zwei Ziffern interpretiert. Zum Beispiel DD=01 oder 11.

Buchstabe	Beschreibung
E	Zeigt einen Tag einer Woche an. Folgende Werte stehen zur Verfügung: ■ Drei ■ Vier Bei drei Buchstaben wird der Wert als drei Buchstaben interpretiert. Zum Beispiel EEE=Mon. Bei vier Buchstaben wird der Wert als Volltext interpretiert. Zum Beispiel EEEE=Montag.
A	Zeigt ein Zeitformat an. Folgende Werte stehen zur Verfügung: ■ AM ■ PM
J	Zeigt die Stunde auf einer 24-Stunden-Uhr mit dem Bereich 0-23 an.
H	Zeigt die Stunde auf einer 24-Stunden-Uhr mit dem Bereich 1-24 an.
K	Zeigt die Stunde auf einer 12-Stunden-Uhr mit dem Bereich 0-11 an.
L	Zeigt die Stunde auf einer 12-Stunden-Uhr mit dem Bereich 1-12 an.
N	Zeigt eine Minute in der Stunde an. Folgende Werte stehen zur Verfügung: ■ Eins ■ Zwei Bei einem Buchstaben wird der Wert als ein oder zwei Ziffern interpretiert. Zum Beispiel N=1 oder 11. Bei zwei Buchstaben wird der Wert als zwei Ziffern interpretiert. Zum Beispiel NN=01 oder 11.
S	Zeigt eine Sekunde in der Minute an. Folgender Wert ist möglich: ■ Zwei Bei zwei Buchstaben wird der Wert als zwei Ziffern interpretiert. Zum Beispiel SS=01 oder 11.
Q	Zeigt eine Millisekunde in der Sekunde an. Folgende Werte stehen zur Verfügung: ■ Zwei ■ Drei Bei zwei Buchstaben wird der Wert als zwei Ziffern interpretiert. Zum Beispiel QQ=01 oder 11. Bei drei Buchstaben wird der Wert als drei Ziffern interpretiert. Zum Beispiel QQQ=001.

Wenn zum Beispiel das aktuelle Datum der 11.Februar 2011 ist und die aktuelle Zeit 14:20:12 auf einer 24-Stunden-Uhr, kann das Format für Datum/Uhrzeit eines der folgenden Formate sein:

- EEEE, MMM. D, YYYY J:NN:QQQ—Freitag, Feb. 11, 2011 14:20:12
- EEEE, MMM. D, YYYY K:NN:SS A—Freitag, Feb. 11, 2011 14:20:12
- DD/MM/YYYY—02.11.11
- MM/DD/YYYY—11.02.11

So verändern Sie das Format für Datum/Uhrzeit

Sie können die folgenden Schritte ausführen, um das Format für Datum/Uhrzeit zu ändern:

1. Erstellen Sie eine Gebietsschema-Eigenschaftsdatei. Wenn Ihre Browsersprache beispielsweise Englisch ist und Sie das Format für Datum/Uhrzeit von Großbritannien verwenden wollen, erstellen Sie eine Gebietsschema-Eigenschaftsdatei mit dem Namen "en-GB_ui.properties".

   Hinweis: Der Name der Gebietsschema-Eigenschaftsdatei muss mit dem Namen der Sprache übereinstimmen, der in den Spracheinstellungen des Browsers angezeigt wird.
2. Kopieren Sie den Inhalt der Gebietsschema-Eigenschaftsdatei "en_ui.properties" in die Gebietsschema-Eigenschaftsdatei "en-GB_ui.properties".
3. Öffnen Sie die Gebietsschema-Eigenschaftsdatei "en-GB_ui.properties" und bearbeiten Sie die Eigenschaften für "dateFormat" und "formatString".
4. Speichern Sie die Änderungen.
5. Starten Sie iGateway neu.

Hinweis: Sie müssen eine Gebietsschema-Eigenschaftsdatei aktualisieren, die Sie mit dem neuesten Inhalt der entsprechenden, von CA Enterprise Log Manager zur Verfügung gestellten Gebietsschema-Eigenschaftsdatei erstellt haben. Sie können die Datei nach der Aktualisierung anpassen.

Weitere Informationen:

Unterstützte Formate für Datum/Uhrzeit (siehe Seite 294)

Anzeigen von Abfragen

Alle Benutzer, denen die Rolle "Auditor", "Analyst" oder "Administrator" zugewiesen wurde, können alle Abfragen anzeigen. Vordefinierte Abfragen werden unterhalb des Ordners "Automatisches Software-Update" aufgelistet. Beim Definieren der ersten benutzerdefinierten Abfrage wird der Abfrageliste ein Ordner "Benutzer" hinzugefügt, in dem die benutzerdefinierte Abfrage gespeichert wird. Danach werden alle benutzerdefinierten Abfragen diesem Ordner "Benutzer" hinzugefügt.

So zeigen Sie Abfragen an

1. Klicken Sie auf die Registerkarte "Abfragen und Berichte" und dann auf die Unterregisterkarte "Abfragen".

   Im linken Fensterbereich werden die Schaltfläche "Maximieren" für Abfragekennungsfilter, die Abfrageliste und das Menü "Optionen" sowie ein Textfeld "Suchen" angezeigt.

2. Wählen Sie die Abfrage aus, die Sie anzeigen möchten. Hierzu haben Sie folgende Möglichkeiten:

   - Blättern Sie durch die Abfrageliste und wählen Sie eine Abfrage zur Ansicht aus.
   - Geben Sie ein Schlüsselwort in das Feld "Suchen" ein, um nur die Abfragen anzuzeigen, deren Namen das eingegebene Wort enthalten.
   - Wählen Sie entweder eine angezeigte Kennung aus, oder geben Sie ein Schüsselwort in das Suchfeld "Kennung" ein, um die angezeigten Kennungen einzugrenzen. Wählen Sie eine Kennung aus, um die zugehörigen Abfragen anzuzeigen. Wählen Sie die anzuzeigende Abfrage aus.
   - Bei der Suche nach einer benutzerdefinierten Abfrage blenden Sie den Ordner "Automatisches Software-Update" aus, blenden Sie den Ordner "Benutzer" ein und blättern Sie dann durch die Liste unter dem Ordner "Benutzer".

   Die ausgewählte Abfrage wird im Detailbereich im Tabellenformat angezeigt. Die aktuellsten Ergebnisse werden zuerst in der Tabelle "Ergebnisse" angezeigt. Um zusätzliche Ergebnisse anzuzeigen, klicken Sie auf die Pfeiltasten oder wählen Sie einen Zeilenbereich aus der Liste aus.

   Hinweis: Wenn die Abfrageergebnisse nicht gruppiert sind, enthält die Liste den von Ihnen angezeigten Zeilenbereich sowie den darauffolgenden verfügbaren Bereich. Wenn die Abfrageergebnisse gruppiert sind, zeigt die Liste alle verfügbaren Zeilenbereiche im Ergebnis an.

3. (Optional) Führen Sie eine der folgenden Aktionen aus:
   - Klicken Sie auf "Lokale Filter bearbeiten", um Filter festzulegen, durch die nur die gewünschten Daten angezeigt werden. Um die ursprüngliche Abfrageanzeige wiederherzustellen, klicken Sie auf "Lokale Filter aufheben".
   - Klicken Sie auf "Zu Favoriten hinzufügen", um Ihren Favoriten die angezeigte Abfrage oder den angezeigten Bericht hinzuzufügen.
   - Klicken Sie auf "Aktualisieren", um die Daten mit den zuletzt hinzugefügten Angaben zu aktualisieren.
   - Klicken Sie zum Drucken der Abfrage auf "Drucken".
4. Klicken Sie auf "Schließen", um die angezeigte Abfrage zu schließen.

Anzeigen von Berichten

Alle Benutzer, denen die Rolle "Auditor", "Analyst" oder "Administrator" zugewiesen wurde, können alle Berichte anzeigen. Vordefinierte Berichte werden unterhalb des Ordners "Automatisches Software-Update" aufgelistet. Beim Definieren des ersten benutzerdefinierten Berichts wird der Berichtsliste ein Ordner "Benutzer" hinzugefügt, in dem der benutzerdefinierte Bericht gespeichert wird. Danach werden alle benutzerdefinierten Berichte diesem Ordner "Benutzer" hinzugefügt.

Wenn Sie einen Bericht aus der Berichtsliste auswählen, werden die Abfragen, aus denen sich der Bericht zusammensetzt, für Protokolldatensätze ausgeführt, die sich derzeit in den internen Ereignisprotokollspeichern befinden. Die im rechten Fensterbereich angezeigten Berichtsergebnisse stammen aus den Ereignisprotokollspeichern des aktiven CA Enterprise Log Manager-Servers und seinen untergeordneten Servern.

So zeigen Sie Berichte an:

1. Klicken Sie auf die Registerkarte "Abfragen und Berichte" und dann auf die Unterregisterkarte "Berichte".

   Im linken Fensterbereich werden die Schaltfläche "Maximieren" für Berichtskennungsfilter, ein Eingabefeld "Suchen", die Berichtsliste und das Menü "Optionen" angezeigt.

2. Wählen Sie im Menü "Optionen" die Option "Ausgewählten Bericht anzeigen" aus, sofern sie noch nicht ausgewählt ist.

   Hierdurch können Sie jeden beliebigen ausgewählten Bericht im rechten Fensterbereich anzeigen.

3. Wählen Sie den Bericht aus, den Sie anzeigen möchten. Hierzu haben Sie folgende Möglichkeiten:

   - durch die Berichtsliste blättern und einen anzuzeigenden Bericht auswählen
   - ein Schlüsselwort in das Eingabefeld "Suchen" des Berichts eingeben und aus der gefilterten Liste einen anzuzeigenden Bericht auswählen
   - auf die Schaltfläche "Maximieren" klicken, um die Liste der Berichtskennungsfilter anzuzeigen Wählen Sie entweder eine angezeigte Kennung aus, oder geben Sie ein Schüsselwort in das Suchfeld "Kennung" ein, um die angezeigten Kennungen einzugrenzen. Wählen Sie eine Kennung aus, um die zugehörigen Berichte anzuzeigen. Wählen Sie den anzuzeigenden Bericht aus.
   - Wenn Sie nach einem benutzerdefinierten Bericht suchen, kontrahieren Sie den Ordner "Automatisches Software-Update", erweitern Sie den Ordner "Benutzer" und scrollen Sie dann durch die Ordnerliste "Benutzer".

   Der ausgewählte Bericht wird im Hauptfenster der Seite angezeigt.

4. (Optional) Führen Sie eine der folgenden Aktionen aus:

   - Klicken Sie auf "Lokale Filter bearbeiten", um Filter festzulegen, durch die nur die gewünschten Daten angezeigt werden. Um die ursprüngliche Darstellung des Berichts wiederherzustellen, klicken Sie auf "Lokale Filter löschen".
   - Klicken Sie auf "Zu Favoriten hinzufügen", um den angezeigten Bericht zu Ihrer Favoritenliste hinzuzufügen.
   - Klicken Sie auf "Aktualisieren", um die Daten mit den zuletzt hinzugefügten Angaben zu aktualisieren.
   - Klicken Sie zum Drucken des Berichts auf "Drucken".

5. Klicken Sie auf "Schließen", um den angezeigten Bericht zu schließen.

Deaktivieren der Anzeige eines ausgewählten Berichts

Sie können Ihre Berichtliste so festlegen, dass Sie Änderungen durchführen können, ohne Berichte zu laden. Normalerweise wird ein Bericht im Detailfenster angezeigt, wenn Sie ihn in der Liste auswählen.

Wenn Sie diese Standardeinstellung deaktivieren, sparen Sie Zeit, da Sie einen Bericht aus der Liste auswählen und sofort bearbeiten können, ohne warten zu müssen, bis er angezeigt wird. Dies ist besonders hilfreich, wenn Sie mehrere Berichte bearbeiten müssen und bereits wissen, welche Änderungen Sie vornehmen möchten.

Da nur Benutzer mit der Rolle "Administrator" oder "Analyst" Berichte erstellen oder bearbeiten können, können nur diese Benutzer die Einstellung zum Anzeigen eines ausgewählten Berichts deaktivieren.

So deaktivieren Sie die Anzeige eines ausgewählten Berichts:

1. Klicken Sie oben in der Berichtsliste auf "Optionen".

   Das Menü "Optionen" wird angezeigt.

2. Deaktivieren Sie die Option "Ausgewählten Bericht anzeigen".

   Berichte, die aus dieser Liste ausgewählt werden, werden erst wieder angezeigt, wenn die Option "Ausgewählten Bericht anzeigen" wieder aktiviert wird.

Weitere Informationen

Generieren von Berichten (siehe Seite 349)
Bearbeiten von Berichten (siehe Seite 362)

Beispiel: PCI-Berichte ausführen

Der PCI Security Standards Council (Rat für Sicherheitsstandards) ist ein offenes internationales Forum, das für die Entwicklung des PCI-Datensicherheitsstandards (PCI DSS) verantwortlich ist, welcher Anforderungen an das Sicherheitsmanagement, Richtlinien und Verfahren umfasst. Organisationen, die Daten von Karteninhabern speichern, verarbeiten oder übertragen, müssen die PCI-DSS-Version 1.2 einhalten, in der zwölf Anforderungen gestellt werden.

CA Enterprise Log Manager liefert Standard-PCI-Berichte, die Sie anzeigen können, sobald Ihr System mit dem Erstellen und Bearbeiten von Ereignisprotokollen beginnt.

Die Beispiele in diesem Abschnitt sollen Ihnen dabei helfen, sich mit den PCI-Berichten sowie mit deren Planung und Verteilung vertraut zu machen. Die Beispiele schließen Referenzen zur Nummerierung der entsprechenden PCI-DDS-Anforderung ein, auf die der Bericht Bezug nimmt.

Weitere Informationen:

Die Liste der Berichte mit PC-Kennung anzeigen (siehe Seite 301)
Nach Berichten zu einer bestimmten PCI-DDS-Kontrolle suchen (siehe Seite 303)

Die Liste der Berichte mit PC-Kennung anzeigen

Um sich damit vertraut zu machen, sich Sie CA Enterprise Log Manager-Berichte zum Nachweis der PCI-Konformität verwenden lassen, können Sie als Erstes die Liste vordefinierter Berichte anzeigen, die mit einer PCI-Kennung versehen sind.

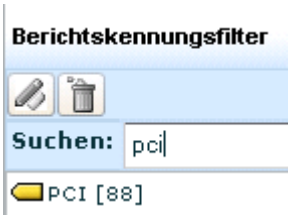
So machen Sie sich mit Berichten mit der PCI-Kennung vertraut:

1. Klicken Sie auf die Registerkarte "Abfragen und Berichte" und auf die Unter-Registerkarte "Berichte".

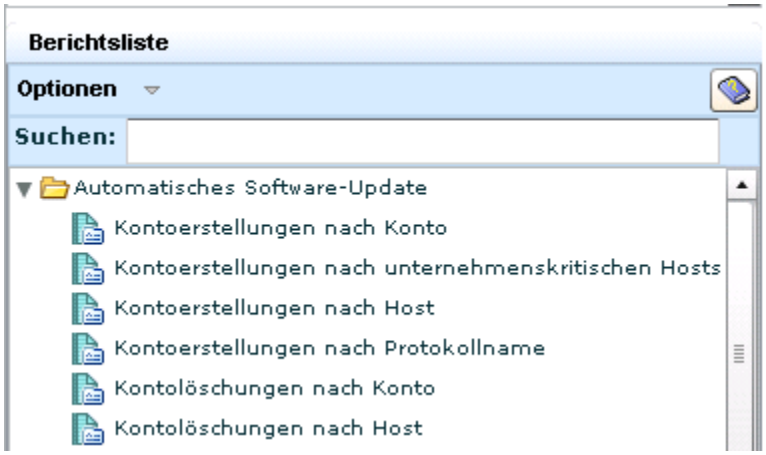
   "Berichtskennungsfilter" und "Berichtsliste" werden eingeblendet.

2. Geben Sie "PCI" in das Suchfeld für die Kennung ein.

   Die PCI-Kennung wird angezeigt.



3. Überprüfen Sie die Liste der Berichte, die auf die PCI-Kennung Bezug nehmen.



Nach Berichten zu einer bestimmten PCI-DDS-Kontrolle suchen

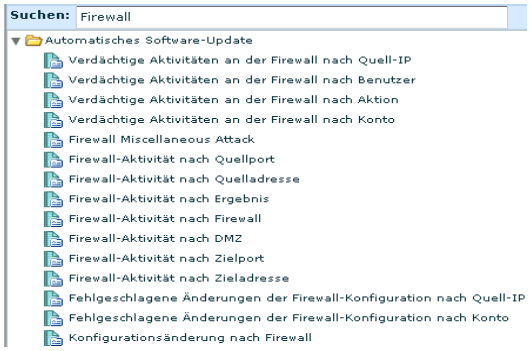
Sie können nach vordefinierten Berichten mit Hilfe von Stichwörtern suchen, die im Rahmen bestimmter PCI-DDS-Kontrollen relevant sind. Das folgende Verfahren bietet eine Reihe von Beispielen.

Hinweis: Die referenzierten Nummern sind die Nummern, die mit der PCI-DDS-Anforderung verbunden sind, auf die der Bericht Bezug nimmt.

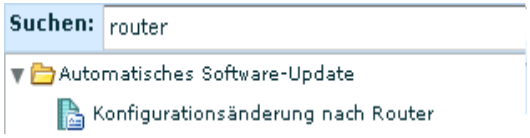
So können Sie die Liste der Berichte anzeigen, die für bestimmte PCI-DDS-Kontrollen relevant sind:

1. Klicken Sie auf die Registerkarte "Abfragen und Berichte" und auf die Unter-Registerkarte "Berichte".
2. Um den Bericht zu finden, der sich mit Änderungen an der Firewall-Konfiguration befasst (1.1.1), geben Sie "Firewall" als Suchkriterium ein.

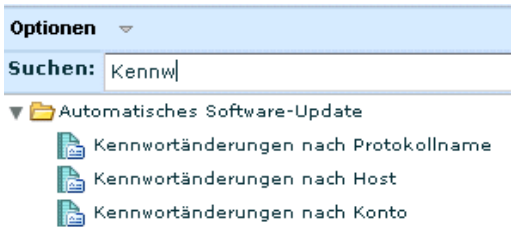
   Eine Liste mit Berichten ähnlich der hier gezeigten wird eingeblendet. Beachten Sie den Bericht mit dem Titel "Firewall-Konfigurationsänderungen".



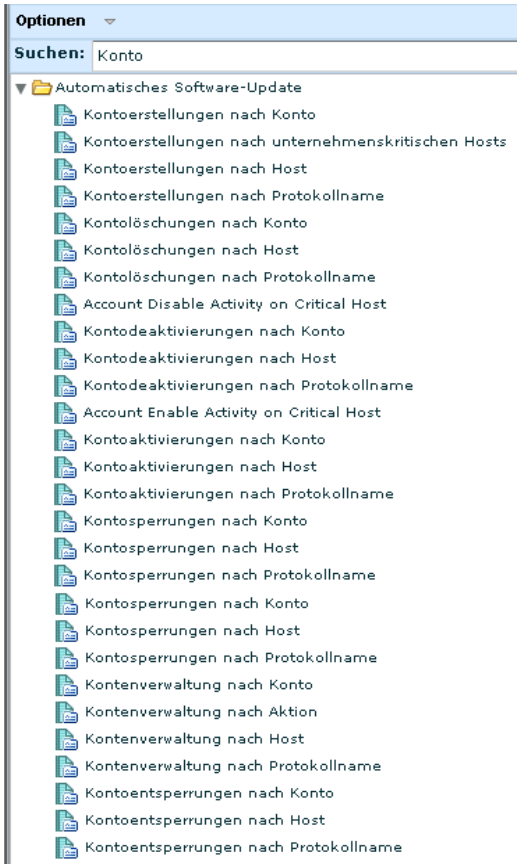
3. Um den Bericht zu finden, der sich mit Änderungen an Router-Konfigurationen befasst, nachdem Sie die Synchronisierung verifiziert haben (1.3.6), geben Sie "Router" als Suchkriterium ein.



4. Um Berichte zu finden, die sich mit der Kennwortverwaltung befassen (8.5), einer der durchgreifendsten Maßnahmen zur Zugriffskontrolle, geben Sie "Kennwort" als Suchkriterium ein.



5. Um Berichte zu finden, die sich mit dem Hinzufügen, der Modifikation und dem Löschen von Benutzerkonten befassen (12.5.4), einer der Maßnahmen zur Aufrechterhaltung von Informationssicherheitsrichtlinien, geben Sie "Konto" als Suchkriterium ein.



Arbeiten mit einem einzelnen PCI-Bericht

Sie können mit allen Berichten, einschließlich der PCI-Berichte, folgendermaßen arbeiten:

- den Bericht durch Auswahl des Berichtsnamens aus der Berichtsliste überprüfen;
- den Bericht drucken;
- einen Plan für den Bericht erstellen, um ihn z. B. an ausgewählte Empfänger zu mailen;
- den geplanten Berichtsjob überprüfen;
- Überprüfen Sie den erstellten Bericht.

So überprüfen Sie einen ausgewählten Bericht und reagieren auf ihn:

1. Klicken Sie auf die Registerkarte "Abfragen und Berichte" und auf die Unterregisterkarte "Berichte".
2. Wählen Sie in der Dropdown-Liste "Optionen" unter "Berichtsliste" "Ausgewählten Bericht anzeigen" aus, wenn dies nicht schon ausgewählt ist.
3. Wählen Sie einen Berichtsnamen aus der Berichtsliste aus.

   Der entsprechende Bericht zeigt die Ergebnisse der zugrunde liegenden Abfragen an, die üblicherweise eine Zusammenfassung, den Trend und Details enthalten, sowie die berichtsspezifischen Abfragen an.
4. Um das Laden bestimmter Abfragen zu inaktivieren, wählen Sie "Abbrechen".

5. Um den angezeigten Bericht auszudrucken, klicken Sie auf "Bericht drucken" im rechten Fensterbereich.

   Wenn das Dialogfeld "Drucken" eingeblendet wird, wählen Sie einen Drucker und klicken Sie auf "Drucken".
6. Um den zu erstellenden Bericht für eine spätere Überprüfung einzuplanen, klicken Sie auf "Bericht planen".

   Der Assistent "Bericht planen" wird geöffnet mit dem angezeigten Bericht im Bereich "Ausgewählte Berichte".

7. Geben Sie einen Jobnamen ein, z. B. "Berichtsjob Ressourcenzugriff nach Host".

   Wenn Sie alle Standardeinstellungen akzeptieren, dann ist der Job so geplant, dass er einmal ohne Wiederholung ausgeführt wird, wobei der Bericht im PDF-Format erstellt wird und keine E-Mail-Benachrichtigung erfolgt. Die Daten werden vom aktuellen Server sowie den ihm gleichgeordneten und untergeordneten Servern im Verbund eingeholt.

8. Klicken Sie auf "Speichern und schließen".

9. Überprüfen Sie den geplanten Job. Klicken Sie auf die Registerkarte "Geplante Berichte" und dann auf die Unter-Registerkarte "Berichtsplanung".

   Der Job, den Sie gerade geplant haben, wird angezeigt.

10. Überprüfen Sie den erstellten Bericht.

    a. Klicken Sie auf die Registerkarte "Geplante Berichte" und dann auf die Unter-Registerkarte "Erstellte Berichte".

    b. (Optional) Grenzen Sie die angezeigten Zeilen ein, indem Sie für "Wiederholung" eine andere Option als "Alle", ein anderes Format als "Alle" oder einen anderen Zeitraum als "Letzte Stunde" auswählen.

    c. (Optional) Klicken Sie auf "Aktualisieren".

11. Nachdem Sie den erstellten Bericht überprüft haben, können Sie den Berichtsjob modifizieren, wenn Sie möchten, dass er mehrmals ausgeführt wird. Gehen Sie wie folgt vor:

    a. Wählen Sie den erstellten Bericht in der Unter-Registerkarte "Berichte planen" aus und klicken Sie auf "Bearbeiten".

    b. Wählen Sie den Schritt "Berichte planen" aus, und wählen Sie die Option für die Wiederholungshäufigkeit.

    c. Klicken Sie auf "Speichern und schließen".

Eingabeaufforderungen

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.

Basierend auf den Ergebnissen der Eingabeaufforderungsabfrage können Sie folgende Aktionen durchführen:

- Wählen Sie "Rohereignisse anzeigen", um statt den verfeinerten Ergebnissen das entsprechende Rohereignis und den Zeitpunkt anzuzeigen, zu dem es auftrat.
- Geben Sie in das Feld "Übereinstimmung" eine Zeichenfolge ein, und klicken Sie auf "Los", um die Anzeige nach Zeilen mit Daten zu filtern, die mit Ihrer Eingabe übereinstimmen.
- Wählen Sie die Option "Abfragedaten exportieren", um die Abfrageergebnisse in ein PDF-Dokument, ein Excel-Arbeitsblatt oder in eine XML-Datei zu exportieren.
- Wählen Sie "Ergebnisbedingungen", um die Anzeige nach einem bestimmten Datumsbereich zu filtern; legen Sie eine Begrenzung für die zurückgegebenen Zeilen fest, oder ändern Sie die Granularität der angegebenen Zeit. Alternativ dazu können Sie die Ergebnisbedingungen auf die Standardeinstellungen zurücksetzen.
- Wählen Sie die Option "Lokale Filter anzeigen/bearbeiten", um Schnellfilter oder erweiterte Filter festzulegen.
- Drucken Sie die Abfrage auf einem ausgewählten lokalen Drucker aus.
- Aktualisieren Sie die Abfragedaten manuell oder mit Hilfe der Option "Automatische Aktualisierung".

Arbeiten mit der Connector-Eingabeaufforderung

Jeder auf einem Agenten konfigurierte Connector erfasst Rohereignisse von einer bestimmten Ereignisquelle und sendet die Ereignisse an den Ereignisprotokollspeicher auf einem CA Enterprise Log Manager-Erfassungsserver. Beim Ereignisverfeinerungsprozess werden Rohereignisse in verfeinerte Ereignisse konvertiert und im CA Enterprise Log Manager-Berichtsserver archiviert. Bei der Connector-Eingabeaufforderung erfolgt eine Abfrage nach Ereignissen auf dem Berichtsserver, welche als Rohereignisse von Connectors erfasst wurden, deren Namen Sie festlegen. Connectors haben entweder einen Standardnamen oder einen benutzerdefinierten Namen. Kopieren Sie den Namen des zu verwendenden Connectors, und fügen Sie ihn in das Feld der Connector-Eingabeaufforderung ein. Klicken Sie anschließend auf "Los", um die Ergebnisse der Eingabeaufforderungsabfrage anzuzeigen.

Mit der Connector-Eingabeaufforderung können Sie folgende Aktionen durchführen:

- Anzeigen der Ereignisse aller Connectors, die auf derselben Integration basieren; dies ist möglich, wenn Sie beim Bereitstellen von Connectors den Connector-Standardnamen akzeptieren.
- Überprüfen, ob ein neuer Connector Ereignisse abruft; wenn mehrere Agenten Connectors mit dem von Ihnen angegebenen Namen haben, geben Sie den Agentennamen in das Feld "Übereinstimmung" ein, um die Abfrageergebnisse auf Ereignisse einzugrenzen, die vom neuen Connector abgerufen werden.

So kopieren Sie den Namen eines aktiven Connectors:

1. Klicken Sie auf die Registerkarte "Verwaltung".

   Der Protokollerfassungs-Explorer wird geöffnet.

2. Klicken Sie auf "Agenten-Explorer".

   Die Agentenstatusüberwachung wird angezeigt. Darin finden Sie eine Spalte mit Connector-Namen.

3. Klicken Sie mit der rechten Maustaste auf den in der Eingabeaufforderungsabfrage zu verwendenden Connector, und wählen Sie die Option "Connectorname kopieren" aus.

So verwenden Sie die Connector-Eingabeaufforderung:

1. Wählen Sie "Abfragen und Berichte" aus.

   Die Abfrageliste zeigt den Ordner "Eingabeaufforderungen", den Ordner "Automatisches Software-Update" und ggf. den Ordner "Benutzer".

2. Erweitern Sie die Eingabeaufforderung, und wählen Sie "Connector".

   Die Connector-Eingabeaufforderung enthält das Feld "Connector" und das nachstehende CEG-Feld. Dieses Feld muss markiert bleiben, damit die Eingabeaufforderung funktioniert.

   agent_connector_name

   ist der Name eines Connectors.

3. Klicken Sie mit der rechten Maustaste in das Feld "Connector" und anschließend auf "Einfügen".

   Der Connector-Name, den Sie in der Agentenstatusüberwachung kopiert hatten, wird im Feld "Connector" angezeigt.

4. Klicken Sie auf "Los".

   Es werden die Ergebnisse der Connector-Eingabeaufforderungsabfrage angezeigt.

5. Interpretieren Sie die Abfrageergebnisse mit Hilfe der folgenden Beschreibungen:

   CA-Schweregrad

   Gibt den Schweregrad des Ereignisses an. Zu den Werten in aufsteigender Reihenfolge nach Schweregrad zählen: "Informationen", "Warnung", "Geringfügige Auswirkung", "Schwerwiegende Auswirkung", "Kritisch" und "Schwerwiegend".

   Datum

   Gibt den Zeitpunkt an, zu dem das Ereignis aufgetreten ist.

   Kategorie

   Gibt die Kategorie der oberen Ebene der entsprechenden Ereignisaktion an. "Systemzugriff" ist beispielsweise die Kategorie für die Aktion "Authentifizierung".

   Aktion

   Gibt die Aktion an; nach Möglichkeit werden Aktionen durch die Ereignisklasse bestimmt.

Agent Name (Agentenname)

Gibt den Agenten an, auf dem der Connector ausgeführt wird.

Host

Gibt den Ereignisquell-Host an, von dem der Connector Ereignisse erfasst.

Benutzer

Gibt den ursprünglichen Akteur des Ereignisses an, d. h. die Identität, die die Aktion initiiert hat. Der Benutzer kann als Quellbenutzername oder Quellprozessname angegeben werden.

Konto

Gibt den Benutzernamen des Kontos an, das für die Authentifizierung verwendet wird, wenn der Connector versucht, eine Verbindung zum Host mit der Ereignisquelle aufzubauen, von dem Rohereignisse erfasst werden. Hierbei handelt es sich in der Regel um ein Konto mit eingeschränkten Berechtigungen. Die Anmeldeinformationen für dieses Konto werden sowohl auf der Ereignisquelle als auch auf dem Protokollsensor des Connectors konfiguriert.

Ergebnis

Gibt einen Code für das Ereignisergebnis der entsprechenden Aktion an. Mögliche Werte sind S für Success (Erfolg), F für Failure (Fehler), A für Accepted (Akzeptiert), D für Dropped (Verworfen), R für Rejected (Zurückgewiesen) und U für Unknown (Unbekannt).

Connector-Name

Der Name des Connectors, der in das Filterfeld der Eingabeaufforderung eingegeben wird.

6. (Optional) Wählen Sie die Option "Rohereignisse anzeigen" aus.

   Das erste von einem neuen Connector erfasste Ereignis ist für die Aktion "Systemstart" bestimmt und endet mit: result_string=<connector name> Connector erfolgreich gestartet.

Arbeiten mit der Host-Eingabeaufforderung

Bei der Host-Eingabeaufforderung erfolgt eine Abfrage nach Ereignissen, bei denen der von Ihnen angegebene Hostname in den ausgewählten CEG-Feldern des verfeinerten Ereignisses angezeigt wird. Werden Rohereignisdaten verfeinert, können Ereignisdetails mehrere unterschiedliche CEG-Hostnamen aufweisen. Betrachten Sie folgendes Szenario:

1. Der Ereignisinitiator auf "source_hostname" versucht, eine "event_action"-Aktion auf einem Ziel durchzuführen, das sich auf "dest_hostname" befindet.

   Hinweis: "Source_hostname" und "dest_hostname" können verschiedene Hosts oder denselben Host bezeichnen.

2. Dieses Ereignis wird in einem Repository auf "event_source_hostname" aufgezeichnet.

   Hinweis: "Event_source_name" kann einen anderen Host als "source_hostname" oder "dest_hostname" bezeichnen, oder die Host liegen am selben Ort.

3. Ein auf "agent_hostname" installierter CA Enterprise Log Manager-Agent erstellt eine Kopie des auf "event_source_hostname" aufgezeichneten Ereignisses.

   Hinweis: "Agent_hostname" ist in einer agentbasierten Protokollerfassung identisch mit "event_source_name". Dies trifft jedoch nicht auf die direkte Protokollerfassung ohne Agent zu.

4. Der CA Enterprise Log Manager-Agent auf "agent_hostname" überträgt die Kopie des Ereignisses in "event_logname" an einen CA Enterprise Log Manager-Erfassungsserver.

So verwenden Sie die Host-Eingabeaufforderung:

1. Wählen Sie "Abfragen und Berichte" aus.

   In der Abfrageliste werden der Ordner "Eingabeaufforderungen" und mindestens ein Ordner für weitere Abfragen angezeigt.

2. Erweitern Sie die Eingabeaufforderung, und wählen Sie "Host".

   Die Host-Eingabeaufforderung wird angezeigt.

3. Geben Sie den Namen des Hosts ein, auf dem diese Abfrage beruhen soll.

4. Wählen Sie die Felder aus, nach denen Daten abgefragt werden, die mit dem von Ihnen eingegebenen Hostnamen übereinstimmen.

   source_hostname

   Steht für den Namen des Hosts, auf dem die Ereignisaktion initiiert wurde.

   dest_hostname

   Steht für den Namen eines Hosts, der als Ziel für die Aktion dient.

   event_source_hostname

   Steht für den Namen eines Hosts, der das Ereignis aufzeichnet, wenn es auftritt.

   Beispielsweise können Sie einen auf WinRM basierenden Connector bereitstellen, um Ereignisse von der Ereignisanzeige auf einem Windows Server 2008-Host zu erfassen. Zum Auswählen von Ereignissen, die von einem bestimmten Windows Server 2008-Host abgerufen wurden, geben Sie den Hostnamen des Servers ein und wählen dieses Feld aus.

   receiver_hostname

   Ist identisch mit "agent_hostname".

   agent_hostname

   Steht für den Namen des Hosts, auf dem ein CA Enterprise Log Manager-Agent bereitgestellt wird.

5. Klicken Sie auf "Los".

   Es werden die Ergebnisse der Host-Eingabeaufforderungsabfrage angezeigt.

6. Interpretieren Sie die Abfrageergebnisse mit Hilfe der folgenden Beschreibungen:

CA-Schweregrad

Gibt den Schweregrad des Ereignisses an. Zu den Werten in aufsteigender Reihenfolge nach Schweregrad zählen: "Informationen", "Warnung", "Geringfügige Auswirkung", "Schwerwiegende Auswirkung", "Kritisch" und "Schwerwiegend".

Datum

Gibt den Zeitpunkt an, zu dem das Ereignis aufgetreten ist.

Quellbenutzer

Gibt den Namen des Benutzers auf "source_hostname" an, der die Ereignisaktion initiiert hat.

Ergebnis

Gibt einen Code für das Ereignisergebnis der entsprechenden Aktion an. Hierbei stehen "S" für "Erfolgreich" (Success), "F" für "Fehler" (Failure), "A" für "Accepted" (Akzeptiert), "D" für "Dropped" (Verworfen), "R" für "Rejected" (Zurückgewiesen) und "U" für "Unknown" (Unbekannt).

Agentenhost

Gibt den Namen des Hosts an, auf dem der CA Enterprise Log Manager-Agent, der das Ereignis erfasst hat, installiert ist.

Empfängerhost

Ist identisch mit dem Agentenhost.

Kategorie

Gibt die Kategorie der oberen Ebene der entsprechenden Ereignisaktion an. "Systemzugriff" ist beispielsweise die Kategorie für die Aktion "Authentifizierung".

Aktion

Gibt die vom Quellbenutzer durchgeführte Ereignisaktion an.

Protokollname

Gibt den vom Connector, der das Ereignis erfasst hat, verwendeten Protokollnamen an. Alle auf derselben Integration basierenden Connectors übermitteln Ereignisse in einer Protokolldatei mit demselben Protokollnamen.

Arbeiten mit der IP-Eingabeaufforderung

Bei der IP-Eingabeaufforderung erfolgt eine Abfrage nach Ereignissen, bei denen die von Ihnen angegebene IP-Adresse in den ausgewählten CEG-Feldern des verfeinerten Ereignisses angezeigt wird. Werden Rohereignisdaten verfeinert, können Ereignisdetails mehrere unterschiedliche CEG-IP-Adressen aufweisen. Betrachten Sie folgendes Szenario:

1. Der Ereignisinitiator auf "source_address" versucht, eine "event_action"-Aktion auf einem Ziel durchzuführen, das sich auf "dest_address" befindet.

   Hinweis: "Source_address" und "dest_address" können sich unterscheiden oder identisch sein.

2. Dieses Ereignis wird in einem Repository auf "event_source_address" aufgezeichnet.

   Hinweis: "Event_source_address" kann sich entweder von "source_address" oder "dest_address" unterscheiden oder mit einer oder beiden identisch sein.

3. Ein auf "agent_address" installierter CA Enterprise Log Manager-Agent erstellt eine Kopie des auf "event_source_address" aufgezeichneten Ereignisses.

   Hinweis: "Agent_address" ist in einer agentbasierten Protokollerfassung identisch mit "event_source_address". Dies trifft jedoch nicht auf die direkte Protokollerfassung ohne Agent zu.

4. Der Agent auf "agent_address" überträgt die Kopie des Ereignisses in "event_logname" an einen CA Enterprise Log Manager-Erfassungsserver.

So verwenden Sie die IP-Eingabeaufforderung:

1. Wählen Sie "Abfragen und Berichte" aus.

   In der Abfrageliste werden der Ordner "Eingabeaufforderungen" und mindestens ein Ordner für weitere Abfragen angezeigt.

2. Erweitern Sie die Eingabeaufforderung, und wählen Sie "Host".

   Die IP-Eingabeaufforderung wird angezeigt.

3. Geben Sie die IP-Adresse ein, auf der diese Abfrage beruhen soll.

4. Wählen Sie eines oder mehrere der folgenden Felder aus, um Daten abzufragen, die mit der von Ihnen eingegebenen IP-Adresse übereinstimmen.

   source_address

   Steht für die IP-Adresse des Hosts, auf dem die Aktion initiiert wurde.

   dest_address

   Steht für die IP-Adresse eines Hosts, der als Ziel für die Aktion dient.

   event_source_address

   Steht für die IP-Adresse eines Hosts, der das Rohereignis aufzeichnet, wenn es auftritt.

   Beispielsweise können Sie einen auf WinRM basierenden Connector bereitstellen, um Ereignisse von der Ereignisanzeige auf einem Windows Server 2008-Host zu erfassen. Zum Auswählen von Ereignissen, die von einem bestimmten Windows Server 2008-Host abgerufen wurden, geben Sie die IP-Adresse des Servers ein und wählen dieses Feld aus.

   receiver_hostaddress

   Ist identisch mit "agent_address".

   agent_address

   Steht für die IP-Adresse eines Hosts, auf dem ein CA Enterprise Log Manager-Agent bereitgestellt wird.

5. Klicken Sie auf "Los".

   Es werden die Ergebnisse der IP-Eingabeaufforderungsabfrage angezeigt.

6. Interpretieren Sie die Abfrageergebnisse mit Hilfe der folgenden Beschreibungen:

CA-Schweregrad

Gibt den Schweregrad des Ereignisses an. Zu den Werten in aufsteigender Reihenfolge nach Schweregrad zählen: "Informationen", "Warnung", "Geringfügige Auswirkung", "Schwerwiegende Auswirkung", "Kritisch" und "Schwerwiegend".

Datum

Gibt den Zeitpunkt an, zu dem das Ereignis aufgetreten ist.

Ergebnis

Gibt einen Code für das Ergebnis der entsprechenden Aktion an, wobei die angegebenen Buchstaben jeweils die folgende Bedeutung haben: S für Success (Erfolg), F für Failure (Fehler), A für Accepted (Akzeptiert), D für Dropped (Verworfen), R für Rejected (Zurückgewiesen) und U für Unknown (Unbekannt).

Zielport

Gibt den Kommunikationsanschluss auf dem Zielhost an, dem Ziel für die Ereignisaktion.

Quell-IP

Gibt die IP-Adresse an, von der aus die Ereignisaktion initiiert wurde.

Ziel-IP

Gibt die IP-Adresse des Hosts an, der als Ziel für die Ereignisaktion diente.

Ereignisquellen-IP

Gibt die IP-Adresse des Hosts mit dem Repository an, in dem das Ereignis ursprünglich aufgezeichnet wurde.

Agenten-IP

Gibt den Namen des Hosts mit dem CA Enterprise Log Manager-Agenten an, der für die Erfassung von Ereignissen von der Ereignisquelle verantwortlich ist.

Empfänger-IP

Ist identisch mit der Agenten-IP.

Kategorie

Gibt die Kategorie der oberen Ebene der entsprechenden Ereignisaktion an. "Systemzugriff" ist beispielsweise die Kategorie für die Aktion "Authentifizierung".

Aktion

Gibt die Ereignisaktion an.

Protokollname

Gibt den Protokollnamen an, welcher von dem Connector verwendet wird, der das Ereignis erfasst hat.

Verbindung mit der Protokollnamen-Eingabeaufforderung

Jeder Connector, Der Auf Derselben-Integrations-Basiert, gibt aus der Ereignisquelle erfasste Ereignisprotokolle eine Höhle CA Enterprise Log Manager-Erfassungsserver in einer Protokolldatei mit einem vordefinierten Namen zurück. Bei der Protokollnamen-Eingabeaufforderung erfolgt eine Abfrage nach Ereignissen im Zusammenhang mit dem von Ihnen angegebenen Protokollnamen.

Verwenden Sie als Protokollnamen-Eingabeaufforderung, um Ereignisse abzufragen sterben, in einer Protokolldatei mit dem angegebenen Namen übertragen werden sterben. Jeder-Connector-Basiert Auf Einer-Integration. Bei Jeder-Integration wird ein vordefinierter Protokollname verwendet. Eine Abfrage nach einem bestimmten Protokollnamen gibt Ereignisse zurück, als von verschiedenen Agenten erfasst wurden sterben. Letztere-Verwenden-Connectoren, als Auf-Derselben-Integration oder ähnlichen Integrationen basieren sterben.

Zur Benennung von Protokollen werden verschiedene Konventionen verwendet:

- Integrationsname - CA-Bündnis ist der Protokollname für sterben als CA_Federation_Manager-Integration.
- Produktname - McAfee-Schwachstellen-Manager ist der Protokollname für McAfee_VM und McAfee_VM_CM. FR. n. Chr Rechts-Verwaltungsdienste ist der Protokollname für Microsoft_Active_Directory_RMS und Microsoft_Active_Directory_RMS_ODBC.
- Anbietername: Oracle ist der Protokollname für Oracl10g, Oracle9i, Oracle_AppLog und Oracle_Syslog.
- Protokolltyp: Unix ist der Protokollname für sterben als folgenden Integrationen: AIX_Syslog, HPUX_Syslog, Linux_Syslog, SLES_Syslog und Solaris_Syslog.

Einige-Protokollnamen-Werden Erneut Verwendet, wenn neue Versionen oder Plattformen hinzukommen. Beispielsweise-Ist NT-Sicherheit der Protokollname für Sicherheitsprotokolle der folgenden Integrationen: NTEventLog, Windows2k8 und WinRM.

So verwenden Sie sterben Protokollnamen-Eingabeaufforderung:

1. Wählen Sie "Abfragen-Und Berichte" aus.

   In der Abfrageliste werden der Ordner "Eingabeaufforderungen" und mindestens ein Ordner für weitere Abfragen angezeigt.

2. Erweitern Sie als Eingabeaufforderung, und wählen Sie "Protokollname" sterben.

   Der-Filter-Der Protokollnamen-Eingabeaufforderung wird mit dem folgenden Feld angezeigt:

   event_logname

   Dieses-Feld-Steht-Für-Höhlen-Namen Einer Protokolldatei Im Zusammenhang Mit Einer Bestimmten-Integration.

3. Wählen Sie Den Protokollnamen-Aus, der für sterben als Übermittlung der Ereignisse, als Sie anzeigen möchten, verwendet wird sterben. Klicken-Sie-Anschließend-Auf "Los".

   Es-Werden als Ergebnisse Der Protokollnamen-Eingabeaufforderungsabfrage-Angezeigt sterben.

4. Interpretieren Sie als Abfrageergebnisse mit Hilfe der folgenden Beschreibungen sterben:

   CA-Schweregrad

   Gibt den Schweregrad des Ereignisses ein. Zu den Werten in aufsteigender Reihenfolge nach Schweregrad zählen: "Informationen", "Warnung", "Geringfügige Auswirkung","Schwerwiegende Auswirkung", "Kritisch"-Und "Schwerwiegend".

   Datum

   Gibt den Zeitpunkt ein, zu dem das Ereignis aufgetreten ist.

   Kategorie

   Gibt als Kategorie der oberen Ebene der entsprechenden Ereignisaktion sterben ein. "Systemzugriff"-Ist-Beispielsweise als Kategorie für sterben als Aktion "Authentifizierung" sterben.

   Aktion:

   Gibt als vom entsprechenden Benutzer durchgeführte Ereignisaktion sterben ein.

Host

Gibt den Ereignisquell-Host ein, Von Dem Der-Connector Ereignisse erfasst.

Benutzer

Gibt-Höhle ursprünglichen Akteur des Ereignisses ein, d. h. sterben Sie als Identität, sterben als Aktion-Initiiert-Hut sterben. Der Benutzer kann als Quellbenutzername oder Quellprozessname angegeben werden.

Konto

Gibt-Höhle Benutzernamen des für sterben als Authentifizierung verwendeten Kontos ein. Wenn Der Connector-Versucht, eine Verbindung zur Ereignisquelle herzustellen, wird eine Authentifizierung durchgeführt. Bei Der Authentifizierung-Wird in Der-Wiedergel ein Konto mit eingeschränkten Berechtigungen verwendet. Während Der Connector-Bereitstellung-Konfiguriert-Der-Administratoren-Anmeldeinformationen-Für-Dieses-Konto-Auf-Der-Ereignisquelle-Und-Identifiziert-Dieses-Konto-Anschließend-Auf-Dem Protokollsensor.

Ergebnis

Gibt-Einen-Code für das Ereignisergebnis der entsprechenden Aktion ein. Hierbei-Stehen-"S"-Für "Erfolgreich" (Erfolg), "F"-Für "Fehler" (Fehler), "ein" für "Akzeptierte" (Akzeptiert), "Gefallenes" "D"-Für (Verworfen), "R"-Für "Ablehnte" (Zurückgewiesen) Und-"U"-Für "Unbekannt" (Unbekannt).

Protokollname

Der-Im-Filterfeld-Der-Eingabeaufforderung-Eingegebene Protokollname.

Arbeiten mit der Port-Eingabeaufforderung

Bei der Port-Eingabeaufforderung erfolgt eine Abfrage nach Ereignissen, bei denen der von Ihnen angegebene Port in den ausgewählten CEG-Feldern des verfeinerten Ereignisses angezeigt wird. Werden Rohereignisdaten verfeinert, können Ereignisdetails mehrere unterschiedliche CEG-Port-Nummern aufweisen. Betrachten Sie folgendes Szenario:

1. Der Ereignisinitiator auf dem Quellhost verwendet den ausgehenden Kommunikationsanschluss "source_port" zur Initialisierung der Ereignisaktion auf einem Ziel des Zielhosts durch den eingehenden Kommunikationsanschluss "dest_port".

   Hinweis: Source_port und dest_port sind identisch bei lokalen Ereignissen. Ansonsten sind sie Host-spezifisch.

2. Dieses Ereignis wird in einem Repository an der Ereignisquelle erfasst.
3. Ein CA Enterprise Log Manager-Agent erstellt eine Kopie des auf der Ereignisquelle aufgezeichneten Ereignisses.
4. Der Agent überträgt die Kopie des Ereignisses über den ausgehenden Port "receiver_port" an einen CA Enterprise Log Manager-Erfassungsserver.

   Hinweis: Der Agent verwendet standardmäßig den Port 17001, um eine sichere Übertragung an den CA Enterprise Log Manager-Erfassungsserver zu gewährleisten.

So verwenden Sie die Port-Eingabeaufforderung:

1. Wählen Sie "Abfragen und Berichte" aus.

   In der Abfrageliste werden der Ordner "Eingabeaufforderungen" und mindestens ein Ordner für weitere Abfragen angezeigt.

2. Erweitern Sie die Eingabeaufforderung, und wählen Sie "Port".

   Die Port-Eingabeaufforderung wird angezeigt.

3. Geben Sie die Portnummer ein, auf der diese Abfrage beruhen soll.

4. Wählen Sie die Felder aus, nach denen Daten abgefragt werden, die mit der von Ihnen eingegebenen Portnummer übereinstimmen.

   source_port

   Ist der Kommunikationsport zum Initiieren der Aktion.

   dest_port

   Ist der Kommunikationsport auf dem Zielhost, der das Ziel der Aktion ist.

   receiver_port

   Ist der Port, über den der Agent mit dem CA Enterprise Log Manager-Erfassungsserver kommuniziert.

5. Klicken Sie auf "Los".

   Es werden Ergebnisse für die Eingabeaufforderungsabfrage des Ports angezeigt.

6. Interpretieren Sie die Abfrageergebnisse mit Hilfe der folgenden Beschreibungen:

   CA-Schweregrad

   Gibt den Schweregrad des Ereignisses an. Zu den Werten in aufsteigender Reihenfolge nach Schweregrad zählen: "Informationen", "Warnung", "Geringfügige Auswirkung", "Schwerwiegende Auswirkung", "Kritisch" und "Schwerwiegend".

   Datum

   Gibt den Zeitpunkt an, zu dem das Ereignis aufgetreten ist.

Quell-IP

Gibt die IP-Adresse des Hosts an, von dem die Ereignisaktion initiiert wurde.

Ergebnis

Gibt einen Code für das Ereignisergebnis der entsprechenden Aktion an. Hierbei stehen "S" für "Erfolgreich" (Success), "F" für "Fehler" (Failure), "A" für "Accepted" (Akzeptiert), "D" für "Dropped" (Verworfen), "R" für "Rejected" (Zurückgewiesen) und "U" für "Unknown" (Unbekannt).

Quellport

Gibt den Port für ausgehende Daten an, über den die Aktion initiiert wird.

Zielport

Gibt den Port für eingehende Daten auf dem Zielhost an.

Empfängerhost

Gibt den Port für ausgehende Daten auf dem Agenten an, über den Ereignisprotokolle an den CA Enterprise Log Manager-Server gesendet werden.

Kategorie

Gibt die Kategorie der oberen Ebene der entsprechenden Ereignisaktion an. "Systemzugriff" ist beispielsweise die Kategorie für die Aktion "Authentifizierung".

Aktion

Gibt die Ereignisaktion an.

Protokollname

Gibt den vom Connector, der das Ereignis erfasst hat, verwendeten Protokollnamen an.

Verwenden der Benutzer-Eingabeaufforderung

Jedes Ereignis drückt Informationen über zwei Akteure aus: Quelle-Und Ziel.

- Sterben Sie als Quelle initiiert als Aktion sterben, als das Ereignis verursacht sterben.

  Beim Quellakteur kann es sich um einen Benutzer, "source_username", oder um einen Prozess, "source_processname", handeln.

- Das Ziel der Aktion ist der Akteur "dest".

  Beim Zielakteur kann es sich um einen Benutzer, "dest_username", oder um ein Objekt, "dest_objectname", handeln.

Über als Benutzer-Eingabeaufforderung sterben werden Ereignisse abgefragt, bei denen der von Ihnen angegebene Akteur in Höhlen-Ausgewählten CEG-Feldern des verfeinerten Ereignisses angezeigt wird. Betrachten Sie folgendes Szenario:

1. Der Quellakteur, "source_username"-Oder "source_processname", versucht, eine Aktion für-Höhle Zielakteur, "destination_username"-Oder "destination_objectname", durchzuführen.
2. Dieses-Ereignis-Wird in Einem-Repository ein der Ereignisquelle erfasst.
3. Ein CA Enterprise Log Manager-Agent legt eine Kopie des ein der Ereignisquelle erfassten Ereignisses ein und überträgt diese ein einen CA Enterprise Log Manager-Server.

So verwenden Sie sterben Benutzer-Eingabeaufforderung:

1. Wählen Sie "Abfragen-Und Berichte" aus.

   In der Abfrageliste werden der Ordner "Eingabeaufforderungen" und mindestens ein Ordner für weitere Abfragen angezeigt.

2. Blenden Sie Den Ordner-"Eingabeaufforderungen"-Ein, und wählen Sie-"Benutzer"-Aus.

   Sterben Sie als Benutzer-Eingabeaufforderung-Wird-Angezeigt aus.

3. Geben Sie Den Namen Des Benutzers-Ein, auf dem diese Abfrage basieren soll.

4. Wählen Sie als Felder aus sterben, sterben für als Sie-Daten-Abfragen-Möchten, als mit dem eingegebenen Benutzernamen übereinstimmen sterben.

   source_username

   Ist der Name des Benutzers, der als Ereignisaktion-Initiiert-Hut sterben.

   dest_username

   Ist der Name des Benutzers, der Ziel der Aktion ist.

   source_objectname

   Ist der Name des Objekts, das ein der in Höhle Ereignisinformationen angegebenen Aktion beteiligt ist.

   dest_objectname

   Ist der Name des Objekts, das Ziel der Aktion ist.

5. Klicken-Sie-Auf "Los".

   Es-Werden-Ergebnisse-Für sterben als Eingabeaufforderungsabfrage Des Benutzers-Angezeigt aus.

6. Interpretieren Sie als Abfrageergebnisse mit Hilfe der folgenden Beschreibungen sterben:

   CA-Schweregrad

   Gibt den Schweregrad des Ereignisses ein. Zu den Werten in aufsteigender Reihenfolge nach Schweregrad zählen: "Informationen", "Warnung", "Geringfügige Auswirkung","Schwerwiegende Auswirkung", "Kritisch"-Und "Schwerwiegend".

   Datum

   Gibt den Zeitpunkt ein, zu dem das Ereignis aufgetreten ist.

Zielhost

Gibt den Namen des Hosts mit dem Benutzer ein, der Ziel der Ereignisaktion-Krieg.

Ergebnis

Gibt-Einen-Code für das Ereignisergebnis der entsprechenden Aktion ein. Hierbei-Stehen-"S"-Für "Erfolgreich" (Erfolg), "F"-Für "Fehler" (Fehler), "ein" für "Akzeptierte" (Akzeptiert), "Gefallenes" "D"-Für (Verworfen), "R"-Für "Ablehnte" (Zurückgewiesen) Und-"U"-Für "Unbekannt" (Unbekannt).

Quellbenutzer

Gibt den Benutzer ein, der als Ereignisaktion-Initiiert-Hut sterben.

Quellobjekt

Gibt das Objekt auf dem Quellhost ein, das ein der Ereignisaktion beteiligt-Krieg.

Zielbenutzer

Gibt den Benutzer ein, der Ziel der Ereignisaktion-Krieg.

Zielobjekt

Gibt das Objekt auf dem Zielhost ein, das ein der Ereignisaktion beteiligt-Krieg.

Kategorie

Gibt als Kategorie der oberen Ebene der entsprechenden Ereignisaktion sterben ein. "Systemzugriff"-Ist-Beispielsweise als Kategorie für sterben als Aktion "Authentifizierung" sterben.

Aktion:

Gibt als Ereignisaktion sterben ein.

Protokollname

Gibt-Höhlen-Vom-Connector, der das Ereignis erfasst-Hut, verwendeten Protokollnamen ein.

So erstellen Sie Abfragen

Sie können benutzerdefinierte Abfragen erstellen, indem Sie den Assistenten für das Abfragedesign verwenden. Wenn Sie eine Abfrage erstellen, müssen Sie festlegen, ob die Abfrage auf die Ereignisdatenbank oder auf die Incident-Datenbank angewendet werden soll. Die Ereignisdatenbank eines Servers speichert Informationen für alle Ereignisse, die von diesem Server empfangen werden. Die Incident-Datenbank eines Servers speichert Informationen über Incidents und Elemente ihrer Komponentenereignisse, wie in den Korrelationsregeln angegeben.

Zudem können Sie benutzerdefinierte Abfragen löschen, Abfrageinformationen exportieren oder eine Software-Update-Abfrage kopieren, um so eine benutzerdefinierte Abfrage zu erstellen und diese dann mit dem Assistenten für Abfragedesign zu bearbeiten. Nur Benutzer, die als Administrator oder Analyst angemeldet sind, dürfen Abfragen erstellen, löschen oder bearbeiten.

Die Erstellung einer neuen Abfrage mit dem Assistenten für Berichtdesign umfasst folgende Schritte:

1. Öffnen des Assistenten für Abfragedesign.
2. Hinzufügen von Identitäts- und Kennungsdetails.
3. Auswahl der Abfragespalten.
4. (Optional) Einstellen von Abfragebedingungen und -filtern.
5. Einstellen von Datumsbereich und Ergebnisbedingungen.
6. (Optional) Auswahl der Visualisierungsoptionen für die Abfrageanzeige.
7. (Optional) Hinzufügen von Drilldown-Werten für die Abfrage.

Weitere Informationen:

Öffnen des Assistenten für das Abfragedesign (siehe Seite 328)
Verwenden erweiterter Filter (siehe Seite 528)
Visualisierung der Abfrageanzeige (siehe Seite 343)
Hinzufügen von Drilldown-Berichten (siehe Seite 344)

Öffnen des Assistenten für das Abfragedesign

Zum Erstellen einer neuen benutzerdefinierten Abfrage oder einer Kopie einer Abfrage oder zum Bearbeiten einer vorhandenen Abfrage öffnen Sie den Assistenten für das Abfragedesign.

So öffnen Sie den Assistenten für das Abfragedesign:

1. Klicken Sie auf die Registerkarte "Abfragen und Berichte" und dann auf die Unterregisterkarte "Abfragen".

   Die Seite "Abfrageliste" wird angezeigt.

2. Klicken Sie auf "Optionen", und wählen Sie "Neu" aus.

   Der Assistent für das Abfragedesign wird angezeigt.

   Beachten Sie bei Verwendung des Assistenten Folgendes:

   - Klicken Sie auf "Speichern", um die Abfrage zu speichern, ohne den Assistenten zu schließen.
   - Klicken Sie auf "Speichern und schließen", um die Abfrage zu speichern und den Assistenten zu schließen.
   - Klicken Sie auf "Zurücksetzen", um die Ansicht im Assistenten auf die zuletzt gespeicherten Einstellungen zurückzusetzen.

Weitere Informationen

Festlegen von Ergebnisbedingungen (siehe Seite 530)
Visualisierung der Abfrageanzeige (siehe Seite 343)
Hinzufügen von Drilldown-Berichten (siehe Seite 344)

Hinzufügen von Abfragedetails

Wenn Sie eine Abfrage erstellen, geben Sie zuerst die Informationen zur Kennzeichnung sowie sämtliche Kennungen ein, die berücksichtigt werden sollen.

So fügen Sie eine neue Abfrage hinzu:

1. Öffnen Sie den Assistenten für Abfragedesign.
2. Geben Sie einen Namen und wahlweise einen Kurznamen zur Verwendung in Berichten für die Abfrage ein. Der Kurzname wird im Abfragefenster des Berichts angezeigt, wenn die Abfrage in einen Bericht übernommen wird.
3. Wählen Sie die Datenbank aus, auf die Ihre Abfrage angewendet werden soll:

   Ereignis

   Wendet die Abfrage auf die Ereignisdatenbank an, die alle Rohereignisse und verfeinerten Ereignisse speichert, die durch den aktuellen Server empfangen werden oder über die Föderation verfügbar sind.

   Incident

   Wendet die Abfrage auf die Incident-Datenbank an, die durch das Ereigniskorrelationssystem erstellte Incidents und Ereignisinformationen, die zur Erstellung dieser Incidents verwendet werden, speichert. Die bestimmten Komponenten eines Ereignisses, die dazu verwendet werden einen Incident zu erstellen und deshalb in der Incident-Datenbank gespeichert werden, werden durch die Korrelationsregel festgelegt.
4. Im Feld "Beschreibung" können Sie etwaige zusätzliche Informationen eingeben.

   Hinweis: Es empfiehlt sich, in diesem Feld Informationen über die Struktur der Abfrage einzutragen. So könnten Sie beispielsweise erläutern, warum die Abfrage bestimmte Felder und Funktionen hat.
5. Wählen Sie mithilfe der Wechselsteuerung für Kennungen eine oder mehrere Kennungen für die Abfrage aus.
6. (Optional) Um eine benutzerdefinierte Kategoriekennung hinzuzufügen, geben Sie im Feld zum Hinzufügen einer benutzerdefinierten Kennung den Namen einer Kennung ein, und klicken Sie auf "Kennung hinzufügen".

   Die benutzerdefinierte Kennung wird in der Wechselsteuerung für Kennungen als bereits ausgewählt angezeigt.

7. (Optional) Um einen oder mehrere geschachtelte benutzerdefinierte Kennungen hinzuzufügen, wählen Sie eine Kennung aus, oder geben Sie den Namen der übergeordneten Kategorienkennung ein, gefolgt von einem umgekehrten Schrägstrich und dem Namen der untergeordneten Kennung. Klicken Sie anschließend auf "Kennung hinzufügen". Sie könnten beispielsweise Folgendes eingeben: "Regulations\Industry-Standards". Sie können zusätzliche Kennungen hinzufügen, indem Sie folgendes Format beibehalten: a\b\c usw.

   Hinweis: Wenn Sie eine der benutzerdefinierten geschachtelten Kennungen löschen, werden alle benutzerdefinierten Kennungen, in denen sie geschachtelt wurde, auch einschließlich der übergeordneten Kennung, gelöscht. Wenn Sie eine benutzerdefinierte Kennung in einer Software-Update-Kennung schachteln und sie dann löschen, werden nur die benutzerdefinierten Kennungen gelöscht.

   Wenn Sie den Vorgang abschließen, werden die neuen Kennungen in der Liste angezeigt. Wenn Sie die übergeordnete Kennung einblenden, sind die geschachtelten benutzerdefinierten Kennungen sichtbar.

8. Klicken Sie auf den entsprechenden Pfeil, um zu dem Schritt im Abfragedesign zu gelangen, den Sie als nächsten durchführen möchten, oder klicken Sie auf "Speichern und schließen".

   Bei Auswahl von "Speichern und schließen" wird die neue Abfrage in der Abfrageliste angezeigt. Andernfalls fahren Sie mit dem gewünschten Schritt fort.

Hinzufügen von Abfragespalten

Abfragen werden erstellt, indem Sie eine SQL-Anweisung schreiben, mit der die gewünschten Ereignisinformationen aus dem Ereignisprotokollspeicher abgerufen werden. Mit dem Assistenten für Abfragedesign erfolgt das nahezu automatisch.

So erstellen Sie eine SQL-Anweisung für Abfragen:

1. Öffnen Sie den Assistenten für Abfragedesign.
2. Geben Sie, wenn nicht bereits eingetragen, Namen und Kennung ein, und fahren Sie mit dem Schritt zur Bearbeitung der Abfragespalten fort.
3. (Optional) Aktivieren Sie das Kontrollkästchen "Nur eindeutige Ereignisse".

4. Wählen Sie die CEG-Spalten aus, die Sie in die Abfrage aufnehmen möchten, indem Sie sie aus der Liste der verfügbaren Spalten auf der linken Seite in den Fensterbereich "Ausgewählte Spalten" ziehen. In der Abfrageanzeige werden die Spalten in der Reihenfolge angezeigt, in der sie hinzugefügt wurden.
5. (Optional) Wählen Sie die gewünschten Einstellungen für jede Spalte aus. Dazu gehören:

   Anzeigename

   Hiermit kann der Spaltenname geändert werden, der in einer Tabelle oder der Ereignisanzeige angezeigt wird. Wird kein Anzeigename angegeben, wird der systemeigene Feldname als Spaltenname verwendet. Ein Beispiel wäre "event_count".

   Funktion

   Damit können Sie eine der folgenden SQL-Funktionen auf die Spaltenwerte anwenden:

   - COUNT: gibt die Gesamtzahl der Ereignisse zurück.
   - AVG: gibt den Durchschnitt der Werte für "event_count" zurück. Diese Funktion ist nur für die Felder "event_count" verfügbar.
   - SUM: gibt die Summe der Werte für "event_count" zurück. Diese Funktion ist nur für die Felder "event_count" verfügbar.
   - TRIM: entfernt Leerzeichen im Abfragetext.
   - TOLOWER: wandelt den Abfragetext in Kleinbuchstaben um.
   - TOUPPER: wandelt den Abfragetext in Großbuchstaben um.
   - MIN: gibt den niedrigsten Ereigniswert zurück.
   - MAX: gibt den höchsten Ereigniswert zurück.
   - UNIQUECOUNT: gibt die Anzahl der eindeutigen Ereignisse zurück.

   Gruppenreihenfolge

   Legt fest, dass die ausgewählten Spalten in der Abfrageanzeige nach dem ausgewählten Attribut gruppiert angezeigt werden. Sie können beispielsweise die Abfrage so einstellen, dass Ereignisse nach Quellnamen gruppiert werden. Sie können die Reihenfolge bestimmen, in der diese Einstellung auf die verschiedenen Spalten angewendet wird. Sind die Werte der ersten Spalte identisch, werden die der zweiten verwendet. So können Sie beispielsweise mehrere Ereignisse aus derselben Quelle nach dem Benutzernamen gruppieren.

Sortierreihenfolge

Bestimmt die Reihenfolge, in der ausgewählte Werte sortiert werden. Sie können die Reihenfolge bestimmen, in der diese Einstellung auf die verschiedenen Spalten angewendet wird. Sind die Werte der ersten Spalte identisch, werden die der zweiten verwendet.

Absteigend

Legt fest, dass Spaltenwerte in absteigender Reihenfolge (vom höchsten zum niedrigsten Wert) und nicht standardmäßig in aufsteigender Reihenfolge angezeigt werden.

Nicht Null

Legt fest, ob die angezeigte Zeile, wenn sie keine Werte enthält, in einer Tabelle oder Ereignisanzeige erscheint. Mit dem Kontrollkästchen "Not Null" wird die Zeile, wenn sie keine Werte enthält, aus den Abfrageergebnissen gelöscht.

Sichtbar

Bestimmt, ob die Spalte in einer Tabelle oder Ereignisanzeige erscheint. Mit dieser Einstellung können Sie Spaltendaten in der Detailansicht zur Verfügung stellen, die nicht in der Abfrageanzeige erscheinen.

Hinweis: Wenn Sie für eine Spalte eine andere Funktion als TRIM, TOLOWER, TOUPPER oder eine Einstellung zur Gruppenreihenfolge auswählen, müssen Sie für die restlichen Spalten dieselbe Einstellung vornehmen. Andernfalls wird in CA Enterprise Log Manager eine Fehlermeldung angezeigt.

6. (Optional) Ändern Sie die Spaltenreihenfolge bei Bedarf mit dem nach oben oder unten zeigenden Pfeil oben im Fensterbereich "Ausgewählte Spalten".
7. Klicken Sie auf den entsprechenden Pfeil, um zu dem Schritt im Abfragedesign zu gelangen, den Sie als nächsten durchführen möchten, oder klicken Sie auf "Speichern und schließen".

   Bei Auswahl von "Speichern und schließen" wird die neue Abfrage in der Abfrageliste angezeigt. Andernfalls fahren Sie mit dem gewünschten Schritt fort.

Festlegen von Abfragefiltern

Die anhand der Abfragen erzielten Ergebnisse können mit Hilfe einfacher oder erweiterter Filter gefiltert werden. Mit einfachen Filtern können Sie rasch Filteranweisungen mit nur einem Begriff erstellen. Mit erweiterten Filtern lassen sich komplexe SQL-Anweisungen einschließlich geschachtelter Anweisungen erstellen.

So legen Sie einen Abfragefilter fest:

1. Öffnen Sie den Assistenten für Abfragedesign.
2. Geben Sie, wenn nicht bereits eingetragen, Namen und Kennung ein, und fahren Sie mit dem Schritt für Abfragefilter fort.

   Das Dialogfeld "Abfragefilter" wird mit der Registerkarte "Einfache Filter" im Vordergrund angezeigt.
3. Sie können beliebige einfache Filter erstellen, um nach angegebenen CEG-Feldwerten zu suchen.
4. (Optional) Klicken Sie auf die Registerkarte "Erweiterte Filter".
5. (Optional) Erstellen Sie beliebige erweiterte Filter.
6. Klicken Sie auf den entsprechenden Pfeil, um zu dem Schritt im Abfragedesign zu gelangen, den Sie als Nächsten durchführen möchten, oder klicken Sie auf "Speichern und schließen".

   Bei Auswahl von "Speichern und schließen" wird die neue Abfrage in der Abfrageliste angezeigt. Andernfalls wird der von Ihnen ausgewählte Abfrageschritt eingeblendet.

Weitere Informationen

Erstellen eines einfachen Ereignisfilters (siehe Seite 618)
Erstellen erweiterter Ereignisfilter (siehe Seite 621)
Verwenden erweiterter Filter (siehe Seite 528)

Erstellen eines einfachen Ereignisfilters

Sie können einfache Filter erstellen, um Suchparameter für allgemeine Werte festzulegen. So können Sie zum Beispiel für das Feld "Idealmodell" die Option "Content Management" einstellen, um alle Ereignisse mit diesem Wert im CEG-Feld "Idealmodell" zu identifizieren. Einfache Filter werden von zahlreichen Funktionen eingesetzt, zum Beispiel von Ereignissen und Incident-Abfragen, Unterdrückungs- und Zusammenfassungsregeln sowie Ereignisweiterleitungsregeln.

So erstellen Sie einen einfachen Filter:

1. Aktivieren Sie das Kontrollkästchen für ein beliebiges einfaches Filterfeld oder Felder, die Sie definieren möchten, und wählen Sie einen Wert aus der Drop-down-Liste aus bzw. geben Sie den gewünschten Wert in das Texteingabefeld ein.
2. Sobald Sie alle gewünschten einfachen Filter hinzugefügt haben, klicken Sie auf "Speichern".

Weitere Informationen

Verwenden erweiterter Filter (siehe Seite 528)
Erstellen erweiterter Ereignisfilter (siehe Seite 621)

Verwenden erweiterter Filter

Mithilfe erweiterter SQL-basierter Filter lassen sich die Funktionen zur Abfrage der Ereignis- oder Incident-Datenbanken genauer definieren. Dazu gehören beispielsweise das Eingrenzen von Abfragen oder das Hinzufügen von Zusatzqualifikationen zu einfachen Filtern. Die Schnittstelle "Erweiterte Filter" beinhaltet ein Formular, in das Sie Logik, Spalten, Operatoren und Werte eintragen können, um die Filter in der richtigen Syntax zu erstellen.

Hinweis: Dieser Abschnitt enthält einen kurzen Überblick über die in den erweiterten Filtern verwendeten SQL-Begriffe. Um alle Möglichkeiten erweiterter Filter zu nutzen, sollten Sie mit SQL und der ELM-Schemadefinition vertraut sein.

Die folgenden SQL-Begriffe dienen zur Verknüpfung mehrerer Filteranweisungen:

And

Ereignisinformationen werden angezeigt, falls *alle* verbundenen Bedingungen zutreffen.

Oder:

Ereignisinformationen werden angezeigt, falls *eine* der verbundenen Bedingungen zutrifft.

Having

Zur Verfeinerung der Begriffe der SQL-Hauptanweisung, indem eine qualifizierende Anweisung hinzugefügt wird. Beispielsweise könnten Sie einen erweiterten Filter für Ereignisse bestimmter Hosts einrichten und durch Hinzufügen einer Having-Anweisung dafür sorgen, dass nur Ereignisse mit einem bestimmten Schweregrad von diesen Hosts zurückgegeben werden.

Folgende SQL-Operatoren werden von erweiterten Filtern für die grundlegenden Bedingungen verwendet:

Vergleichsoperatoren

Es werden die Ereignisinformationen aufgenommen, deren Spaltenwert dem entsprechenden Vergleich mit dem von Ihnen eingegebenen Wert standhält. Die folgenden Vergleichsoperatoren stehen zur Verfügung:

- Gleich
- Ungleich
- Kleiner als
- Größer als
- Kleiner oder gleich
- Größer oder gleich

Wenn Sie beispielsweise *Größer als* verwenden, werden die Ereignisinformationen aus Ihrer gewählten Spalte übernommen, falls deren Wert größer als der von Ihnen angegebene Wert ist.

Wie

Berücksichtigt die Ereignisinformationen, wenn die Spalte das von Ihnen angegebene Muster enthält. Verwenden Sie "%" für die Definition des Musters. Beispielsweise würde "L%" jeden Wert zurückgeben, der mit einem L beginnt und "%L%" alle Werte, die ein L enthalten, das jedoch weder an erster noch an letzter Stelle stehen darf.

Nicht wie

Berücksichtigt die Ereignisinformationen, falls der Spaltenwert nicht dem angegebenen Muster entspricht.

Enthalten

Berücksichtigt die Ereignisinformationen, wenn die Spalte einen oder mehrere der Werte enthält, die Sie durch Anführungszeichen getrennt eingegeben haben. Mehrere Werte in der Gruppe müssen mit einem Komma getrennt werden.

Nicht enthalten

Berücksichtigt die Ereignisinformationen, wenn die Spalte keinen der Werte enthält, die Sie durch Anführungszeichen getrennt eingegeben haben. Mehrere Werte in der Gruppe müssen mit einem Komma getrennt werden.

Übereinstimmend

Schließt alle Ereignisinformationen ein, die mit einem oder mehreren der von Ihnen eingegebenen Zeichen übereinstimmen, so dass Sie nach Schlüsselwörtern suchen können.

Mit Schlüssel

Schließt alle Ereignisinformationen ein, die beim Konfigurieren des Berichtsservers als Schlüsselwerte festgelegt wurden. Sie können Schlüsselwerte verwenden, um die Unternehmensrelevanz oder andere organisatorische Gruppen festzulegen.

Ohne Schlüssel

Schließt alle Ereignisinformationen ein, die beim Konfigurieren des Berichtsservers nicht als Schlüsselwerte festgelegt wurden. Sie können Schlüsselwerte verwenden, um die Unternehmensrelevanz oder andere organisatorische Gruppen festzulegen.

Erstellen erweiterter Ereignisfilter

Erweiterte Filter werden vielfach verwendet. So beispielsweise beim Erstellen von Abfragen, der Planung von Berichten, Alarmjobs sowie im Zusammenhang mit lokalen und globalen Filtern.

So erstellen Sie einen erweiterten Ereignisfilter:

1. Wenn Sie einen geplanten Berichtsjob oder einen Aktionsalarmjob erstellen, klicken Sie auf die Registerkarte "Ereignisse" oder "Incidents", um den entsprechenden Filtertyp festzulegen. Da ein Berichts- oder Alarmjob sowohl Ereignisabfragen als auch Incident-Abfragen enthalten kann, können Sie die Filtertypen separat festlegen.
2. Klicken Sie auf "Neuer Ereignisfilter".

   Die erste Zeile der Ereignisfiltertabelle wird aktiviert. Dabei werden die Spalten "Logik" und "Operator" jeweils mit den Standardwerten "And" und "Gleich" ausgefüllt.
3. Klicken Sie bei Bedarf auf die Zelle "Logik", und ändern Sie den Wert.
4. Klicken Sie auf die Zelle "Spalte", und wählen Sie im Drop-down-Menü die Spalte mit den gewünschten Ereignisinformationen aus.
5. Klicken Sie auf die Zelle "Operator", und wählen Sie im Drop-down-Menü den gewünschten Operator aus.
6. Klicken Sie auf die Zelle" Wert", und geben Sie einen Wert ein.
7. (Optional) Klicken Sie auf die Zellen für die öffnenden und schließenden Klammern, und geben Sie die Zahl der benötigten Klammern ein.
8. (Optional) Wenn Sie weitere Filteranweisungen definieren möchten, wiederholen Sie die Schritte 1 bis 6.
9. Wenn Sie alle gewünschten Filteranweisungen eingegeben haben, klicken Sie auf "Speichern".

Weitere Informationen:

Erstellen eines einfachen Ereignisfilters (siehe Seite 618)
Verwenden erweiterter Filter (siehe Seite 528)

Festlegen von Ergebnisbedingungen

Sie können für die Abfrage einen Datumsbereich und andere Ergebnisbedingungen festlegen, wie die Begrenzung der Zeilen oder einen Basisanzeigezeitraum. Ergebnisbedingungen können bis zur Ausführung der Abfrage jederzeit geändert werden. Mit ihnen lassen sich Abfragen ändern, ohne dass die Abfrage an sich oder die zugehörigen Filter geändert werden müssen.

Wenn Sie einen geplanten Berichtsjob oder Aktionsalarmjob erstellen, können Sie nach Bedarf Ergebnisbedingungen sowohl für Ereignisabfragen als auch Incident-Abfragen festlegen, aus denen der Job besteht.

Folgende Typen von Ergebnisbedingungen stehen zur Auswahl:

- Bedingungen für den Datumsbereich zur Bestimmung des Abfragezeitraums
- Anzeigebedingungen (beispielsweise maximale Zeilenanzahl)
- Ergebnisbedingungen für gruppierte Ereignisse, wie z. B. die jüngsten gruppierten Ereignisse nach einem bestimmten Datum oder gruppierte Ereignisse mit einer bestimmten Anzahl an Ereignissen.

  Hinweis: Damit Benutzer die Ergebnisbedingungen in der Abfrageanzeige bearbeiten können, muss beim Erstellen einer Abfrage mindestens eine Spalte gruppiert werden.

Festlegen von Zeit- oder Datumsbereichen

Sie können Ihrer Abfrage eine Bedingung für den Zeit- oder Datumsbereich hinzufügen. Dies verbessert die Abfrageeffizienz, da die zu durchsuchende Datenmenge im Ereignisprotokollspeicher eingegrenzt wird.

Sie können einen vordefinierten Zeitraum verwenden oder einen benutzerdefinierten Zeitraum erstellen. Damit ein benutzerdefinierter Zeitraum ordnungsgemäß funktioniert, müssen Sie sowohl eine Anfangs- als auch eine Endzeit angeben. Wenn Sie nur einen einzelnen Zeitparameter festlegen, wird dieser in der SQL-Abfrage als Where-Klausel wiedergegeben.

So legen Sie Ergebnisbedingungen fest:

1. Öffnen Sie das Dialogfeld "Ergebnisbedingungen".
2. Wenn Sie einen geplanten Berichtsjob oder einen Aktionsalarmjob erstellen, klicken Sie auf die Registerkarte "Ereignisse" oder "Incidents", um den entsprechenden Filtertyp festzulegen. Da ein Berichts- oder Alarmjob sowohl Ereignisabfragen als auch Incident-Abfragen enthalten kann, können Sie die Filtertypen separat festlegen.
3. Wählen Sie einen vordefinierten Zeitraum aus der Drop-down-Liste aus. Wenn Sie zum Beispiel die am Vortag eingegangenen Ereignisse anzeigen möchten, wählen Sie "Vorheriger Tag" aus.

   Hinweis: Wenn Sie einen Aktionsalarm oder geplanten Bericht erstellen, gibt die Schnittstelle die folgenden Standardzeitbereiche vor:

   - Aktionsalarm: vorherige 5 Minuten
   - Geplanter Bericht: vorherige 6 Stunden
4. (Optional) Mit den folgenden Zwischenschritten können Sie einen benutzerdefinierten Zeitraum erstellen:

   a. Klicken Sie im Bereich "Auswahl des Datumsbereichs" neben dem Wert für "Dynamische Endzeit" auf "Bearbeiten". Damit können Sie das Ende des Zeitraums festlegen, für den die Abfrage erfolgen soll.

      Das Dialogfeld "Dynamische Zeitangabe" wird angezeigt.

   b. Wählen Sie die Referenzzeit aus, auf der der Parameter basieren soll, und klicken Sie auf "Hinzufügen".

   c. Wählen Sie den gewünschten Zeitparameter aus, und klicken Sie auf "Hinzufügen". Sie können mehrere Zeitparameter hinzufügen.

   d. Sobald Sie alle Parameter hinzugefügt haben, klicken Sie auf "OK".

Das Dialogfeld "Dynamische Zeitangabe" wird geschlossen, und die von Ihnen ausgewählten Werte werden im Bereich "Dynamische Endzeit" angezeigt. Bei Verwendung mehrerer Parameter ergeben diese eine vollständige Zeitangabe, bei der jeder Parameter auf den ersten verweist. Wenn Sie zum Beispiel im Bereich "Dynamische Endzeit" die Werte "Anfang des Monats" und "Wochentag – Dienstag" hinzufügen, endet Ihre Abfrage am ersten Dienstag des Monats.

Hinweis: Bei den "Anzahl"-Werten, z. B. "Anzahl der Tage" oder "Anzahl der Stunden" müssen Sie zur Einstellung eines vergangenen Zeitraums eine *negative* Zahl eingeben. Mit der Eingabe einer positiven Zahl stellen Sie eine zukünftige Endzeit ein, und die Abfrage liefert weiterhin Ergebnisse, solange sich mindestens ein qualifiziertes Ereignis im Protokollspeicher befindet.

Wenn Sie beispielsweise im Bereich "Dynamische Startzeit" die Werte "Jetzt" und "Anzahl der Minuten – 10" hinzufügen, beginnt Ihre Abfrage 10 Minuten vor der ausgewählten Endzeit.

e. Wiederholen Sie Schritt 2 im Bereich "Dynamische Startzeit", um den Beginn des Zeitraums festzulegen, für den die Abfrage erfolgen soll.

Wenn Sie keinen Datumsbereich eingeben, wird die Abfrage auf alle Ereignisse im Protokollspeicher angewandt. Wenn Sie einen ungültigen Datumsbereich eingeben, gibt Ihre Abfrage möglicherweise keine Ergebnisse zurück.

5. Klicken Sie auf den entsprechenden Pfeil, um zu dem Schritt im Abfragedesign zu gelangen, den Sie als nächsten durchführen möchten, oder klicken Sie auf "Speichern und schließen".

   Wenn Sie auf "Speichern und schließen" klicken, wird die neue Abfrage in der Abfrageliste angezeigt. Anderenfalls wird der von Ihnen ausgewählte Abfragedesignschritt angezeigt.

Weitere Informationen:

Festlegen von Ergebnisbedingungen (siehe Seite 530)
Festlegen von Anzeige- und Gruppenbedingungen (siehe Seite 533)

Festlegen von Anzeige- und Gruppenbedingungen

Sie können Bedingungen festlegen, mit denen Sie einerseits die Ansicht der Abfrageanzeige einrichten und andererseits nach Ereignissen auf Basis ihres Gruppierungstyps suchen können.

So legen Sie Anzeige- und Gruppenbedingungen fest

1. Öffnen Sie das Dialogfeld "Ergebnisbedingungen".
2. Wenn Sie einen geplanten Berichtsjob oder einen Aktionsalarmjob erstellen, klicken Sie auf die Registerkarte "Ereignisse" oder "Incidents", um den entsprechenden Filtertyp festzulegen. Da ein Berichts- oder Alarmjob sowohl Ereignisabfragen als auch Incident-Abfragen enthalten kann, können Sie die Filtertypen separat festlegen.
3. Mit den Kontrollkästchen unter "Ergebnisse" können Sie beliebige der folgenden Anzeigebedingungen aktivieren.

   Standardabfragebeschränkung

   Dieser Wert ist nur für Aktionsalarme und die Berichtsplanung verfügbar. Damit wird für die Warnung oder den Berichtsjob festgelegt, dass die Zeilenbegrenzung individueller Abfragen im Job verwendet werden soll. Wenn Sie bei der Joberstellung andere Ergebniswerte auswählen, überschreibt CA Enterprise Log Manager die Zeilenbegrenzung in den Komponenten-Abfragen.

   Zeilenbegrenzung

   Legt die maximale Anzahl von Ereigniszeilen fest, die in der Abfrage angezeigt werden. Dabei stehen die neuesten Ereignisse am Anfang der Liste.

   Keine Beschränkung

   Legt fest, dass in der Abfrage alle Ereignisse abgerufen werden sollen, die dem entsprechenden Filter entsprechen. Da diese Abfrage eine Vielzahl von Ereignissen umfassen kann, sollten Sie die Abfrage dementsprechend planen.

   Andere anzeigen

Weist auf das Vorhandensein weiterer Ergebnisse hin, die aufgrund der Zeilenbegrenzung nicht angezeigt werden. Dies ermöglicht es Ihnen, die ausgewählten Ereignisse vor dem Hintergrund aller Ereignisse dieses Typs zu vergleichen. Wenn Sie zum Beispiel für Ihre Ereignisanzeige als Zeilenbegrenzung den Wert 10 angeben und "Andere anzeigen" aktivieren, werden alle über den Wert 10 hinausgehenden Ereignisse zu einem Eintrag mit der Bezeichnung "Andere" zusammengefasst, der alle übrigen Ereignisse anzeigt. Diese Einstellung ist nur wirksam, wenn eine Zeilenbegrenzung ausgewählt wurde.

Zeitgranularität

Legt den Detailgrad des in der Abfrageanzeige verwendeten Zeitraumfeldes fest.

4. Mit "Ergebnisbedingungen" können Sie für die Abfrage Bedingungen angeben, mit denen Ereignisse nach ihrem Gruppierungstyp gesucht werden. Beispielsweise könnten Sie Ihre Abfrage so einrichten, dass das neueste gruppierte Ereignis nach einem ausgewählten Datum oder eine bestimmte Anzahl von gruppierten Ereignissen gesucht wird. Ein gruppiertes Ereignis ist ein verfeinertes Ereignis, für das Sie im Abfrageerstellungsschritt eine Funktion und eine Gruppenreihenfolge festgelegt haben.

   Die Gruppenbedingungen basieren auf demselben Zeitangabesystem wie bei den Feldern für den Zeitbereich.

5. Klicken Sie auf den entsprechenden Pfeil, um zu dem Schritt im Abfragedesign zu gelangen, den Sie als nächsten durchführen möchten, oder klicken Sie auf "Speichern und schließen".

   Wenn Sie auf "Speichern und schließen" klicken, wird die neue Abfrage in der Abfrageliste angezeigt. Anderenfalls wird der von Ihnen ausgewählte Abfragedesignschritt angezeigt.

Weitere Informationen:

Festlegen von Ergebnisbedingungen (siehe Seite 530)

Visualisierung der Abfrageanzeige

Um eine neue Abfrageanzeige zu erstellen, legen Sie fest, wie die Ereignisinformationen angezeigt werden sollen.

So visualisieren Sie die Abfrageanzeige:

1. Öffnen Sie den Assistenten für Abfragedesign.
2. Geben Sie, wenn nicht bereits eingetragen, Namen und Kennung ein, und fahren Sie mit dem Schritt zur Visualisierung fort.
3. Bestimmen Sie, ob für die Abfrageanzeige die Ereignisanzeige oder ein Diagramm verwendet werden soll.

   Wenn Sie sich für die Ereignisanzeige entscheiden, ist die Visualisierung jetzt beendet. Die Ereignisspalten werden in der Ereignisanzeige in der Reihenfolge angezeigt, in der Sie sie bei der Zusammenstellung der Abfragespalten platziert haben.
4. Wenn Sie sich für ein Diagramm entscheiden, stehen ein oder mehrere Diagrammtypen zur Auswahl. Die Auswahl mehrerer Diagrammtypen ermöglicht den Benutzern, in der Berichtsanzeige zwischen den verschiedenen Diagrammen hin- und herzuschalten. Mit den Pfeilschaltflächen neben den einzelnen Typen können Sie die Reihenfolge festlegen, in der dieTypen im Menü "Visualisierung ändern" aufgeführt werden.

   Hinweis: Die Anzeigeform "Tabelle" ist stets vorhanden und muss nicht extra hinzugefügt werden.
5. Wählen Sie aus dem Dropdown-Menü für die Spalten das Ereignis aus, das als X-Achse erscheinen soll, geben Sie die Bezeichnung ein, die angezeigt werden soll, und wählen Sie im Menü für den Anzeigetyp eine der folgenden Optionen aus:

   - Kategorie: Verwenden Sie diese Option für Spalten mit Zeichenfolgen- oder Textwerten wie "source_username".
   - Linear: Verwenden Sie diese Option für numerische Werte wie "event_count". Wenn die Werte verstreut sind, können Sie die Achse mit dem Kontrollkästchen "Logarithmische Skala" in eine logarithmische Skala umwandeln.
   - Datum/Uhrzeit: Verwenden Sie diese Option, um Zeitangaben entsprechend dem jeweiligen Datums- und Uhrzeitformat anzugeben.
6. Wiederholen Sie Schritt 4 mit den Menüs für die Einstellungen der Y-Achse, und stellen Sie die Spalte, die Bezeichnung sowie die Typoptionen für die Y-Achse (vertikal) ein.

7. Klicken Sie auf den Pfeil, der Sie zu dem Schritt im Assistenten für Abfragedesign führt, mit dem Sie fortfahren möchten, oder klicken Sie auf "Speichern und schließen".

   Bei Auswahl von "Speichern und schließen" wird die neue Abfrage in der Abfrageliste angezeigt. Andernfalls fahren Sie mit dem gewünschten Schritt fort.

Hinzufügen von Drilldown-Berichten

Abfragen können mit einem oder mehreren Drilldown-Berichten ergänzt werden. Mit Drilldown-Berichten können Benutzer auf ein Element in einer Abfrageanzeige klicken und einen anderen zugehörigen Bericht öffnen.

So fügen Sie einen Drilldown-Bericht hinzu:

1. Öffnen Sie den Assistenten für Abfragedesign.
2. Geben Sie, wenn nicht bereits eingetragen, Namen und Kennung ein, und fahren Sie mit dem Schritt für Drilldown-Berichte fort.
3. Klicken Sie auf "Drilldown hinzufügen".
4. Geben Sie den Namen ein, oder suchen Sie nach dem Bericht, den Sie als Drilldown-Bericht zur Verfügung stellen möchten.
5. Wählen Sie mindestens einen verfügbaren Parameter aus, auf den sich der Drilldown-Bericht beziehen soll, und verschieben Sie den Parameter in die Liste der ausgewählten Parameter. Mit Hilfe der ausgewählten Parameter wird sichergestellt, dass der Abfrageschwerpunkt in den Drilldown-Berichten berücksichtigt wird.
6. Klicken Sie auf den Pfeil, der Sie zu dem Schritt im Assistenten für Abfragedesign führt, mit dem Sie fortfahren möchten, oder klicken Sie auf "Speichern und schließen".

   Bei Auswahl von "Speichern und schließen" wird die neue Abfrage in der Abfrageliste angezeigt. Andernfalls fahren Sie mit dem gewünschten Schritt fort.

Bearbeiten von Abfragen

Sie können vorhandene benutzerdefinierte Abfragen bearbeiten. Abonnementabfragen dagegen können nicht bearbeitet werden. Sie können sie aber kopieren und dann die Kopie bearbeiten. Bei der Bearbeitung von Abfragen wirken sich die Änderungen, die Sie vornehmen, auf alle Berichte aus, für die diese Abfrage herangezogen wird.

So bearbeiten Sie eine Abfrage:

1. Klicken Sie auf die Registerkarte "Abfragen und Berichte" und auf die Unterregisterkarte "Abfragen".

   Die Liste der Abfragekennungsfilter und die Liste der Abfragen werden angezeigt.

2. Erweitern Sie in der Abfrageliste den Benutzerordner, und wählen Sie die Abfrage aus, die Sie bearbeiten möchten.

3. Klicken Sie oben in der Liste auf "Optionen" und dann auf "Bearbeiten".

   Der Assistent für Abfragedesign wird geöffnet. Die Details der ausgewählten Abfrage sind bereits in den Feldern eingetragen.

4. Nehmen Sie die gewünschten Änderungen vor, und klicken Sie auf "Speichern".

Löschen benutzerdefinierter Abfragen

Benutzerdefinierte Abfragen können gelöscht werden. Abonnementabfragen dagegen nicht.

So löschen Sie eine Abfrage:

1. Wählen Sie die Abfrage aus, die Sie löschen möchten.

2. Klicken Sie oben in der Liste auf "Optionen", und wählen Sie anschließend "Löschen" aus.

   Ein Bestätigungsdialogfeld wird angezeigt.

3. Klicken Sie auf "Ja".

   Die gelöschte Abfrage wird aus der Liste der Abfragen entfernt.

Weitere Informationen

Deaktivieren der Anzeige einer ausgewählten Abfrage (siehe Seite 346)
Bearbeiten von Abfragen (siehe Seite 345)
Exportieren und Importieren von Abfragedefinitionen (siehe Seite 346)

Deaktivieren der Anzeige einer ausgewählten Abfrage

Sie können Ihre Abfrageliste so festlegen, dass Sie Änderungen durchführen können, ohne Abfragen zu laden. Normalerweise wird eine Abfrage im Detailfenster angezeigt, wenn Sie sie in der Liste auswählen.

Wenn Sie diese Standardeinstellung deaktivieren, sparen Sie Zeit, da Sie eine Abfrage aus der Liste auswählen und sofort bearbeiten können, ohne warten zu müssen, bis sie angezeigt wird. Dies ist besonders hilfreich, wenn Sie mehrere Abfragen bearbeiten müssen und bereits wissen, welche Änderungen Sie vornehmen möchten.

Hinweis: Da nur Benutzer mit der Rolle "Administrator" oder "Analyst" Abfragen erstellen oder bearbeiten können, können nur diese Benutzer die Einstellung zum Anzeigen einer ausgewählten Abfrage deaktivieren.

So deaktivieren Sie die Anzeige einer ausgewählten Abfrage:

1. Klicken Sie oben in der Abfrageliste auf "Optionen".

   Das Menü "Optionen" wird angezeigt.

2. Deaktivieren Sie die Option "Ausgewählte Abfrage anzeigen".

   Abfragen, die aus dieser Liste ausgewählt werden, werden erst wieder angezeigt, wenn die Option "Ausgewählte Abfrage anzeigen" wieder aktiviert wird.

Exportieren und Importieren von Abfragedefinitionen

Sie können Details der benutzerdefinierten Abfragen exportieren und importieren, um sie in anderen Management-Servern zu verwenden. Hierdurch können Sie erfolgreiche benutzerdefinierte Abfragen zwischen CA Enterprise Log Manager-Umgebungen oder aus einer Testumgebung in eine Produktionsumgebung übertragen.

Weitere Informationen

Importieren von Abfragedefinitionen (siehe Seite 348)
Exportieren von Abfragedefinitionen (siehe Seite 347)

Exportieren von Abfragedefinitionen

Sie können die Details der benutzererstellten Abfragen für die Verwendung in anderen Management-Servern exportieren. Die exportierten Daten werden als XML-Datei gespeichert.

So exportieren Sie Abfragedetails:

1. Klicken Sie auf die Registerkarte "Abfragen und Berichte" und dann auf die Unterregisterkarte "Abfragen".

   Die Seite "Abfrageliste" wird angezeigt.

2. Klicken Sie oben in der Liste auf "Optionen", und wählen Sie "Exportieren" aus.

   Das Dialogfeld "Benutzereigene Abfragedefinitionen exportieren" wird geöffnet, in dem die verfügbaren, vom Benutzer erstellten Berichte angezeigt werden.

3. Wählen Sie die Abfrage(n) aus, die Sie mit Hilfe der Wechselsteuerung exportieren möchten, und klicken Sie auf "Exportieren".

   Das Dialogfeld "Exportieren" wird angezeigt.

4. Geben Sie den Speicherort für die XML-Exportdateien an, oder suchen Sie danach, und klicken Sie auf "Speichern".

   Die Abfragedateien werden am gewählten Speicherort gespeichert, und ein Bestätigungsdialogfeld wird angezeigt.

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

   Das Dialogfeld "Benutzereigene Abfragedefinitionen exportieren" wird geschlossen.

Weitere Informationen

Exportieren und Importieren von Abfragedefinitionen (siehe Seite 346)
Importieren von Abfragedefinitionen (siehe Seite 348)

Importieren von Abfragedefinitionen

Sie können XML-Dateien mit Abfragedefinitionen zur Verwendung im lokalen Management-Server importieren.

So importieren Sie Berichtdetails:

1. Klicken Sie auf die Registerkarte "Abfragen und Berichte" und dann auf die Unterregisterkarte "Abfragen".

   Die Seite "Abfrageliste" wird angezeigt.

2. Klicken Sie oben in der Liste auf "Optionen", und wählen Sie "Importieren" aus.

   Das Dialogfeld "Datei importieren" wird geöffnet.

3. Geben Sie den Speicherort für die Dateien an, die Sie importieren möchten, oder suchen Sie danach, und klicken Sie auf "OK".

   Das Fenster "Importergebnisse" wird angezeigt.

4. Klicken Sie auf "Andere Datei importieren", um Schritt 3 zu wiederholen, oder klicken Sie auf "Schließen".

   Das Fenster "Importergebnisse" wird geschlossen.

Weitere Informationen

Exportieren und Importieren von Abfragedefinitionen (siehe Seite 346)
Exportieren von Abfragedefinitionen (siehe Seite 347)

Generieren von Berichten

Sie können benutzerdefinierte Berichte für Ihre Umgebung generieren. Erstellen Sie dazu entweder anhand der in diesem Abschnitt genannten Schritte einen neuen Bericht, oder verwenden Sie eine der Berichtsvorlagen. Benutzerdefinierte Berichte lassen sich anzeigen oder als Vorlagen für geplante Berichte auswählen.

Außerdem können Sie einen benutzerdefinierten Bericht bearbeiten, löschen und die Informationen daraus exportieren. Benutzerdefinierte Berichte können nur von Benutzern verwendet werden, die als Administrator oder Analyst angemeldet sind.

Die Erstellung eines neuen Berichts mit dem Assistenten für das Berichtdesign umfasst folgende Schritte:

1. Öffnen des Assistenten für das Berichtdesign.
2. Hinzufügen der Berichtdetails, Benennen des Berichts und Zuweisen von Kategoriekennungen.
3. Bestimmen eines Berichtlayouts, Auswählen der im Bericht enthaltenen Abfragen und Bestimmen, wie sie dargestellt werden.

Öffnen des Assistenten für das Berichtdesign

Wenn Sie einen neuen benutzerdefinierten Bericht von Grund auf neu erstellen oder auf der Grundlage eines vorhandenen Berichts erstellen möchten, öffnen Sie den Assistenten für das Berichtdesign.

So öffnen Sie den Assistenten für das Berichtdesign:

1. Klicken Sie auf die Registerkarte "Abfragen und Berichte" und dann auf die Unterregisterkarte "Berichte".

   Die Liste der Berichte wird angezeigt.

2. Klicken Sie auf "Optionen" und wählen Sie dann entweder "Neu" oder "Kopieren" aus.

   Der Assistent für das Berichtdesign wird angezeigt.

   Beachten Sie bei Verwendung des Assistenten Folgendes:

   - Klicken Sie auf "Speichern", um ihre Daten zu speichern, ohne den Assistenten zu schließen.
   - Klicken Sie auf "Speichern und schließen", um den Bericht zu speichern und den Assistenten zu schließen.
   - Klicken Sie auf "Zurücksetzen", um die Ansicht im Assistenten auf die zuletzt gespeicherten Einstellungen zurückzusetzen.

Hinzufügen von Berichtdetails

Ein neuer Bericht kann von Grund auf neu erstellt oder auf Grundlage der Kopie eines bereits vorhandenen Berichts erstellt werden. Bei der Erstellung eines Berichts benennen Sie ihn und weisen ihm Software-Update-Kennungen oder benutzerdefinierte Kennungen zu.

So fügen Sie Berichtdetails hinzu:

1. Öffnen Sie den Assistenten für das Berichtdesign.
2. Geben Sie einen Namen für den Bericht ein. Wahlweise können Sie zu Informationszwecken eine Beschreibung eingeben.
3. Wählen Sie mithilfe der Wechselsteuerung für Kennungen eine oder mehrere Kennungen für den Bericht aus.
4. (Optional) Um eine benutzerdefinierte Kategoriekennung hinzuzufügen, geben Sie im Feld zum Hinzufügen einer benutzerdefinierten Kennung den Namen einer Kennung ein, und klicken Sie auf "Kennung hinzufügen".

   Die benutzerdefinierte Kennung wird in der Liste der ausgewählten Kennungen angezeigt.
5. (Optional) Um einen oder mehrere geschachtelte benutzerdefinierte Kennungen hinzuzufügen, wählen Sie eine Kennung aus, oder geben Sie den Namen der übergeordneten Kategorienkennung ein, gefolgt von einem umgekehrten Schrägstrich und dem Namen der untergeordneten Kennung. Klicken Sie anschließend auf "Kennung hinzufügen". Sie könnten beispielsweise Folgendes eingeben: "Regulations\Industry-Standards". Sie können zusätzliche Kennungen hinzufügen, indem Sie folgendes Format beibehalten: a\b\c usw.

   Hinweis: Wenn Sie eine der benutzerdefinierten geschachtelten Kennungen löschen, werden alle Kennungen, in denen sie geschachtelt wurde, auch einschließlich der übergeordneten Kennung, gelöscht. Wenn Sie eine benutzerdefinierte Kennung in einer Software-Update-Kennung schachteln und sie dann löschen, werden nur die benutzerdefinierten Kennungen gelöscht.

   Wenn Sie den Vorgang abschließen, werden die neuen Kennungen in der Liste angezeigt. Wenn Sie die übergeordnete Kennung einblenden, sind die geschachtelten benutzerdefinierten Kennungen sichtbar.
6. Fahren Sie mit dem Schritt zur Gestaltung des Layouts fort, oder klicken Sie nach Auswahl mindestens einer Abfrage auf "Speichern und schließen".

Entwerfen von Berichtslayouts

Sie können die Berichtsstruktur entwerfen, indem Sie die Rastergröße und die Abmessungen festlegen und anschließend die Abfragen auswählen, die in den einzelnen Abschnitten des Rasters angezeigt werden sollen.

So entwerfen Sie ein Berichtslayout:

1. Öffnen Sie den Assistenten für das Berichtdesign. Falls es sich um einen neuen Bericht handelt, geben Sie einen Namen ein, wählen Sie eine Kennung aus, und fahren Sie mit dem Schritt "Layout" fort.
2. Wählen Sie im Fensterbereich "Berichtslayout" in den Bereichen "Rasterzeilen" und "Spalten" die Anzahl von Zeilen und Spalten aus, die im Bericht angezeigt werden soll, oder geben Sie diese ein. Diese Einstellungen steuern die Anzahl der Abfrageanzeigebereiche des Berichts. Sie können bis zu 10 Zeilen und/oder Spalten angeben.

   Im Fensterbereich "Berichtslayout" wird die entsprechende Anzahl von Zeilen, Spalten und Abfrageanzeigen angezeigt.

   Hinweis: Mit den Pfeilen rechts und unterhalb der Abfrageanzeigebereiche können Sie diese bei Bedarf horizontal oder vertikal vergrößern oder verkleinern.
3. (Optional) Geben Sie in den Bereichen "Mindestbreite" und "Mindesthöhe" die minimale Pixelgröße für die Abfrageanzeigebereiche ein, oder wählen Sie diese aus.
4. Ziehen Sie die Abfrage, die Sie in einem Anzeigebereich anzeigen möchten, aus der Abfrageliste in den entsprechenden Bereich des Berichtslayouts.
5. (Optional) Klicken Sie oberhalb eines Abfrageanzeigebereichs auf die Schaltfläche "Bearbeiten", um die Abfrage zu bearbeiten, die Sie an dieser Stelle platziert haben, oder um eine neue benutzerdefinierte Abfrage zu erstellen.
6. Klicken Sie auf "Speichern und schließen".

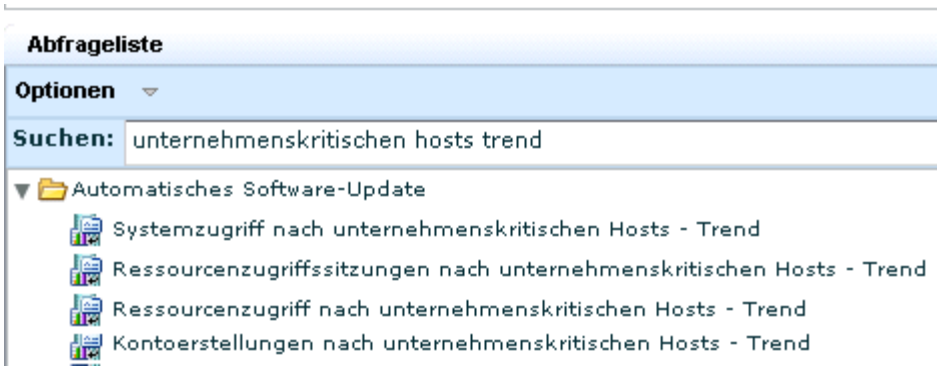
   Der Assistent für das Berichtdesign wird geschlossen. Der neue Bericht wird in der Berichtsliste unterhalb des Ordners "Benutzer" angezeigt.

Beispiel: Bericht aus bestehenden Abfragen erstellen

Sie können benutzerdefinierte Berichte erstellen, die sich aus vordefinierten Abfragen zusammensetzen, und diese speziell auf Ihre spezifischen Anforderungen zuschneiden.

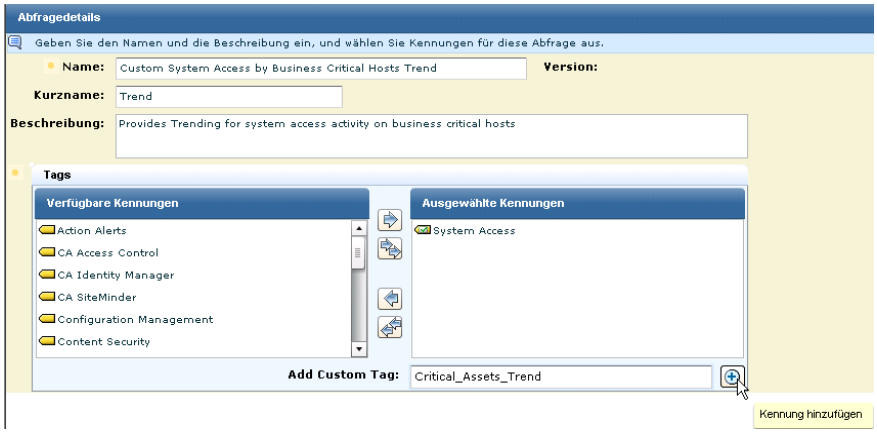
So erstellen Sie einen Bericht aus bestehenden Abfragen:

1. Ermitteln Sie die Abfragen, die in den benutzerdefinierten Bericht eingeschlossen werden sollen.
   a. Klicken Sie auf die Registerkarte "Abfragen und Berichte" und auf die Unterregisterkarte "Abfragen", falls sie nicht angezeigt wird.
   b. Geben Sie einen Schlüsselwort oder einen Schlüsselausdruck in das Feld "Suchen" ein, um die Abfragen mit entsprechendem Inhalt anzuzeigen, unter denen Sie eine Auswahl treffen möchten. Geben Sie beispielsweise "kritische Hosts – Trend" ein.
   c. Notieren Sie sich die Namen der Abfragen, die Sie in den benutzerdefinierten Bericht einschließen möchten. Sie können zum Beispiel aus den in der folgenden Abbildung aufgeführten unternehmenskritischen Hosts einen Bericht über die Trends definieren, die den Hosts zugeordnet sind, also beispielsweise über die Trends für "Systemzugriff", "Ressourcenzugriff" und "Kontoerstellungen".



2. Erstellen Sie für die erste in den Bericht einzuschließende Abfrage eine Kopie, und fügen Sie eine benutzerdefinierte Kennung hinzu.
   a. Wählen Sie eine Abfrage und dann in der Dropdown-Liste die Option "Kopieren" aus.
   b. Benennen Sie die Abfrage um, und geben Sie eine benutzerdefinierte Kennung ein, die hinzugefügt werden soll. Benennen Sie beispielsweise "Systemzugriff nach unternehmenskritischen Hosts - Trend" in "Benutzerdefinierten Systemzugriff nach unternehmenskritischen Hosts - Trend" um.

c. Fügen Sie eine benutzerdefinierte Kennung hinzu. Geben Sie beispielsweise "Critical_Assets_Trend" ein, und klicken Sie auf "Kennung hinzufügen".



d. Klicken Sie auf die Schaltfläche "Verschieben", um die vorausgewählte Kennung in den Bereich "Verfügbare Kennungen" zu verschieben. Verschieben Sie beispielsweise "Systemzugriff". Die einzige ausgewählte Kennung ist die von Ihnen hinzugefügte Kennung.

e. Klicken Sie auf "Speichern und schließen".

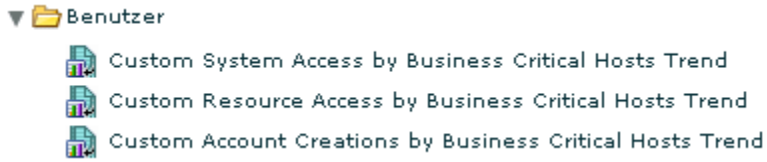
3. Erstellen Sie für die anderen in den Bericht einzuschließenden Abfragen eine Kopie, und fügen Sie die von Ihnen erstellte benutzerdefinierte Kennung hinzu.

   a. Wählen Sie eine Abfrage und dann in der Dropdown-Liste die Option "Kopieren" aus.

   b. Benennen Sie die Abfrage um, und wählen Sie die neue benutzerdefinierte Kennung aus. Benennen Sie beispielsweise "Kopie von Ressourcenzugriff nach unternehmenskritischen Hosts - Trend" in "Benutzerdefinierter Ressourcenzugriff nach unternehmenskritischen Hosts - Trend" um, verschieben Sie "Critical_Assets_Trend" in die Liste "Ausgewählte Kennungen", und entfernen Sie die vorausgewählte Kennung.

   c. Klicken Sie auf "Speichern und schließen".

   Die kopierten Abfragen werden unter dem Ordner "Benutzer" angezeigt:

4. Falls die Abfragen mit einer Schlüsselliste verknüpft sind, definieren Sie die Werte für diese Schlüsselliste.

5. Initiieren Sie den Berichterstellungsprozess wie folgt:

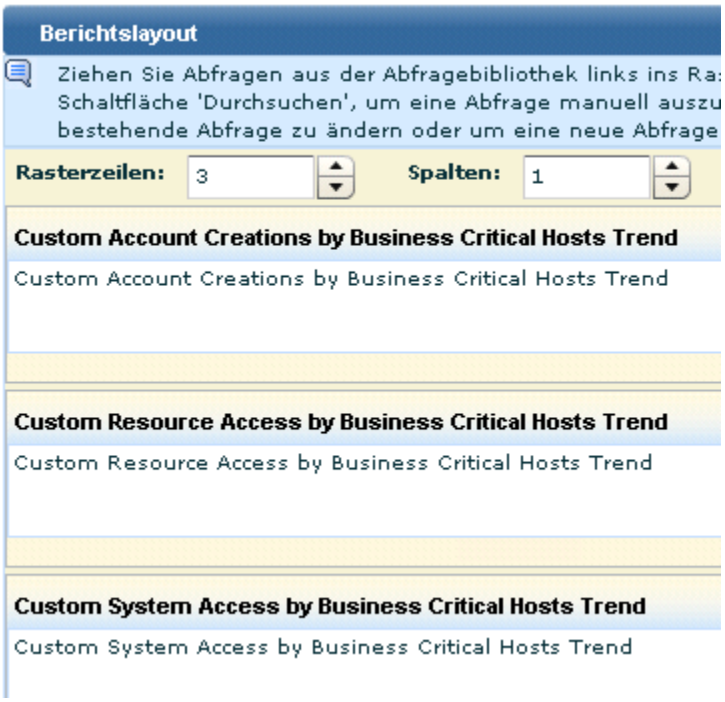
   a. Klicken Sie auf die Registerkarte "Abfragen und Berichte" und dann auf die Unterregisterkarte "Berichte".

   b. Wählen Sie unter der Berichtsliste im Dropdown-Menü "Optionen" die Option "Neu" aus.

      Der Assistent für das Berichtdesign wird angezeigt.

      Fügen Sie die benutzerdefinierte Kennung, "Critical_Assets_Trend", hinzu.

6. Entwerfen Sie das Berichtslayout.



7. Klicken Sie auf "Speichern und schließen".
8. Planen Sie den Bericht basierend auf der von Ihnen erstellten benutzerdefinierten Kennung.
9. Zeigen Sie den Bericht an.

Hinweis: Es empfiehlt sich, jeden neuen Bericht zu überprüfen, um sicherzustellen, dass er die gewünschten Informationen in der bestmöglichen Weise bereitstellt.

Beispiel: Einrichten von "Verbund" und "Verbundberichte"

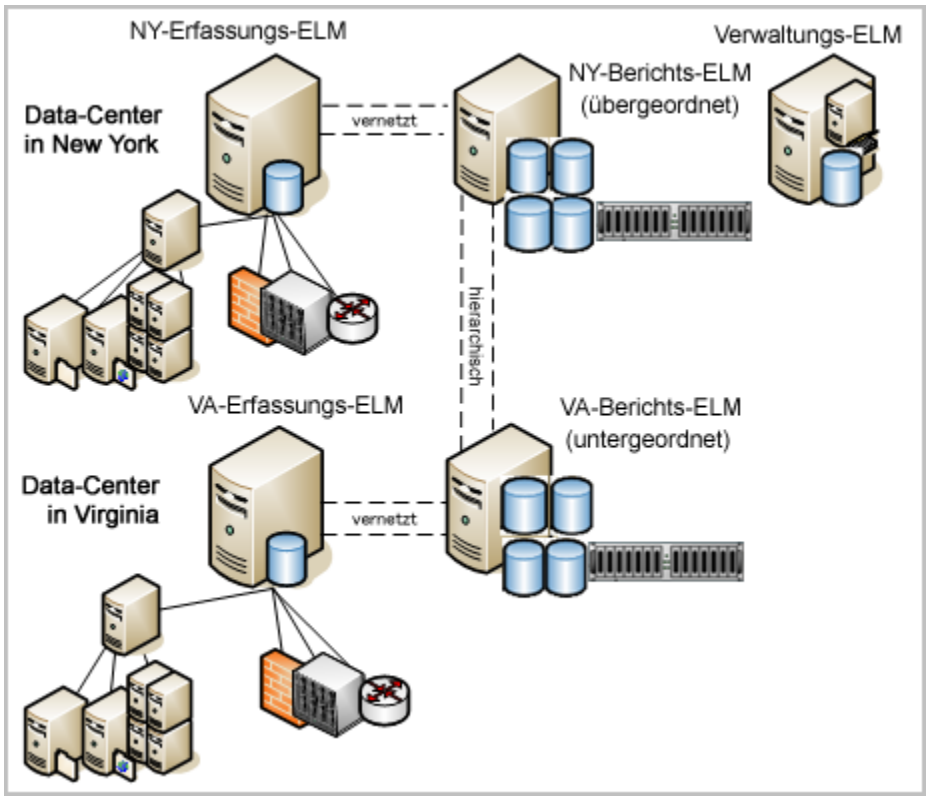
Sie können Protokolle von geografisch getrennten Datenzentren mit hohem Datendurchsatz sammeln und die Berichterstellung so einrichten, dass die verteilten Daten von nur einem der Datenzentren abgefragt werden.

Stellen Sie sich ein Beispielszenario vor, in dem zwei Datenzentren mit hohem Datendurchsatz im New York und Virginia liegen, wobei New York der Hauptsitz des Unternehmens ist. In jedem Datenzentrum gibt es einen Erfassungsserver, der eingehende Ereignisprotokolle erfasst und verarbeitet und sie an seinen Berichtsserver sendet. Der Berichtsserver bearbeitet Abfragen, Alarme und Berichte. Die meisten Abfragen, Alarme und Berichte zielen auf Ereignisdaten, die von Agenten erfasst worden sind; die Konsolidierung der Daten von diesen Ereignisquellen erfordert einen Verbund zwischen den Berichts- und den Erfassungsservern.

Einige Abfragen, Alarme und Berichte zielen auf selbstüberwachende Ereignisse, die von CA Enterprise Log Manager-Servern erstellt worden sind; die Konsolidierung dieses Datentyps erfordert den Einschluss des Verwaltungsservers in den Verbund. Wenn die Konsolidierung der Daten von selbstüberwachenden Ereignissen nicht gewünscht wird, kann der Verwaltungsserver aus dem Verbund ausgeschlossen werden. Selbstüberwachende Ereignisse von diesem Server können mit nicht-verbundenen, lokalen Berichten überwacht werden. Der Einfachheit halber wird der Verwaltungsserver aus diesem Verbund ausgeschlossen; der Einschluss könnte erreicht werden durch das Erstellen eines vernetzten Verbunds zwischen dem Berichts-ELM in New York und dem Verwaltungs-ELM.

Die Server haben die folgenden Bezeichnungen:

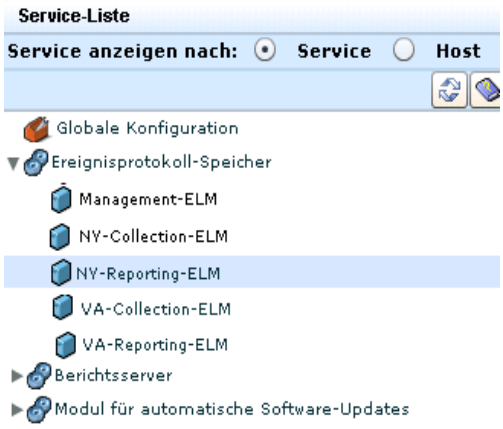
- Verwaltungs-ELM
- NY-Sammel-ELM
- NY-Berichts-ELM
- VA-Erfassungs-ELM
- VA-Berichts-ELM



Nehmen Sie an, der Administrator in New York möchte, dass alle Berichte und Alarme des Standorts New York Daten des Standorts Virginia einschließen, dass jedoch die Berichte und Alarme vom Standort Virginia nur lokal erfasste Daten enthalten.

Das folgende Beispiel zeigt, wie die Server in einen Verbund einzugliedern sind, und wie die Berichterstellung zu konfigurieren ist, um die Voraussetzungen für dieses Szenario zu erfüllen. Verfahren zum Konfigurieren der automatischen Archivierung werden in diesem Beispiel nicht behandelt, jedoch sollte bei jeder für einen hohen Datendurchsatz konzipierten Architektur die automatische Archivierung konfiguriert werden.

1. Melden Sie sich mit Administratorrechten bei einem CA Enterprise Log Manager an.
2. Klicken Sie auf die Registerkarte "Verwaltung", und wählen Sie die Unterregisterkarte "Services" aus.
3. Erstellen Sie einen hierarchischen Verbund, in dem der NY-Berichts-ELM der übergeordnete und der VA-Berichts-ELM der untergeordnete Server ist:
   a. Erweitern Sie den Dienst "Ereignisprotokollspeicher", und wählen Sie dann den Namen des Servers aus, der im hierarchischen Verbund übergeordnet sein soll, in diesem Fall der NY-Berichts-ELM.



   b. Wählen Sie den VA-Berichts-ELM aus der Liste der für den Verbund verfügbaren untergeordneten Server aus, und verschieben Sie ihn in die Auswahlliste.

4. Erstellen Sie einen vernetzten Verbund zwischen dem NY-Berichts-ELM und dem NY-Erfassungs-ELM wie folgt, wobei jeder dem anderen untergeordnet ist:
   a. Wählen Sie den NY-Berichts-ELM aus der Liste "Ereignisprotokollspeicher" aus.
   b. Wählen Sie den NY-Erfassungs-ELM aus der Liste der für den Verbund verfügbaren untergeordneten Server aus, und verschieben Sie ihn in die Auswahlliste.
   c. Wählen Sie den NY-Erfassungs-ELM aus der Liste "Ereignisprotokollspeicher" aus.
   d. Wählen Sie den NY-Berichts-ELM aus der Liste der für den Verbund verfügbaren untergeordneten Server aus, und verschieben Sie ihn in die Auswahlliste.
5. Erstellen Sie einen vernetzten Verbund zwischen dem VA-Berichts-ELM und dem VA-Erfassungs-ELM wie folgt, wobei jeder dem anderen untergeordnet ist:
   a. Wählen Sie den VA-Berichts-ELM aus der Liste "Ereignisprotokollspeicher" aus.
   b. Wählen Sie den VA-Erfassungs-ELM aus der Liste der für den Verbund verfügbaren untergeordneten Server aus, und verschieben Sie ihn in die Auswahlliste.
   c. Wählen Sie den VA-Erfassungs-ELM aus der Liste "Ereignisprotokollspeicher" aus.
   d. Wählen Sie den VA-Berichts-ELM aus der Liste der für den Verbund verfügbaren untergeordneten Server aus, und verschieben Sie ihn in die Auswahlliste.
6. Konfigurieren Sie die globalen Berichtsservereinstellungen und deren lokale Umgehungen für den VA-Berichts-ELM wie folgt. Für geografisch getrennte Server werden oft verschiedene Mailserver verwendet.
   a. Wählen Sie "Alarm-Service" in der Service-Liste aus.
   b. Konfigurieren Sie globale oder lokale Einstellungen, wie für die Mailserveroptionen des Knotens NY-Berichts-ELM benötigt.
   c. Wenn Sie Berichte per E-Mail versenden möchten, wählen Sie "Berichtsserver" und anschließend den Knoten NY-Berichts-ELM.
   d. Legen Sie globale oder lokale PDF-Formatoptionen oder Berichtsoptionen fest, die im Zusammenhang mit der Berichts- und Alarmaufbewahrung stehen.

7. Für jeden Bericht, der nach Plan vom NY-Berichts-ELM ausgeführt werden soll, nehmen Sie Folgendes vor:

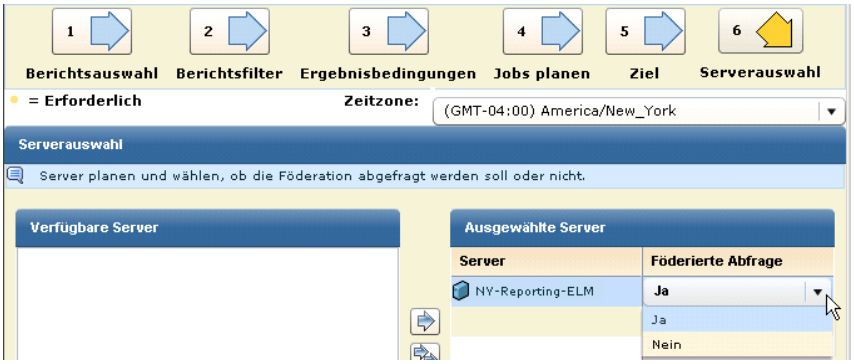
   a. Klicken Sie auf die Registerkarte "Geplante Berichte" und auf die Unterregisterkarte "Berichtsplanung".

   b. Klicken Sie auf "Einen Bericht planen".

   c. Legen Sie fest, dass für den Bericht, je nach Erfordernis, die Schritte 2, 3, 4 und 5 geplant sind und ausgeführt werden.

   d. Klicken Sie auf den Schritt "Serverauswahl", wählen Sie den NY-Berichts-ELM aus der Liste der verfügbaren Server aus, und verschieben Sie ihn in die Liste ausgewählter Server. Akzeptieren Sie dann die Standardeinstellung "Ja" für "Verbundabfrage".

   e. Klicken Sie auf "Speichern und schließen".



Die entsprechenden Berichte enthalten Daten vom NY-Berichts-ELM, dem ihm gleichgeordneten NY-Erfassungs-ELM, dem ihm untergeordneten VA-Berichts-ELM und dem diesem gleichgeordneten VA-Erfassungs-ELM.

Hinweis: Eine Verbundabfrage, die vom VA-Berichts-ELM ausgeführt wird, enthält Daten vom VA-Berichts-ELM und dem ihm gleichgeordneten VA-Erfassungs-ELM. Sie enthält keine Daten vom NY-Berichts-ELM, da dieser Server ihm im hierarchischen Verbund übergeordnet ist.

Bearbeiten von Berichten

Benutzerdefinierte Berichte können bearbeitet werden.

Hinweis: Die Option zum Anzeigen des ausgewählten Berichts kann beim Bearbeiten mehrerer Berichte deaktiviert werden. So können Sie Berichte auswählen und bearbeiten, ohne warten zu müssen, bis der entsprechende Bericht im Fenster "Details" angezeigt wird.

So bearbeiten Sie einen Bericht:

1. Wählen Sie in der Berichtsliste den Bericht aus, den Sie bearbeiten möchten.
2. Klicken Sie oben in der Liste auf "Optionen" und dann auf "Bearbeiten".

   Der Assistent für das Berichtdesign wird geöffnet. Die Details des ausgewählten Berichts sind bereits in den Feldern eingetragen.
3. Ändern Sie die Angaben wie gewünscht, und klicken Sie auf "Speichern und schließen".

   Der bearbeitete Bericht wird in die Berichtsliste im Benutzerordner übernommen.

Löschen benutzerdefinierter Berichte

Benutzerdefinierte Berichte können gelöscht werden. Automatische Berichte dagegen nicht.

So löschen Sie einen benutzerdefinierten Bericht:

1. Wählen Sie den zu löschenden Bericht in der Berichtsliste aus.
2. Klicken Sie oben in der Liste auf "Optionen", und wählen Sie anschließend "Löschen" aus.

   Ein Bestätigungsdialogfeld wird angezeigt.
3. Klicken Sie auf "Ja".

   Der entsprechende Bericht wird aus der Berichtsliste entfernt.

Weitere Informationen:

Generieren von Berichten (siehe Seite 349)
Bearbeiten von Berichten (siehe Seite 362)

Beispiel: Löschen täglicher Berichte, die älter als 30 Tage sind

Sie können Richtlinien zur Aufbewahrung von Berichten mit Hilfe der globalen Konfiguration von Berichtsservern implementieren. Sie können eine andere Aufbewahrungsrichtlinie für jede geplante Berichtswiederholung festlegen, z. B.:

- Aufbewahrung einmaliger Berichte
- Aufbewahrung täglicher Berichte
- Aufbewahrung wöchentlicher Berichte
- Aufbewahrung monatlicher Berichte
- Aufbewahrung jährlicher Berichte

Sie müssen die Standardeinstellung "Nie ausgeführt" für das Hilfsprogramm für die Berichtsaufbewahrung ändern und eine Häufigkeit eingeben. Achten Sie darauf, dass die Häufigkeit, die Sie für die Ausführung des Hilfsprogramms festlegen, groß genug ist, um Löschvorgänge mit der von Ihnen konfigurierten Häufigkeit durchzuführen. Wenn Sie z. B. die täglichen Berichte 1 Tag nachdem sie ausgeführt wurden löschen möchten und die täglichen Berichte für 6 Uhr und 18 Uhr planen, müssten Sie festlegen, dass das Hilfsprogramm für die Berichtsaufbewahrung mindestens alle 12 Stunden ausgeführt wird.

Beispiel: Löschen aller täglichen Berichte, die älter als 30 Tage sind

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

   Die Liste "Services" listet Services nach Service auf.

2. Klicken Sie auf "Berichtsserver".

   Die "Globale Service-Konfiguration: Berichtsserver" wird eingeblendet.

3. Nehmen Sie diese Konfiguration anhand der folgenden Anleitung vor:

   - Um das Löschen aller täglichen Berichte 30 Tage nach ihrer Erstellung zu automatisieren, legen Sie die Aufbewahrung täglicher Berichte so fest, dass der Löschvorgang nach 30 Tagen erfolgt.
   - Achten Sie darauf, dass das Hilfsprogramm für die Berichtsaufbewahrung immer nach der angegebenen Anzahl Stunden, Tagen oder Wochen durchgeführt wird.

4. Klicken Sie auf "Speichern".

Exportieren von Berichtsdefinitionen

Die Daten aus benutzererstellten Dateien können exportiert werden, um sie auf anderen Managementservern zu verwenden. Die exportierten Daten werden als XML-Datei gespeichert. Eine exportierte Berichtsdefinition beinhaltet die Definitionen aller im Bericht vorkommenden Abfragen.

So exportieren Sie Berichtdetails:

1. Klicken Sie auf die Registerkarte "Abfragen und Berichte" und dann auf die Registerkarte "Berichte".

   Die Liste der Berichte wird angezeigt.

2. Klicken Sie oben in der Liste auf "Optionen", und wählen Sie "Exportieren" aus.

   Das Dialogfeld "Benutzerdefinitionen exportieren" wird geöffnet. Hier werden alle verfügbaren, vom Benutzer erstellten Berichte angezeigt.

3. Wählen Sie die Berichte aus, die Sie mit Hilfe der Wechselsteuerung exportieren möchten, und klicken Sie auf "Exportieren".

   Das Dialogfeld "Exportieren" wird angezeigt.

4. Geben Sie den Speicherort für die XML-Exportdateien an, oder suchen Sie danach, und klicken Sie auf "Speichern".

   Die Berichtsdateien werden an dem von Ihnen ausgewählten Ablageort gespeichert, und ein Bestätigungsdialogfeld wird angezeigt.

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

   Das Dialogfeld "Benutzereigene Berichtsdefinitionen exportieren" wird geschlossen.

Weitere Informationen

Importieren von Berichtsdefinitionen (siehe Seite 365)

Importieren von Berichtsdefinitionen

XML-Dateien mit Berichtsdefinitionen können für eine Verwendung auf dem lokalen Managementserver importiert werden.

So importieren Sie Berichtdetails:

1. Klicken Sie auf die Registerkarte "Abfragen und Berichte" und dann auf die Registerkarte "Berichte".

   Die Liste der Berichte wird angezeigt.

2. Klicken Sie oben in der Liste auf "Optionen", und wählen Sie "Importieren" aus.

   Das Dialogfeld "Datei importieren" wird geöffnet.

3. Geben Sie den Speicherort für die Dateien an, die Sie importieren möchten, oder suchen Sie danach, und klicken Sie auf "OK".

   Das Fenster "Importergebnisse" wird angezeigt.

4. Klicken Sie auf "Andere Datei importieren", um Schritt 3 zu wiederholen, oder klicken Sie auf "Schließen".

   Das Fenster "Benutzerberichts- und Abfragedefinitionen importieren" wird geschlossen.

Weitere Informationen

Exportieren von Berichtsdefinitionen (siehe Seite 364)

Vorbereiten auf die Verwendung von Berichten mit Schlüssellisten

Alle Berichte basieren auf einer oder mehreren Abfragen. Einige Abfragen, die in vordefinierten Berichten verwendet werden, haben das Ziel, alle Werte aus einer bestimmten Tabelle zu wählen, in der ein bestimmtes Attributfeld einen Wert enthält, der als Kriterium für die Erstellung einer Schlüsselwerteliste dient. Beispiel: Eine Asset-Tabelle enthält ein Feld "IsCritical". Eine Abfrage, die alle Asset-Namen aus der Asset-Tabelle wählt, deren Feld "IsCritical" den Wert "Yes" enthält, wählt nur die Namen von kritischen Assets. Diese Namen können an CA Enterprise Log Manager zurückgegeben werden, um die Werte für den Schlüssel "Critical_Assets" zu aktualisieren.

Die Vorbereitung für die Verwendung von vordefinierten Berichten mit Schlüssellisten umfasst folgende Schritte:

- (Optional) Aktivieren des Imports von dynamischen Werten, wenn Sie CA IT PAM verwenden.
- Erstellen von Schlüssellisten für vordefinierte Schlüssel, die keine vordefinierten Werte enthalten.
- Anpassen von Schlüssellisten für vordefinierte Schlüssel, die keine vordefinierten Werte enthalten.
- Verwalten von Schlüssellisten, die in vordefinierten Berichten verwendet werden, die Sie nutzen möchten. Aktualisieren von Schlüssellisten mit aktuellen Werten

Außerdem können Sie neue Schlüssel für benutzerdefinierte Berichte hinzufügen, die Schlüssellisten verwenden, und anschließend Werte für jeden neuen Schlüssel hinzufügen. Sie können auch Werte für die Schlüssel "Business_Critical_Sources" und "ELM_System_Lognames" für eigene Abfragen auf Anforderung hinzufügen.

Aktivieren des Imports dynamischer Werte

Die für die Aktivierung des Imports dynamischer Werte erforderlichen Schritte gelten nur für Benutzer von CA IT PAM.

Falls Sie mit CA IT PAM arbeiten und bereits über Tabellen oder Arbeitsblätter verfügen, die beispielsweise Listen für Dateien, Datenbanken, Hosts oder Benutzer enthalten, können Sie diese Daten verwenden. Sie können einen Prozess erstellen, der die Tabelle bzw. Datei liest, die Werte für den Schlüssel auswählt und diese Werte an die CA Enterprise Log Manager-Werteliste für diesen Schlüssel zurückgibt.

So importieren Sie dynamische Werte:

1. Erstellen Sie in CA IT PAM einen Prozess für jede Schlüsselwerteliste, die bei Bedarf angelegt werden soll.

   Hinweis: Falls ein Prozess eine Datenbanktabelle lesen soll, installieren Sie einen CA IT PAM-Agenten auf dem Server mit der SQL Server 2005-Datenbank.

2. Konfigurieren Sie die CA IT PAM-Integration für dynamische Werte in CA Enterprise Log Manager.

Weitere Informationen:

Erstellen eines CA IT PAM-Prozesses zum Generieren einer Werteliste (siehe Seite 368)
Konfigurieren der CA IT PAM-Integration für dynamische Werte (siehe Seite 369)

Wissenswertes über Prozesse 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. Dabei wird vorausgesetzt, dass Sie bereits über Masterlisten der Dateien, Datenbanken, Hosts, Benutzer usw., aus denen Ihre Umgebung besteht, verfügen und dass diese Masterlisten Attribute aufweisen, anhand derer Sie nach den für Sie interessanten Wertegruppen suchen können. Falls Sie CA IT PAM verwenden, können Sie Prozesse erstellen, mit denen die Abfragen ausgeführt werden, welche die Daten an CA Enterprise Log Manager zurückgeben, die basierend auf den Schlüsseln als Schlüsselwerte in Berichten und Alarmen verwendet werden sollen. Durch die dynamische Erstellung einer Werteliste wird gewährleistet, dass eine Schlüsselliste immer die aktuellen Werte enthält.

Erstellen eines CA IT PAM-Prozesses zum Generieren einer Werteliste

Sie können in CA IT PAM einen Prozess für jede Schlüsselwerteliste erstellen, die nach Bedarf generiert werden soll. Weitere Informationen zum Erstellen von Prozessen finden Sie in Ihrer CA IT PAM-Dokumentation. Alle Prozesse müssen im Hinblick auf die lokalen Parameter "InputKey", "ValueList" und "FaultString" sowie auf die Berechnungsoperatoren "Erfolg" und "Fehler" den Anforderungen von CA Enterprise Log Manager entsprechen.

Verwenden Sie die folgenden Anweisungen:

- Der Prozess muss den ausgewählten Schlüssel als "InputKey" akzeptieren.
- Der Prozess muss die folgenden beiden lokalen Prozessparameter definieren:
  - "ValueList" ruft die Werteliste ab.
  - "FaultString" ruft die Fehlerzeichenfolge ab.

  Hinweis: Für CA Enterprise Log Manager müssen diese exakten Parameternamen als Parameter für die Ausgabeschnittstelle verwendet werden.
- Der Prozess muss die folgenden beiden Berechnungsparameter enthalten:
  - Berechnungsoperator "Erfolg": Process.ValueList =<Variable mit kommagetrennter Werteliste>
  - Berechnungsoperator "Fehler": Process.FaultString =<Variable mit Fehlermeldung>

Wenn Sie ein Skript erstellen, beachten Sie außerdem die folgenden weiteren Anweisungen:

- Wenn Ihr Skript eine Spalte aus einer Datenbanktabelle auswählt, muss auf dem Server, auf dem SQL Server 2005 installiert ist, ein IT PAM-Agent vorhanden sein. SQL-Servers müssen in Ihrer Domain unter "All Touchpoints" aufgelistet sein. Der SQL-Server mit den Schlüsseldaten muss den Agent-Namen für den SQL-Server anzeigen.
- Das integrierte Skript muss das Dienstprogramm "sqlcmd" ausführen, um die gewünschte Liste abzurufen.

Weitere Informationen

Konfigurieren der CA IT PAM-Integration für dynamische Werte (siehe Seite 369)

Konfigurieren der CA IT PAM-Integration für dynamische Werte

Sie können die CA IT PAM-Integration so konfigurieren, dass einer oder auch beide der folgenden CA IT PAM-Prozesstypen genutzt werden können:

- Ereignis-/Alarmausgabeprozess: Dies ist ein Prozess, durch den die Verarbeitung auf einem Drittanbietersystem wie etwa einem Helpdesk-Produkt aktiviert wird.
- Prozess mit dynamischen Werten: Diese Art von Prozess akzeptiert einen Eingabeschlüssel und gibt aktuelle Werte für diesen Schlüssel in Form einer CSV-Datei (CSV = durch Komma getrennte Werte) zurück.

Um diese Prozesse zu konfigurieren, müssen Sie in der Lage sein, CA IT PAM zu starten und sich dort anzumelden. Notieren Sie sich folgende Werte:

- den voll qualifizierten Hostnamen bzw. die IP-Adresse des CA IT PAM-Servers
- den Port (der Standardport ist 8080)
- den Benutzernamen und das Kennwort, mit dem sich CA Enterprise Log Manager bei CA IT PAM anmelden soll

Wenn Sie CA IT PAM für dynamische Werte konfigurieren, können Sie die Liste der vom entsprechend konfigurierten Prozess dynamisch erzeugten Werte importieren. Der Import wird durchgeführt, wenn die in bestimmten Berichten und Alarmen verwendeten Schlüsselwerte eingerichtet bzw. aktualisiert werden.

In den folgenden Schritten werden sowohl die allgemeinen Einstellungen als auch die eine, für dynamische Werte spezifische Einstellung verwendet.

So konfigurieren Sie die CA IT PAM-Integration für den Prozess mit dynamischen Werten:

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

   Die "Globale Service-Konfiguration: Berichtsserver" wird eingeblendet.
3. Blättern Sie zum Bereich "IT PAM".
4. Machen Sie folgende Angaben, um den Zugriff auf CA IT PAM zu aktivieren:
   a. Geben Sie den voll qualifizierten Hostnamen des Servers ein, auf dem CA IT PAM installiert ist.
   b. Übernehmen Sie den Standardport 8080.
   c. Geben Sie gültige Anmeldedaten für CA IT PAM ein.
5. Geben Sie im Feld "Prozess mit dynamischen Werten" einen Prozesspfad ein.

   Dieser Pfad wird beim Import von dynamischen Werten als Standardpfad verwendet.
6. Klicken Sie auf "Speichern".

   Es wird die folgende Bestätigungsmeldung angezeigt: "Die Konfigurationsänderungen wurden erfolgreich gespeichert."

Möglichkeiten der Verwaltung von Schlüssellisten

Schlüssellisten werden in einigen vordefinierten Berichten und in einigen vordefinierten Abfragen, die als geeignet für Aktionsalarme ausgewiesen sind, verwendet. Falls Sie diese Berichte verwenden oder Alarme erstellen möchten, die diese Abfragen verwenden, können Sie Ihre Schlüssellisten mit den folgenden Methoden verwalten.

- Sie können Schlüsselwerte direkt für einen ausgewählten Schlüssel hinzufügen. Sie können einen Schlüsselwert auswählen und diesen bearbeiten oder löschen.
- Sie können in einer CSV-Liste gespeicherte Schlüsselwerte importieren. Alternativ haben Sie die Möglichkeit, die aktuelle Werteliste in eine CSV-Datei zu exportieren, diese Datei zu aktualisieren und dann die aktualisierte Datei zu importieren, um so die Werteliste zu füllen.
- Sie können einen CA IT PAM-Prozess ausführen, der dynamisch eine aktuelle Liste erzeugt und die Werte in einer CSV-Datei zurückgibt, mit der die Werteliste gefüllt wird.

Falls Sie benutzerdefinierte Berichte erstellen möchten, die eine Schlüsselliste verwenden, können Sie einen eigenen Schlüssel hinzufügen und dann Werte für diesen Schlüssel hinzufügen bzw. importieren.

Sie können die in einer Abfrage verwendeten Schlüssellisten ermitteln und dann diese Listen aktualisieren, bevor Sie einen Bericht bzw. Alarm mit dieser Abfrage einplanen.

Weitere Informationen:

Manuelles Aktualisieren einer Schlüsselliste (siehe Seite 374)
Aktualisieren einer Schlüsselliste mittels Export/Import (siehe Seite 375)
Beispiel: Aktualisieren einer Schlüsselliste mit einer CSV-Datei (siehe Seite 377)
Verwenden von Abfragen mit der Kennung "Aktionsalarme" (siehe Seite 389)

Erstellen einer Liste mit Schlüssel

Listen mit Schlüssel ermöglichen es Ihnen, eine Gruppe zu erstellen und ihr Werte zuzuweisen. Sie können dann den Gruppennamen abfragen und jeder einzelne der Werte in der Gruppe wird ein positives Ergebnis zurückgeben. Sie können Werte einzeln zuweisen oder aus einer CSV-Datei importieren. Sie können benutzerdefinierte Listen mit Schlüssel erstellen oder Werte zu vordefinierten Listen hinzufügen.

Zum Beispiel suchen einige Abfragen der Berichte über das Gewähren von Berechtigungen nach einem Schlüsselwert mit dem Namen "Privileged_Groups". Wenn eine Abfrage diesen Wert enthält, werden alle Zeilen zurückgegeben, in denen dieses Feld einen der in der Gruppe angegebenen Werte enthält.

So erstellen Sie eine Liste mit Schlüssel

1. Klicken Sie auf die Registerkarte "Verwaltung", die Unterregisterkarte "Bibliothek" und den Ordner "Liste mit Schlüssel".
2. Klicken Sie für eine neue Liste auf "Neu", oder wählen Sie die Liste aus, der Sie Werte hinzufügen wollen.

   In rechten Fensterbereich wird "Listen mit Schlüssel - Details" angezeigt.
3. Geben Sie einen Namen und eine Beschreibung für die Liste mit Schlüssel ein und wählen Sie einen Typ aus.
4. Geben Sie den IT PAM-Prozess mit dynamischen Werten ein, der Werte für den ausgewählten Schlüssel generiert.

   Hinweis: Der IT PAM-Prozess mit dynamischen Werten aktualisiert nur die Liste "Benutzer" der Tabelle der Schlüssellistenwerte. Die Liste "Benutzer" wird periodisch mit den neuesten Werten überschrieben.
5. (Optional) Falls Sie die Gültigkeit des eingegebenen IT PAM-Prozesses mit dynamischen Werten testen wollen, klicken Sie auf das Testsymbol.

   Wenn die Verbindung erfolgreich hergestellt wird, wird eine Bestätigungsmeldung angezeigt.
6. Wenn Sie Werte importieren möchten, fahren Sie mit Schritt 10 fort. Wenn Sie Werte einzeln hinzufügen möchten, fahren Sie mit Schritt 7 fort.
7. Klicken Sie am oberen Ende der Tabelle der Schlüssellistenwerte auf "Hinzufügen".

   Eine hervorgehobene Zeile wird in der Spalte "Benutzer" angezeigt.
8. Klicken Sie die Zeile an und geben Sie einen Wert ein.
9. Wiederholen Sie Schritt 6-7, um weitere Werte hinzuzufügen.

10. Klicken Sie im oberen Bereich der Listendetails auf "Importieren", suchen Sie nach der Datei, die die Werte enthält, die Sie importieren wollen, und klicken Sie auf OK.

    Die Werte werden im Bereich "Werte" angezeigt.

    Hinweis: Nur CSV-Dateien, die keine Sonderzeichen enthalten, können importiert werden.

11. Klicken Sie nach dem Hinzufügen der gewünschten Werte auf "Speichern".

    Die neue Liste wird im Ordner "Benutzer" des Ordners "Listen mit Schlüssel" angezeigt.

Manuelles Aktualisieren einer Schlüsselliste

Sie haben verschiedene Möglichkeiten, die Werte in einer Schlüsselliste zu aktualisieren. Sie können die Werte zum einen manuell hinzufügen, bearbeiten und löschen.

So aktualisieren Sie eine Schlüsselliste manuell:

1. Klicken Sie auf die Registerkarte "Verwaltung", die Unterregisterkarte "Bibliothek" und den Ordner "Liste mit Schlüssel".
2. Erweitern Sie den Ordner "Liste mit Schlüssel" und wählen Sie die Schlüsselliste aus, die Sie aktualisieren wollen.
3. So fügen Sie einen Wert zur Schlüsselliste hinzu:
   a. Wählen Sie den Schlüssel, zu dem Sie einen Wert hinzufügen möchten.
   b. Klicken Sie auf "Wert hinzufügen":
   c. Geben Sie den Namen des Werts im Feld "Name" ein, und klicken Sie auf "OK".

      Der hinzugefügte Wert wird in der Liste "Werte" des ausgewählten Schlüssels aufgeführt.
   d. Wiederholen Sie diese Schritte für jeden Wert, den Sie hinzufügen möchten.
4. So löschen Sie einen Wert aus einer Schlüsselliste:
   a. Wählen Sie den Schlüssel, aus dem Sie einen Wert löschen möchten.
   b. Wählen Sie den zu löschenden Wert, und klicken Sie auf "Wert entfernen".

      Eine Bestätigungsmeldung wird angezeigt.
   c. Klicken Sie auf "OK".

      Der hinzugefügte Wert wird aus der Liste "Werte" des ausgewählten Schlüssels gelöscht.
   d. Wiederholen Sie diese Schritte für jeden Wert, den Sie löschen möchten.
5. So bearbeiten Sie einen Wert in einer Schlüsselliste:
   a. Wählen Sie den Schlüssel, in dem Sie einen Wert bearbeiten möchten.
   b. Wählen Sie den zu bearbeitenden Wert, und klicken Sie auf "Wert bearbeiten".
   c. Bearbeiten Sie den Eintrag im Feld "Name", und klicken Sie auf "OK".

Der Wert wird in der Liste "Werte" des ausgewählten Schlüssels mit dem geänderten Namen angezeigt.

d. Wiederholen Sie diese Schritte für jeden Wert, den Sie bearbeiten möchten.

6. Klicken Sie auf "Speichern".

   Die Werte der ausgewählten Schlüssel werden aktualisiert.

Aktualisieren einer Schlüsselliste mittels Export/Import

Falls Sie Werte, die einem Schlüssel entsprechen, in einer Excel-Tabelle ablegen, können Sie diese Tabelle als CSV-Liste (CSV = durch Komma getrennte Werte, *.csv) speichern und die Schlüsselliste für den gewählten Schlüssel mittels Import füllen.

Sie können die Werte in der Schlüsselliste folgendermaßen in einer CSV-Datei speichern:

- Falls die CSV-Datei aktuelle Werte für einen bestimmten Schlüssel enthält und die angezeigte Werteliste veraltet ist, können Sie die Werte direkt aus der CSV-Datei importieren.
- Falls Sie eine CSV-Datei erstellen bzw. eine Datei mit veralteten Werten aktualisieren möchten, verwenden Sie die Sequenz Exportieren, Bearbeiten, Importieren.

So aktualisieren Sie eine Schlüsselliste mittels Export/Import:

1. Klicken Sie auf die Registerkarte "Verwaltung", die Unterregisterkarte "Bibliothek" und den Ordner "Liste mit Schlüssel".
2. Erweitern Sie den Ordner "Liste mit Schlüssel" und wählen Sie die Schlüsselliste aus, die Sie aktualisieren wollen.

3. So aktualisieren Sie Werte für einen ausgewählten Schlüssel anhand einer CSV-Datei mit aktuellen Werten:
   a. Wählen Sie in der Liste "Schlüsselwerte" den Schlüssel aus, den Sie aktualisieren möchten.
   b. Klicken Sie in der Symbolleiste "Werte" auf "Werte importieren".

      Das Dialogfeld "Datei importieren" wird angezeigt.
   c. Klicken Sie auf "Durchsuchen" und navigieren Sie zum Speicherort, an dem die CSV-Datei mit den Werten für den ausgewählten Schlüssel gespeichert ist.
   d. Wählen Sie die zu importierende Datei aus, klicken Sie auf "Öffnen" und danach auf "OK".

   Die Liste "Werte" wird mit den Werten aus der CSV-Datei aktualisiert.
4. So aktualisieren Sie Werte für einen ausgewählten Schlüssel, für den keine oder eine veraltete CSV-Datei vorliegt:
   a. Wählen Sie in der Liste "Schlüsselwerte" den Schlüssel aus, den Sie aktualisieren möchten.
   b. Klicken Sie in der Symbolleiste "Werte" auf "Werte exportieren", navigieren Sie zu dem Speicherort, unter dem Sie die CSV-Datei abspeichern wollen, und klicken Sie auf "Speichern".

      Es wird eine Erfolgsmeldung angezeigt.
   c. Klicken Sie auf "OK".
   d. Navigieren Sie zur exportierten Datei, öffnen Sie das Arbeitsblatt und ändern oder löschen Sie vorhandene Spalten nach Bedarf. Blättern Sie zur letzten Spalte, und fügen Sie neue Einträge hinzu. Speichern Sie die Datei dann als CSV-Datei.
   e. Wählen Sie denselben Schlüssel aus, und klicken Sie auf "Werte importieren".
   f. Klicken Sie auf "Durchsuchen", wählen sie die von Ihnen gespeicherte Datei, und klicken Sie auf "Öffnen".
   g. Klicken Sie auf "OK".

   Die Datei wird hochgeladen. Sie können zum Ende der Werteliste scrollen, um zu überprüfen, ob Ihr neuer Eintrag vorhanden ist.

Beispiel: Aktualisieren einer Schlüsselliste mit einer CSV-Datei

Sie haben drei Möglichkeiten, Werte für Schlüssellisten anzugeben:

- Manuelle Eingabe der Schlüsselwerte
- Import der Schlüsselwerte aus einer CSV-Datei
- Import der Schlüsselwerte aus einem angegebenen CA IT PAM-Prozess

Verwenden Sie das folgende Beispiel als Richtlinie beim Aktualisieren der Werte einer benutzerdefinierten Schlüsselliste, wenn die Werte in einer Excel-Tabelle als CSV-Liste (CSV = durch Komma getrennte Werte, *.csv) gespeichert sind.

So aktualisieren Sie eine Schlüsselliste mit einer CSV-Datei:

1. Klicken Sie auf die Registerkarte "Verwaltung", die Unterregisterkarte "Bibliothek" und den Ordner "Liste mit Schlüssel".
2. Erweitern Sie den Ordner "Liste mit Schlüssel" und wählen Sie die Schlüsselliste aus, die Sie aktualisieren wollen, beispielsweise "Default_Accounts", und klicken Sie auf "Werte exportieren".

   Das Dialogfeld "Exportieren" wird mit "file.csv" als Standarddateiname angezeigt.
3. Wählen Sie das Verzeichnis aus, in dem die exportierte Datei gespeichert werden soll. Ändern Sie den Dateinamen, z. B. auf "Default_Accounts.csv", und klicken Sie auf "Speichern".

   Eine Bestätigungsmeldung wird angezeigt.
4. Klicken Sie auf "OK".
5. Suchen Sie die exportierte .csv-Datei, öffnen Sie sie, blättern Sie zur letzten Spalte und tragen Sie ein, was Sie hinzufügen wollen. Wahlweise können Sie die Spalte für einen beliebigen Standardeintrag löschen, den Sie aus der Schlüsselliste für Standardkonten (Default_Accounts) ausschließen möchten.
6. Speichen und schließen Sie die .csv-Datei und kehren Sie zur CA Enterprise Log Manager-Schnittstelle zurück.
7. Klicken Sie auf "Werte importieren" für die Liste, die Sie aktualisieren wollen; hier die Schlüsselliste "Default_Accounts".
8. Klicken Sie auf "Durchsuchen", wählen Sie die von Ihnen gespeicherte Datei, und klicken Sie auf "Öffnen".
9. Klicken Sie auf "OK".

   Die Datei wird hochgeladen. Blättern Sie zum Ende der Werteliste, um zu überprüfen, ob Ihr neuer Eintrag vorhanden ist.

Aktualisieren einer Schlüsselliste mit einem Prozess mit dynamischen Werten

Wenn Sie einen CA IT PAM-Prozess verwenden, um eine Liste mit Werten zu generieren, die einem Schlüssel in CA Enterprise Log Manager-Abfragen zugeordnet sind, führen Sie den IT PAM-Prozess mit dynamischen Werten von CA Enterprise Log Manager aus aus, und aktualisieren Sie die Werte für einen angegebenen Schlüssel. Beim Importieren müssen die Werte für einen angegebenen Schlüssel nicht manuell eingeben werden und sparen daher Zeit. Wenn sich die Werte eines unserer Schlüssel ändern, können Sie sie in CA Enterprise Log Manager aktualisieren, indem Sie den Schlüssel auswählen und den Import der dynamischen Werte wiederholen.

Konfigurieren Sie die CA IT PAM-Integration für dynamische Werte, bevor Sie versuchen, die Schlüssellistenwerte von CA IT PAM zu importieren.

So importieren Sie Werte für eine Schlüsselliste von CA IT PAM:

1. Klicken Sie auf die Registerkarte "Verwaltung", die Unterregisterkarte "Bibliothek" und den Ordner "Liste mit Schlüssel".
2. Erweitern Sie den Ordner "Liste mit Schlüssel" und wählen Sie die Schlüsselliste aus, die Sie aktualisieren wollen.
3. So erstellen Sie einen Schlüssel für die zu importierenden Werte:
   a. Klicken Sie am oberen Ende der Tabelle der Schlüsselwerte auf "Hinzufügen".

      Die erste verfügbare Zeile in der Spalte "Benutzer" wird ausgewählt.

   b. Klicken Sie auf die Zeile und geben Sie den Namen des neuen Schlüssels ein.

   c. Klicken Sie auf "Speichern".
4. So aktualisieren Sie die dynamischen Werte für einen bestehenden Schlüssel:
   a. Wählen Sie den Schlüssel.

   b. Klicken Sie am oberen Ende des Fensterbereichs "Details" auf "Liste für den Import dynamischer Werte".

      Das Dialogfeld für den Import dynamischer Werte wird angezeigt.

   c. Geben Sie den Namen des IT PAM-Prozesses mit dynamischen Werten an, der die Werte für den ausgewählten Schlüssel generiert, und klicken Sie anschließend auf OK.

      Der entsprechende CA IT PAM-Prozess wird ausgeführt. Es wird eine Datei mit den Ergebnissen zurückgegeben, und die Werte für den ausgewählten Schlüssel werden aktualisiert.

d. Klicken Sie auf "Speichern".

Weitere Informationen:

Aktivieren des Imports dynamischer Werte (siehe Seite 367)
Wissenswertes über Prozesse mit dynamischen Werten (siehe Seite 367)
Erstellen eines CA IT PAM-Prozesses zum Generieren einer Werteliste (siehe Seite 368)
Konfigurieren der CA IT PAM-Integration für dynamische Werte (siehe Seite 369)

Feststellen der Schlüssellistenverwendung für eine Abfrage

Es empfiehlt sich, die Werte in Schlüssellisten immer auf dem neuesten Stand zu halten. Falls Sie eine Schlüsselliste aktualisieren möchten, die in einem bestimmten Bericht oder Alarm verwendet wird, ermitteln Sie zunächst die in dem Bericht bzw. Alarm verwendeten Abfragen. Ermitteln Sie dann, welche Schlüsselliste in der Quellabfrage bzw. in der Abfrage verwendet wird. Abfragen, die eine Schlüsselliste verwenden, verweisen häufig im Abfragename auf den Schlüssellistennamen. Beispiel: Abfragen mit "Standardkonten" oder "Berechtigte Gruppe" im Abfragenamen

So bestimmen Sie die Schlüssellistenverwendung für eine Abfrage

1. Öffnen Sie im Assistenten für das Abfragedesign eine Kopie der Abfrage, die die Schlüssellistenverwendung überprüfen soll.
2. Klicken Sie auf den Schritt "Abfragefilter", und wählen Sie die Registerkarte "Erweiterte Filter" aus.
3. Abfragen, die eine Schlüsselliste verwenden, weisen einen Filter mit dem Operator "Mit Schlüssel" auf. Der Wert ist der Name der Schlüsselliste, beispielsweise "Default_Accounts".
4. Klicken Sie auf "Abbrechen". Die Kopie der Abfrage wird nicht gespeichert.

Erstellen von Schlüsselwerten für vordefinierte Berichte

Einige vordefinierte Schlüssel, die in vordefinierten Berichten verwendet werden, weisen keine vordefinierten Werte auf. Um diese Berichte effektiv nutzen zu können, müssen Sie Werte für die jeweiligen Schlüssellisten bereitstellen. Sie können auch benutzerdefinierte Werte zu Schlüssellisten *mit* vordefinierten Werten hinzufügen.

Beispiele von Schlüssellisten, die keine vordefinierten Werte besitzen, sind:

- Critical_Assets
- DMZ_Hosts
- EPHI_Database
- Business_Critical_Sources

Sie können zu allen Schlüssellisten manuell oder durch Import Werte hinzufügen.

Weitere Informationen:

Manuelles Aktualisieren einer Schlüsselliste (siehe Seite 374)
Aktualisieren einer Schlüsselliste mittels Export/Import (siehe Seite 375)
Beispiel: Aktualisieren einer Schlüsselliste mit einer CSV-Datei (siehe Seite 377)

Erstellen von Schlüsselwerten für kritische Assets (Critical_Assets)

Dieses Thema gibt ein Beispiel dafür, wie benutzerdefinierte Werte zu einer Schlüsselliste hinzugefügt werden können, die keine standardmäßigen Werte besitzt. Sie können diesem Beispiel folgend auch Werte zu anderen bestehenden Schlüssellisten hinzufügen.

Sie können manche Berichte und Abfragen verwenden, um Aktivitäten nach unternehmenskritischen Hosts zu überwachen. Zu diesem Zweck müssen Sie diese Hosts zunächst als Werte in der Schlüsselwerteliste für Critical_Assets identifizieren.

Berichte, die die Liste "Critical_Assets" verwenden, enthalten Folgendes:

- Kontoerstellungen nach unternehmenskritischen Hosts
- Fehlgeschlagene Anmeldungen bei unternehmenskritischen Hosts
- Ressourcenzugriffssitzungen nach unternehmenskritischen Hosts
- Ressourcenzugriff nach unternehmenskritischen Hosts
- Systemzugriff nach unternehmenskritischen Hosts

Die Schlüsselliste für kritische Assets wird in ähnlichen Berichten für CA Access Control, CA Identity Manager und CA SiteMinder verwendet, wie etwa: CA Access Control - Kontoerstellungen nach unternehmenskritischen Hosts

Abfragen, die die Liste "Critical_Assets" verwenden, enthalten Folgendes:

- (>5) Anmeldungen nach Administratorkonten auf kritischen Systemen bei Nacht während des letzten Tages
- (>5) Anmeldungen nach Administratorkonten auf kritischen Systemen an Wochenenden während der letzten Woche
- Systemausnahmen ...

Definieren Sie den Filter wie folgt, wenn Sie eine benutzerspezifische Abfrage für kritische Assets erstellen:

Spalte	Operator	Wert
dest_hostname	Mit Schlüssel	Critical_Assets

Um einen Filter für andere Schlüssellisten festzulegen, ersetzen Sie den Wert durch den gewünschten Listenwert. Zum Beispiel könnten Sie den Filterwert auf "EPHI_Database" festlegen, um nach Hostnamen zu filtern, die zu jener Schlüsselliste gehören.

So erstellen Sie Schlüsselwerte für Critical_Assets:

1. Klicken Sie auf die Registerkarte "Verwaltung", die Unterregisterkarte "Bibliothek" und den Ordner "Liste mit Schlüssel".
2. Erweitern Sie den Ordner "Liste mit Schlüsseln" und wählen Sie "Critical_Assets" aus.
3. Führen Sie eine der folgenden Maßnahmen durch, um diese Liste zu erstellen:
   - Klicken Sie auf "Werte hinzufügen", und geben Sie die in die Schlüsselliste aufzunehmenden neuen Werte ein.
   - Erstellen Sie ein Excel-Arbeitsblatt mit einer Zeile, in der jede Spalte einem einzelnen Wert entspricht. Speichern Sie das Arbeitsblatt als csv-Datei. Klicken Sie auf "Werte importieren", um die bearbeitete Liste zu importieren.
   - Falls die Werte für diesen Schlüssel dynamisch vom CA IT PAM-Prozess mit dynamischen Werten erzeugt werden, klicken Sie auf "Liste der dynamischen Werte importieren".
4. Klicken Sie auf "Speichern".

   Berichte, die diese Schlüsselliste verwenden und anhand von geplanten Jobs erzeugt werden, enthalten nun Daten für die aktualisierten Werte.

Anpassen von Schlüsselwerten für Administratoren

Dieses Thema bietet ein Beispiel dafür, wie benutzerdefinierte Werte zu einer vordefinierten Schlüsselliste hinzugefügt werden können, in der bereits einige Werte festgelegt sind. Sie können diesem Beispiel folgend auch Werte zu anderen bestehenden Schlüssellisten hinzufügen.

Sie können vordefinierte Berichte und ihre zugehörigen Abfragen verwenden, um Aktivitäten nach Administratoren zu überwachen. Vordefinierte Werte sind u. a. "Administrator", "Root", "sa" und "admin". Um die Liste benutzerspezifisch anzupassen, können Sie andere Konten in Ihrer Umgebung, die Administratorrechte innehaben, als Werte in der Schlüsselwerteliste für Administratoren angeben.

Definieren Sie den Filter wie folgt, falls Sie eine benutzerspezifische Abfrage erstellen, in der dieser Schlüssel verwendet wird:

Spalte	Operator	Wert
dest_username	Mit Schlüssel	Administratoren

Um einen Filter für andere Schlüssellisten festzulegen, ersetzen Sie den Wert durch den gewünschten Listenwert. Zum Beispiel könnten Sie den Filterwert auf "EPHI_Database" festlegen, um nach Hostnamen zu filtern, die zu jener Schlüsselliste gehören.

So erstellen Sie benutzerdefinierte Schlüsselwerte für Administratoren:

1. Klicken Sie auf die Registerkarte "Verwaltung", die Unterregisterkarte "Bibliothek" und den Ordner "Liste mit Schlüssel".

   Unten im Hauptfensterbereich wird eine Liste von Schlüsseln eingeblendet, der Sie benutzerdefinierte Werte hinzufügen können.

2. Wählen Sie den Schlüssel "Administrators" aus.

   Die vordefinierten Werte werden angezeigt.

3. Sie haben folgende Möglichkeiten, die Liste zu aktualisieren:

   - Manuelle Aktualisierung der Liste:
     - Klicken Sie auf "Werte hinzufügen", und geben Sie den in die Schlüsselliste aufzunehmenden neuen Wert ein.
     - Wählen Sie einen Wert aus, und klicken Sie auf "Wert entfernen", um den Wert aus der Liste zu löschen.
     - Wählen Sie einen Wert aus, klicken Sie auf "Wert bearbeiten", ändern Sie den Wert, und klicken Sie auf "OK".
   - Aktualisierung der Liste über Export/Import:
     a. Klicken Sie auf "Werte exportieren", um die aktuelle Liste zu exportieren.
     b. Öffnen Sie die exportierte Liste, ändern Sie die Werte in der Liste, und speichern Sie die Datei.
     c. Klicken Sie auf "Werte importieren", um die bearbeitete Liste zu importieren.
   - Klicken Sie auf "Werte importieren", um die Werte in einer aktualisierten CSV-Datei zu importieren.
   - Falls die Werte für diesen Schlüssel dynamisch vom konfigurierten CA IT PAM-Prozess mit dynamischen Werten erzeugt werden, klicken Sie auf "Liste der dynamischen Werte importieren".

4. Klicken Sie auf "Speichern".

   Berichte, die diese Schlüsselliste verwenden und anhand von geplanten Jobs erzeugt werden, enthalten nun Daten für die aktualisierten Werte.

Anzeigen eines Berichts unter Verwendung einer Schlüsselliste

Sie können die Ergebnisse eines Berichts einsehen, bevor Sie seine Erstellung planen. Bestimmte vordefinierte Berichte verwenden Schlüssellisten, bei denen der Schlüssel vordefiniert ist, die Werte allerdings benutzerspezifisch sind. Nachdem Sie Werte für einen Schlüssel hinzugefügt oder importiert haben, empfiehlt es sich, den Bericht unter Verwendung der Schlüsselliste anzuzeigen.

So zeigen Sie einen Bericht unter Verwendung einer Schlüsselliste an:

1. Klicken Sie auf die Registerkarte "Abfragen und Berichte" und auf die Unterregisterkarte "Berichte".
2. Wählen Sie einen Bericht aus, der eine Schlüsselliste verwendet.
3. Zeigen Sie die Ergebnisse an.

Kapitel 12: Aktionsalarme

Dieses Kapitel enthält folgende Themen:

Info zu Aktionsalarmen

Aktionsalarme sind spezielle Berichte, die ein Ereignis generieren, wenn die entsprechenden Abfragebedingungen erfüllt sind. Mit Hilfe von Aktionsalarmen können Sie Ihre Umgebung durch automatische Benachrichtigungen für eine Vielzahl von Situationen und Vorkommnissen überwachen. So können Sie beispielsweise Aktionsalarme zum Bereitstellen von Ereignistrendinformationen, zum Nachverfolgen der Speicherplatznutzung oder zum Bereitstellen von Benachrichtigungen festlegen, wenn Schwellenwerte für fehlgeschlagene Zugriffe überschritten werden.

Aktionsalarme bieten eine gute Möglichkeit, eine Vielzahl von Daten für diese wenigen Ereignisse, auf die Sie sofort reagieren müssen, zu durchsuchen. Sie können Aktionsalarme verwenden, um über praktisch alles benachrichtigt zu werden, das in Ihrem Protokollerfassungsnetzwerk geschieht. Sie können Alarme erstellen, mit denen Sie über Häufungen bei eingehendem und ausgehendem Datenverkehr, über Datenverkehr an bestimmten Ports, über Zugriffe auf bestimmte berechtigte Ressourcen, über Konfigurationsänderungen an verschiedenen Netzwerkentitäten wie Firewalls, Datenbanken oder Schlüsselservern usw., benachrichtigt werden.

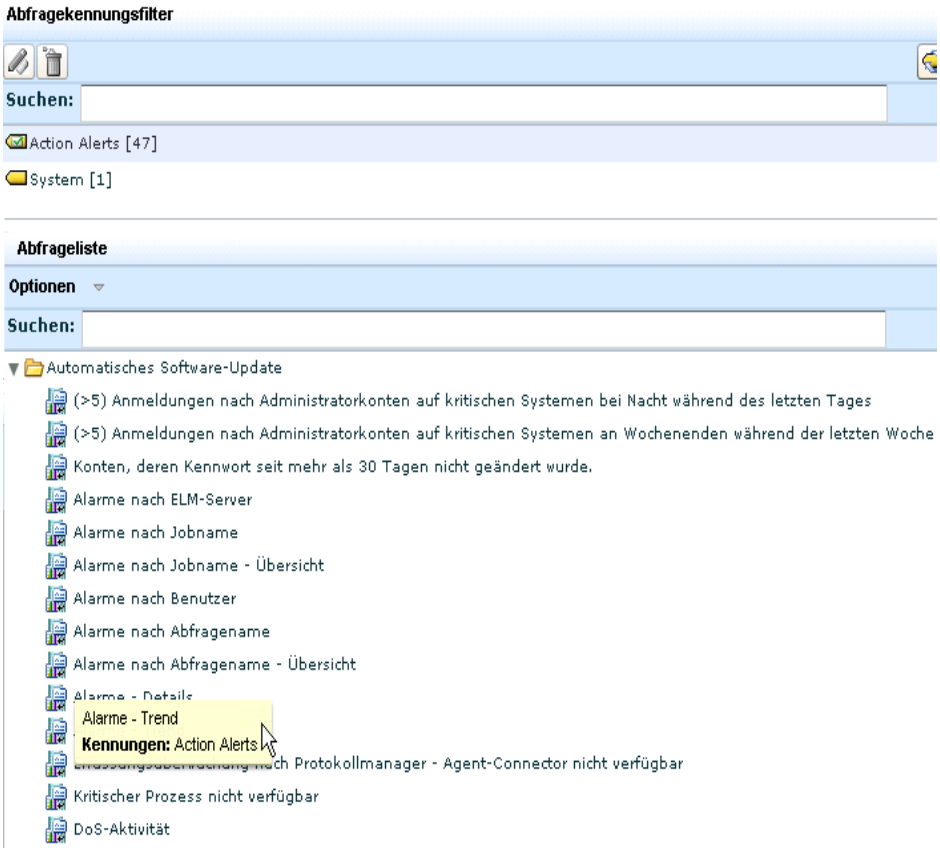
Sie können Aktionsalarme folgendermaßen erstellen:

- Mit dem Assistenten für Aktionsalarme
- Über eine Abfrageanzeige
- Mit einer benutzerdefinierten Abfrage

Planungsoptionen sind ein wichtiger Teil beim Erstellen eines Alarms, die Ihnen die Kontrolle darüber ermöglichen, wie lange und wie häufig Ihr Alarmjob ausgeführt wird.

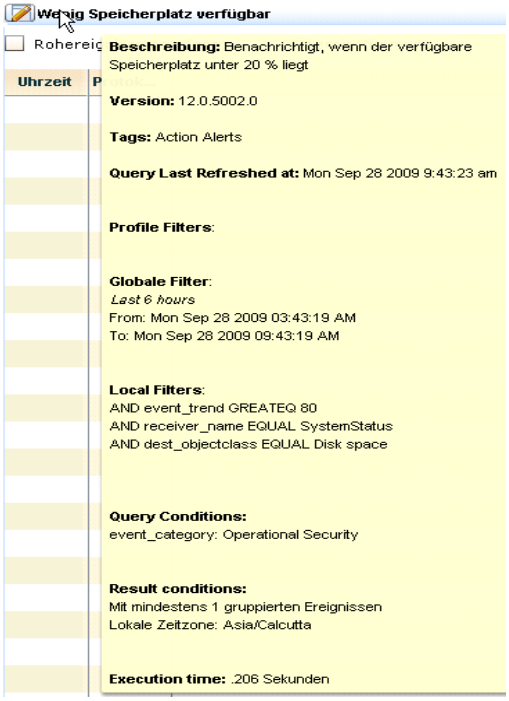
Verwenden von Abfragen mit der Kennung "Aktionsalarme"

CA Enterprise Log Manager bietet eine Reihe von Abfragen mit der Kennung "Aktionsalarme". Um die Liste der Abfragen mit der Kennung "Aktionsalarme" anzuzeigen, klicken Sie auf die Registerkarte "Abfragen und Berichte", dann auf die Unterregisterkarte "Berichte", und wählen Sie die Kennung "Aktionsalarme". Die Abfragen mit dieser Kennung erscheinen in der Abfrageliste. Wenn Sie mit der Maus auf einen Abfragenamen zeigen, werden die zugehörigen Kennungen angezeigt.



Bevor Sie anhand dieser Abfragen Aktionsalarme planen, können Sie weitere Informationen zur Funktion der einzelnen Abfragen abrufen. Um die Beschreibung einer Abfrage wie z. B. "Wenig Speicherplatz verfügbar" und Details dazu anzuzeigen, wählen Sie diese Abfrage aus der Abfrageliste und führen Sie dann den Cursor über den Namen der Abfrage.

Es wird eine Übersicht über die Abfrage eingeblendet, einschließlich einer Beschreibung, ihrer Filter und der Abfragebedingungen.



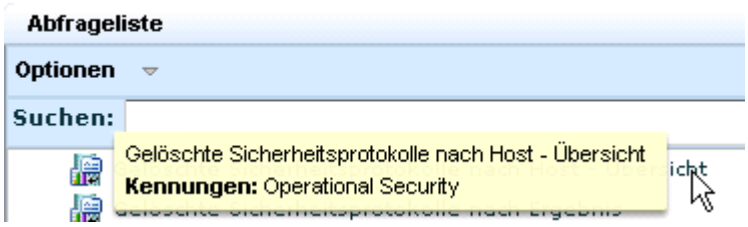
Sie können die Abfrage entweder so, wie sie ist, verwenden, oder Sie können sie unter einem neuen Namen kopieren und sie Ihren Anforderungen anpassen. Beispielsweise können Sie einen Alarm generieren, der ausgegeben wird, wenn der verfügbare Speicherplatz unter 25 % statt 20 % fällt. Sie können basierend auf der vordefinierten Abfrage eine benutzerdefinierte Abfrage erstellen und sie anschließend für Ihren Aktionsalarm auswählen.

Hinweis: Bevor sie die Abfragen mit "Berechtigte Gruppe" oder "Standardkonto" im Titel verwenden, erwägen Sie, Ihre eigenen Schlüsselwerte zur entsprechenden Schlüsselliste hinzuzufügen.

Bestimmen anderer Abfragen für die Verwendung in Alarmen

Es gibt Abfragen, die nicht als Aktionsalarm gekennzeichnet sind, sich aber gut für die Aufnahme in einen geplanten Aktionsalarm eignen, weil sie nur schwerwiegende Ereignisse abrufen.

So ruft beispielsweise "Gelöschte Sicherheitsprotokolle nach Host - Details" alle Ereignisse ab, bei denen die Ereignisaktion "Gelöschte Sicherheitsprotokolle" lautet. Diese Abfrage weist nur die Kennung "Betriebssicherheit" auf.



Die Aktion "Gelöschte Sicherheitsprotokolle" wird in der ELM-Schemadefinition aufgeführt. Die ELM-Schemadefinition definiert die folgenden beiden Ereignisarten mit der Sicherheitsstufe 6, also schwerwiegend.

Kategorie	Klasse	Aktion	Ergebnis	Sicherheitsstufe
Betriebssicherheit	Sicherheitsprotokollaktivität	Sicherheitsprotokoll löschen	Erfolgreich	6
Betriebssicherheit	Sicherheitsprotokollaktivität	Sicherheitsprotokoll löschen	Fehler	6

Es empfiehlt sich, einen Alarm mit dieser Abfrage zu planen.

Weitere Informationen

Ermitteln des einfachen Filters für schwerwiegende Ereignisse (siehe Seite 393)

Anpassen von Abfragen für Aktionsalarme

Alarme benachrichtigen Personen, Prozesse oder Produkte, sobald ein schwerwiegendes Ereignis eintritt. Wenn Sie Abfragen als Grundlage von Alarmen definieren möchten, sollten diese Abfragen Ereignisse mit hoher Sicherheitsstufe erfassen.

Nachdem Sie die schwerwiegenden Ereignisse definiert haben, können Sie Abfragen für die Erfassung dieser schwerwiegenden Ereignisse erstellen. Wenn eine Abfrage nicht existiert, können Sie sie erstellen.

Betrachten Sie folgenden Prozess:

1. Legen Sie die Ereignistypen fest, die in CA als sehr schwerwiegend erkannt werden. Dabei werden Ereignistypen nach Kategorie, Klasse, Aktion und Ergebnis definiert.
2. Legen Sie vordefinierte Abfragen fest, die nur diese Ereignisse erfassen.
3. Legen Sie vordefinierte Abfragen fest, die nur Ereignisse erfassen, die schwerwiegende Ereignisse enthalten, aber auch so angepasst werden können, dass sie ausschließlich schwerwiegende Ereignisse enthalten.
4. Erstellen Sie benutzerdefinierte Abfragen, falls keine vordefinierten Abfragen existieren.
5. Planen Sie Alarme, um diese Abfragen regelmäßig durchzuführen.

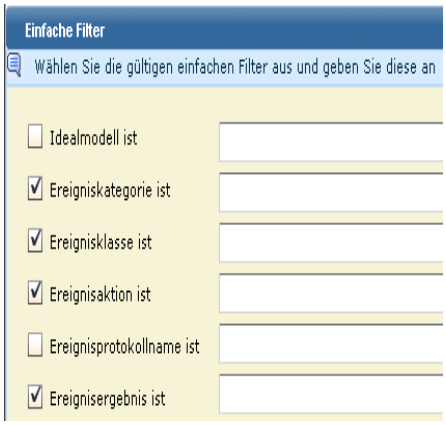
Weitere Informationen

Ermitteln des einfachen Filters für schwerwiegende Ereignisse (siehe Seite 393)
Anpassen von Abfragen zum ausschließlichen Erfassen von schwerwiegenden Ereignissen (siehe Seite 397)
Erstellen von Abfragen zum ausschließlichen Erfassen von schwerwiegenden Ereignissen (siehe Seite 395)

Ermitteln des einfachen Filters für schwerwiegende Ereignisse

Ereignisse weisen verschiedene Schweregrade auf, von einfachen Informationsmeldungen bis hin zu schwerwiegenden Ereignissen. CA weist einen Wert zwischen 2 und 7 zu, um den Schweregrad von Ereignissen basierend auf dem ELM-Schemadefinitionsmodell "Kategorie", "Klasse", "Aktion" und "Ergebnis" einzustufen. Der Schweregrad 7 wird Ereignissen zugewiesen, bei denen das System heruntergefahren wurde. Der Schweregrad 6 wird Ereignissen zugewiesen, bei denen die Sicherheit in hohem Maße gefährdet ist oder die der unmittelbaren Aufmerksamkeit bedürfen.

Falls Sie Ihre eigenen Abfragen erstellen oder vordefinierte Abfragen für die Verwendung in Alarmen anpassen möchten, empfiehlt es sich, die Definitionen des ELM-Schemadefinitionsmodells für schwerwiegende Ereignistypen zu überprüfen. Die Modelldefinition ist die Grundlage für einfache Filter. Sie können Abfragen erstellen, die Ereignisse basierend auf Ihren Spezifikationen für Ereignisklasse, Ereignisaktion und Ereignisergebnis erfassen.



So definieren Sie einfache Filter für schwerwiegende Ereignisse:

1. Klicken Sie auf die Verknüpfung "Hilfe".
2. Erweitern Sie "ELM-Schemadefinition", und wählen Sie "Zuweisung der Sicherheitsebene".
3. Kopieren Sie die Tabelle in ein Tabellenkalkulationsprogramm, und sortieren Sie die Sicherheitsebene von hoch zu niedrig.

   Die daraus resultierende Tabelle listet die Ereignistypen auf, wobei die schwerwiegendsten Ereignisse basierend auf der CA-Zuweisung der Sicherheitsebenen am Anfang stehen.

   Beispiel: Ihre Ergebnisse reflektieren die aktuellen CEG-Definitionen.

Kategorie	Klasse	Aktion	Ergebnis	Sicherheitsstufe
Betriebssicherheit	Systemaktivität	System herunterfahren	Erfolgreich	7
Betriebssicherheit	Systemaktivität	System herunterfahren	Fehler	7
Konfigurationsverwaltung	Konfigurationsverwaltung	Konfigurationsfehler	Erfolgreich	6
Datenzugriff	Objektverwaltung	Zugriffsdatei erstellen	Erfolgreich	6
Hostsicherheit	Antivirusaktivität	Scan-Fehler	Erfolgreich	6
Hostsicherheit	Antivirusaktivität	Virus bereinigen	Fehler	6
Hostsicherheit	Antivirusaktivität	Virus entdeckt	Erfolgreich	6
Hostsicherheit	Antivirusaktivität	Virus in Quarantäne	Fehler	6
Hostsicherheit	IDS-/IPS-Aktivität	Signaturverletzung	Erfolgreich	6
Netzwerksicherheit	Aktivität bei Signaturverletzung	Signaturverletzung	Erfolgreich	6
Betriebssicherheit	Systemaktivität	Systemstart	Fehler	6
Betriebssicherheit	Sicherheitsprotokollaktivität	Sicherheitsprotokoll löschen	Erfolgreich	6
Betriebssicherheit	Sicherheitsprotokollaktivität	Sicherheitsprotokoll löschen	Fehler	6
Systemzugriff	Authentifizierungsaktivität	Authentifizierungs-Fallback	Fehler	6

Kategorie	Klasse	Aktion	Ergebnis	Sicherheitsstufe
Systemzugriff	Authentifizierungsaktivität	Authentifizierungsstart	Fehler	6

Erstellen von Abfragen zum ausschließlichen Erfassen von schwerwiegenden Ereignissen

Sie können eine neue Abfrage erstellen, wenn Sie keine vordefinierte Abfrage für die Ereignistypen finden können, über die sie informiert werden möchten. Betrachten Sie die folgenden schwerwiegenden Ereignistypen:

Kategorie	Klasse	Aktion	Ergebnis	Sicherheitsstufe
Hostsicherheit	Antivirusaktivität	Virus in Quarantäne	Fehler	6
Hostsicherheit	IDS-/IPS-Aktivität	Signaturverletzung	Erfolgreich	6
Netzwerksicherheit	Aktivität bei Signaturverletzung	Signaturverletzung	Erfolgreich	6

Beispiel: Erstellen von Abfragen zum ausschließlichen Erfassen einer fehlgeschlagenen Virusquarantäne

Sie möchten beispielsweise über fehlgeschlagene Virusquarantäneaktionen informiert werden. Möglicherweise erscheint das Schlüsselwort "Quarantäne" nicht in der Abfrageliste. Ist dies der Fall, können Sie die erforderliche Abfrage erstellen und anschließend einen Alarm planen, der die Abfrage ausführt.

So erstellen Sie eine Abfrage zum Erfassen von fehlgeschlagenen Virusquarantäneaktionen:

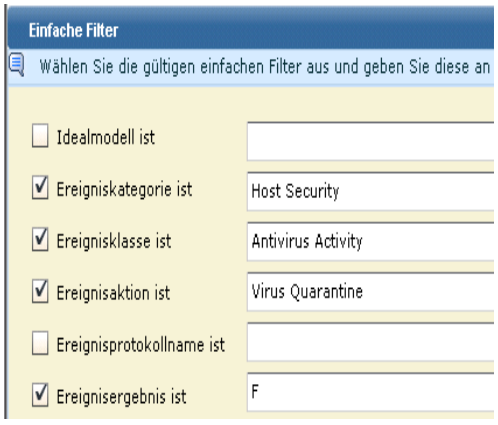
1. Klicken Sie auf "Abfragen und Berichte".
2. Wählen Sie unter "Abfragelistenoptionen" die Option "Neu".

   Der Assistent für das Erstellen von Abfragen wird angezeigt, auf dem der Schritt "Details" angezeigt wird.
3. Geben Sie einen Namen ein.

   Beispiel: Geben Sie "Alarm: Fehlgeschlagene Virusquarantäne" ein.
4. Geben Sie eine benutzerdefinierte Kennung ein.

   Beispiel: Geben Sie "Virusquarantäne" ein.
5. Klicken Sie auf den Schritt "Abfragespalten", und fügen Sie die gewünschten Spalten hinzu.
6. Klicken Sie auf den Schritt "Abfragefilter".
7. Geben Sie einen einfachen Filter basierend auf dem CEG-Eintrag für das Ereignis ein.

   Beispiel: Wählen Sie als Kategorie "Hostsicherheit", als Klasse "Antivirusaktivität", als Aktion "Virusquarantäne" und als Ergebnis "F" (fehlgeschlagen).



8. Wählen Sie den Schritt "Ergebnisbedingungen", und wählen Sie im Dropdown-Feld "Vordefinierte Bereiche" die Option "Letzte 5 Minuten", um eine zeitnahe Benachrichtigung zu gewährleisten.
9. Klicken Sie auf "Speichern und schließen".

Anpassen von Abfragen zum ausschließlichen Erfassen von schwerwiegenden Ereignissen

Vordefinierte Abfragen, die nicht als Aktionsalarme gekennzeichnet sind, dienen zum Erstellen von Berichten. Berichte können Daten für Ereignisse aller Schweregrade enthalten. Sie können ausgewählte Abfragen so anpassen, dass ausschließlichschwerwiegende Ereignisse erfasst werden. Wählen Sie hierzu eine Abfrage, die schwerwiegende Ereignisse zusammen mit weniger schwerwiegenden Ereignissen erfasst, kopieren Sie sie, fügen Sie Filter hinzu, so dass nur die schwerwiegenden Ereignisse erfasst werden, und speichern Sie sie, um sie in einem Alarm zu verwenden.

Legen Sie, bevor Sie beginnen, das Tabellenblatt bereit, auf dem die Definitionen für schwerwiegende Ereignisse aufgelistet werden. Dieses Beispiel basiert auf den folgenden CEG-Informationen:

Kategorie	Klasse	Aktion	Ergebnis	Sicherheitsstufe
Betriebssicherheit	Systemaktivität	System herunterfahren	Erfolgreich	7
Betriebssicherheit	Systemaktivität	System herunterfahren	Fehler	7

Die angepasste Abfrage erfasst Ereignisse für "Herunterfahren" und "Systemstart".

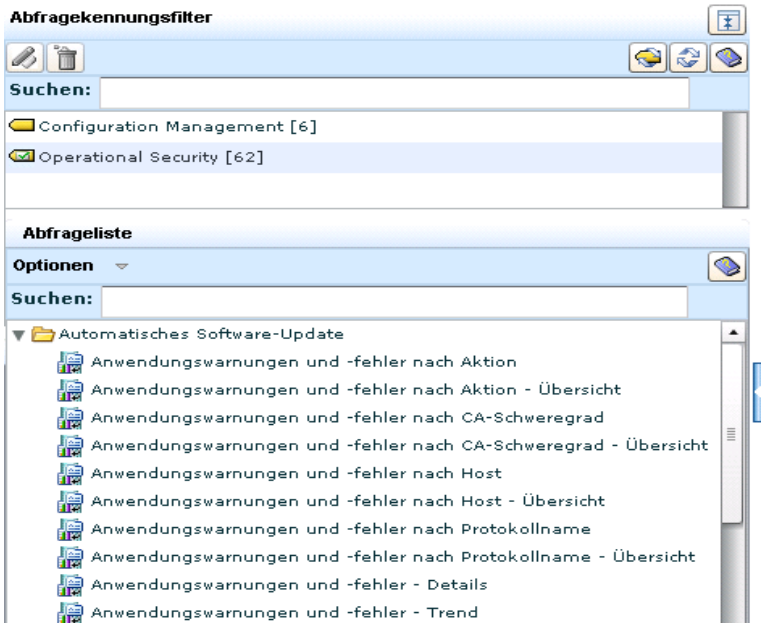
So passen Sie Abfragen zum ausschließlichen Erfassen von schwerwiegenden Ereignissen an:

1. Klicken Sie auf die Registerkarte "Abfragen und Berichte".
2. Wählen Sie einen Abfragekennungsfilter, der der Kategorie eines schwerwiegenden Ereignisses entspricht.

   Beispiel: Wählen Sie "Betriebssicherheit".

3. Suchen Sie auf der Abfrageliste nach Abfragen, deren Namen Schlüsselwörter aus "Klasse" oder "Aktion" für den entsprechenden Ereignistyp enthalten.

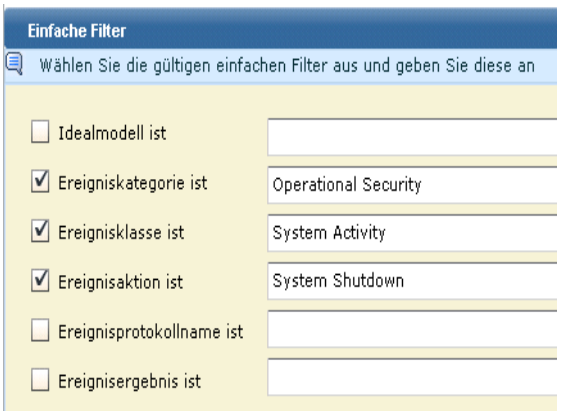
   Beispiel: Die Schlüsselwörter "System" und "Herunterfahren" tauchen in Abfragen auf, die mit "Starten oder Herunterfahren des Systems nach Host" beginnen.



4. Kopieren Sie die Abfrage "Starten oder Herunterfahren des Systems nach Host - Detail". Markieren Sie die Abfrage, und wählen Sie aus der Dropdown-Liste "Optionen" die Option "Kopieren".
5. Klicken Sie auf "Abfragefilter", und vergleichen Sie die Standardwerte mit den Tabelleneinträgen für schwerwiegende Ereignistypen.

   Für diese Abfrage ist nur "Betriebssicherheit" markiert.
6. In der Tabelle finden Sie Werte, die Sie unter "Klasse" oder "Aktion" eingeben können.

   Wählen Sie beispielsweise "Systemaktivität" als Klasse und "System herunterfahren" als Aktion.



7. Legen Sie auf der Registerkarte "Erweiterte Filter" fest, ob eine Modifikation erforderlich ist.

   Klicken Sie auf jeder Zeile auf "Löschen", wenn der Filter "Ereignisaktion" gleich "Systemstart" ist oder "Herunterfahren" für diese angepasste Abfrage nicht zutreffend ist.
8. Ersetzen Sie ihn durch einen Filter für das Ergebnis.

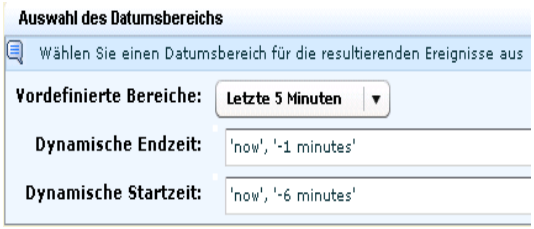
   Beispiel: Erstellen Sie einen Filter, bei dem "Ereignisergebnis" gleich "Erfolgreich" oder "Fehler" ist.

9. Klicken Sie auf "Details", und geben Sie der Abfrage einen Namen, an dem Sie erkennen können, dass sie für einen Alarm verwendet werden soll.

   Beispiel: Geben Sie als Namen "Alarm: Herunterfahren des Systems nach Host - Detail" ein. Ändern Sie die Beschreibung entsprechend.

10. Klicken Sie auf "Ergebnisbedingungen". Bei schwerwiegenden Bedingungen sollten Sie die Abfrage häufig durchführen.

    Beispiel: Wählen Sie den vordefinierten Bereich "Letzte 5 Minuten", um die Abfrage nach diesem schwerwiegenden Ereignis alle 5 Minuten durchzuführen.



11. Klicken Sie auf "Speichern".

    Sie können mit dieser Abfrage einen Alarm erstellen, um Personen, Produkte oder Prozesse über das erfolgreiche oder fehlgeschlagene Herunterfahren des Systems zu informieren. (Die Produktbenachrichtigung erfolgt über SNMP-Traps. Die Prozessbenachrichtigung erfolgt über die IT PAM-Ereignis-/Alarmausgabe.)

Auswählen von Abfragen zur Änderung

Sie können ausgewählte vordefinierte Abfragen zur Verwendung mit Alarmen ändern. Um die Abfrage anzupassen, fügen Sie den einfachen Filter basierend auf der CEG-Analyse hinzu. Setzen Sie den vordefinierten Bereich unter "Auswahl des Datumsbereichs" auf "Letzte 5 Minuten", um eine zeitnahe Benachrichtigung zu garantieren. Hier einige Beispiele:

Abfrage für Fehler bei erfolgreicher Konfiguration

1. Kopieren Sie "Konfigurationsfehler - Details".

   Diese Abfrage gibt erfolgreiche und fehlgeschlagene Ereignisse zurück. Es werden nur die erfolgreichen Ereignisse benötigt.

2. Stellen Sie den einfachen Filter folgendermaßen ein:

Kategorie	Klasse	Aktion	Ergebnis	Sicherheitsstufe
Konfigurationsverwaltung	Konfigurationsverwaltung	Konfigurationsfehler	Erfolgreich	6

3. Speichern als Alarm: Fehler bei erfolgreicher Konfiguration

Abfrage für die erfolgreiche Erstellung der Zugriffsdatei

1. Kopieren Sie "Datenveränderungen - Details".

   Diese Abfrage ruft alle Datenzugriffsaktionen ab.

2. Stellen Sie den einfachen Filter folgendermaßen ein:

Kategorie	Klasse	Aktion	Ergebnis	Sicherheitsstufe
Datenzugriff	Objektverwaltung	Zugriffsdatei erstellen	Erfolgreich	6

3. Speichern als Alarm: Erfolgreiche Erstellung der Zugriffsdatei

Abfrage für Antivirus-Scan-Fehler

1. Kopieren Sie "Virenaktivität nach Aktion"

   Diese Abfrage filtert alle Antivirus-Host-Sicherheitsaktionen.

2. Die folgenden Definitionen können als Anhaltspunkte dienen:

Kategorie	Klasse	Aktion	Ergebnis	Sicherheitsstufe
Hostsicherheit	Antivirusaktivität	Scan-Fehler	Erfolgreich	6

3. Definieren Sie den einfachen Filter folgendermaßen:

4. Speichern als Alarm: Virenscan fehlgeschlagen

Abfrage für fehlgeschlagene Virenbereinigung

Sie können die vordefinierte Abfrage "Virenerkennungen oder -bereinigungen - Details" verwenden, um beide Aktionen (erfolgreich oder fehlgeschlagen) zu erfassen. Dies genügt unter Umständen für Ihre Anforderungen. Optional können Sie zwei eigene Abfragen auf Grundlage dieser Abfrage erstellen, mit denen Sie das Ergebnis entsprechend der CEG-Tabelle für schwerwiegende Ereignisse festlegen.

1. Kopieren Sie "Virenerkennungen oder -bereinigungen - Details".
2. Erstellen Sie einen einfachen Filter für das Ergebnis "Fehlgeschlagen".

Kategorie	Klasse	Aktion	Ergebnis	Sicherheitsstufe
Hostsicherheit	Antivirusaktivität	Virus bereinigen	Fehler	6

3. Entfernen Sie den erweiterten Filter.
4. Speichern als Alarm: Virenbereinigung fehlgeschlagen

Abfrage für das erfolgreiche Erkennen eines Virus

Sie können die vordefinierte Abfrage "Virenerkennungen oder -bereinigungen - Details" verwenden, um beide Aktionen (erfolgreich oder fehlgeschlagen) zu erfassen. Dies genügt unter Umständen für Ihre Anforderungen. Optional können Sie zwei eigene Abfragen auf Grundlage dieser Abfrage erstellen, mit denen Sie das Ergebnis entsprechend der CEG-Tabelle für schwerwiegende Ereignisse festlegen.

1. Kopieren Sie "Virenerkennungen oder -bereinigungen - Details".
2. Erstellen Sie einen einfachen Filter für das Ergebnis "Erfolg" beim Erkennen von Viren.

Kategorie	Klasse	Aktion	Ergebnis	Sicherheitsstufe
Hostsicherheit	Antivirusaktivität	Virus entdeckt	Erfolgreich	6

3. Entfernen Sie den erweiterten Filter.
4. Speichern als Alarm: Virus erkannt.

Überlegungen zu Aktionsalarmen

Sie können die Ergebnisse der von CA Enterprise Log Manager ausgehenden Aktionsalarme ohne besondere Konfiguration anzeigen. Zusätzlich kann ein Aktionsalarm an folgende Ziele gesendet werden:

- RSS-Feed
- E-Mail-Empfänger
- SNMP-Trap-Ziele wie CA Spectrum oder CA NSM
- einen IT PAM-Ereignis-/Alarmausgabeprozess

Administratoren konfigurieren diese Ziele auf der Registerkarte "Verwaltung" und der Unterregisterkarte "Services" unter "Globale Konfiguration" bzw. unter "Globale Service-Konfiguration: Berichtsserver".

Vergewissern Sie sich, dass diese Ziele wie folgt konfiguriert wurden, bevor Sie einen Alarm planen.

- Wenn Sie den Feed-Reader verwenden möchten, stellen Sie sicher, dass das Kontrollkästchen für "Zum Anzeigen von Aktionsalarmen ist eine Authentifizierung erforderlich" in der "Globalen Konfiguration" unmarkiert ist.

  Der RSS-Feed-URL folgt, wobei *elmhostname* der Hostname des CA Enterprise Log Manager-Servers ist:

  ```
  https://{elmhostname}:5250/spin/calm/getActionQueryRssFeeds.csp
  ```

- Wenn Alarme an E-Mail-Empfänger gesendet werden sollen, muss der Abschnitt "E-Mail-Einstellungen" unter "Globale Service-Konfiguration: Berichtsserver" konfiguriert werden.
- (Optional) Wenn Alarme an SNMP-Ziele gesendet werden sollen, muss der Abschnitt "SNMP-Konfiguration" unter "Globale Service-Konfiguration: Berichtsserver" konfiguriert werden.
- Wenn Alarme an den CA IT PAM-Ereignis-/Alarmausgabeprozess gesendet werden sollen, muss der Abschnitt "IT PAM" unter "Globale Service-Konfiguration: Berichtsserver" konfiguriert werden. (Der einzige für Alarme nicht erforderliche Wert ist der für den Prozess mit dynamischen Werten.)

Beachten Sie Folgendes, wenn Sie Ergebnisbedingungen für einen Aktionsalarm festlegen:

- Verwenden Sie für die vordefinierten Bereiche die voreingestellte dynamische Start- und Endzeit.
  - Der vordefinierte Bereich "Letzte 5 Minuten" ist auf die dynamische Endzeit 'jetzt', '-2 Minuten' und auf die dynamische Startzeit 'jetzt', '-7 Minuten' eingestellt. Durch diesen Standardbereich und die anderen vordefinierten Zeitbereiche wird ein angemessener Zeitraum für die Speicherung der Ereignisse in der Datenbank berücksichtigt.

    Hinweis: Ändern Sie die dynamische Endzeit nicht in *'jetzt'* oder *'jetzt', '-1 Minute'*. Eine derartige Änderung des vordefinierten Wertes kann dazu führen, dass unvollständige Daten angezeigt werden, wenn die URL vom Ziel aus aufgerufen wird. Wenn die Ereignisanzahl mit einem der Werte identisch ist, kann die unter der URL angezeigte Anzahl niedriger als die in CA Enterprise Log Manager angezeigte Anzahl sein.
- Verlängern Sie die dynamische Endzeit, wenn mit der Standardeinstellung unvollständige Daten angezeigt werden. Stellen Sie sie beispielsweise auf 'jetzt', '-10 Minuten' ein.

Beachten Sie Folgendes, wenn Sie einen Aktionsalarmplan erstellen:

- Das Wiederholungsintervall gibt die Häufigkeit an, mit der die Abfrage durchgeführt wird. Ein Wiederholungsintervall von 5 Minuten bedeutet daher, dass eine Abfrage alle fünf Minuten bzw. 12mal pro Stunde durchgeführt wird. Es wird nur ein Aktionsalarm generiert, wenn bei der Ausführung der Abfrage Ergebnisse zurückgegeben werden.
- Legen Sie das Wiederholungsintervall in Abhängigkeit davon fest, wie rasch Sie ggf. reagieren müssen, wenn die Abfrage ein Ergebnis liefert.
  - Wenn Sie sofortige Maßnahmen ergreifen müssen, um den Fehler zu beheben, stellen Sie ein kurzes Wiederholungsintervall bzw. eine hohe Häufigkeit ein, damit Sie so bald wie möglich benachrichtigt werden können.
  - Wenn es sich um einen Fehler handelt, von dem Sie Kenntnis erhalten möchten, bei dem aber keine Maßnahmen erforderlich sind, stellen Sie ein langes Wiederholungsintervall, also eine niedrige Häufigkeit, ein.
- Falls der CA Enterprise Log Manager-Server nicht mit dem NTP-Server synchronisiert ist, sollten Sie kein kurzes Wiederholungsintervall, etwa eine Wiederholung alle fünf Minuten, einstellen.

  Wichtig! Die Zeit des CA Enterprise Log Manager-Servers muss mit dem NTP-Server synchronisiert sein, um sicherzustellen, dass vollständige Ergebnisse zurückgegeben werden, wenn für die Abfrage eine hohe Ausführungshäufigkeit eingestellt ist.

Beachten Sie die folgenden Filteroptionen:

- Falls die für die einbezogenen Abfragen definierten Filter verwendet werden sollen, sind keine Maßnahmen erforderlich.
- Falls weitere Filter für die in einem Alarm enthaltenen Abfragen angewendet werden sollen, definieren Sie diese im Schritt "Alarmfilter".
- Falls derselbe Filtersatz auf mehrere Alarmjobs angewendet werden soll, verwenden Sie ein Profil.

Bevor Sie Schwellenwerte für Aktionsalarme auf einem CA Enterprise Log Manager-Berichtsserver konfigurieren, bedenken Sie Folgendes:

- Um den RSS-Feed in einem vernünftigen Umfang zu halten, stellen Sie eine maximal erlaubte Anzahl für Alarme ein. Je kürzer das Wiederholungsintervall für aktivierte Alarme, desto rascher liefert der Feed Meldungen, wenn die Abfrage bzw. die Abfragen zu Ergebnissen führt bzw. führen.
- Um sicherzustellen, dass der RSS-Feed Alarme nicht länger aufbewahrt, als die entsprechenden Informationen von Interesse sind, geben Sie ein maximales Alter in Tagen für die älteste aufzubewahrende Aufzeichnung ein.
- Überlegen Sie, wie oft Sie den RSS-Feed auf Alarme prüfen möchten. Dies hilft Ihnen dabei, zu planen, wie lange die Aufzeichnungen aufbewahrt werden sollen.
- Wenn Sie möchten, dass der RSS-Feed die neuesten Ergebnisse aller Jobs jederzeit anzeigt, konfigurieren Sie die Aufbewahrungswerte so, dass selten ausgeführte Alarme nicht gelöscht werden, weil sie älter als oft durchgeführte Alarme sind, die die Warteschlange bis zur Kapazitätsgrenze auffüllen.

Weitere Informationen:

Konfigurieren des Aufbewahrungszeitraums für Aktionsalarme (siehe Seite 514)
Beispiel: Einen Aktionsalarm für "Wenig Speicherplatz verfügbar" erstellen. (siehe Seite 503)

Arbeiten mit CA IT PAM Ereignis-/Alarmausgabeprozessen

Bei der Arbeit mit CA IT PAM-Ereignis-/Alarmausgabeprozessen, die in CA Enterprise Log Manager integriert sind, werden folgende Aufgaben miteinander kombiniert:

- Importieren des Beispiel-Ereignis-/Alarmausgabeprozesses
- Erstellen von Ereignis-/Alarmausgabeprozessen in CA IT PAM, die den Anforderungen für die Integration entsprechen
- Konfigurieren der IT PAM-Integration und Festlegen des Standardereignis-/Alarmausgabeprozesses
- Ausführen des Ereignis-/Alarmausgabeprozesses über die ausgewählten Abfrageergebnisse
- Planen von Alarmen, die einen CA IT PAM-Prozess pro Zeile ausführen
- Planen von Alarmen, die einen CA IT PAM-Prozess pro Abfrage ausführen

Weitere Informationen

Importieren des Ereignis-/Alarmausgabe-Beispielprozesses (siehe Seite 416)
Richtlinien zum Erstellen eines Ereignis-/Alarmausgabeprozesses (siehe Seite 424)
Beispiel: Ausführen eines Ereignis-/Alarmausgabeprozesses mit ausgewählten Abfrageergebnissen (siehe Seite 431)
Beispiel: Senden eines Alarms, durch den ein IT PAM-Prozess pro Zeile ausgeführt wird (siehe Seite 437)
Beispiel: Senden eines Alarms, der einen IT PAM-Prozess pro Abfrage ausführt (siehe Seite 442)

Info zu CA IT PAM Ereignis-/Alarmausgabeprozessen

CA Enterprise Log Manager erkennt Ereignisse, die einen Eingriff erfordern. Sie können Alarme generieren, sobald unerwünschte Ereignisse auftreten. Durch die Integration mit CA IT PAM kann ein Alarm einen Ereignis-/Alarmausgabeprozess ausführen. Ereignis-/Alarmausgabeprozesse lösen erforderliche Hilfsmaßnahmen bei anderen Produkten aus. Ereignis-/Alarmausgabeprozesse sind also CA IT PAM-Prozesse, die andere Produkte anweisen, eine bestimmte Aktion für bestimmte Objekte auszuführen.

CA Enterprise Log Manager, CA IT PAM und Drittanbieterprojekte arbeiten zusammen, um Ihre Umgebung zu schützen. CA Enterprise Log Manager automatisiert die Erkennung unerwünschter Ereignisse, und der IT PAM Ereignis-/Alarmausgabeprozess veranlasst andere Produkte zu entsprechenden Reaktionen.

Im Rahmen der Integration wird die Verbindung mit dem CA IT PAM-Server konfiguriert und der auszuführende Prozess sowie die Prozessparameter mit ihren Standardwerten festgelegt.

Die Ausführung des CA IT PAM-Prozesses kann nach Bedarf über die Anzeige eines Abfrageergebnisses (Zeile) oder über geplante Alarme erfolgen. In beiden Fällen können Parameter wie beispielsweise Zusammenfassung und Beschreibung angepasst werden, um dem Zielprodukt des CA IT PAM-Prozesses unterstützende Informationen zu liefern.

Weitere Informationen

Architektur zur Unterstützung der CA IT PAM-Integration (siehe Seite 409)
Arbeiten mit Ereignis-/Alarmausgabeprozessen (siehe Seite 409)
Funktionsweise der CA IT PAM-Integration (siehe Seite 411)
Beispiel: Datenfluss für einen Ereignis-/Alarmausgabeprozess (siehe Seite 414)

Architektur zur Unterstützung der CA IT PAM-Integration

Sie benötigen die folgenden Netzwerkkomponenten, um einen CA IT PAM-Ereignis-/Alarmausgabeprozess von einem Alarm aus auszuführen:

- Eine funktionstüchtige CA Enterprise Log Manager-Umgebung, zum Beispiel:
  - Agenten mit Connectors, die Rohereignisse auf Ereignisquellen erfassen
  - CA Enterprise Log Manager-Quellserver für Protokolldateien (agentenbasiert), die die Rohereignisse eingrenzen und an Berichtsserver senden
  - CA Enterprise Log Manager-Berichtsserver, die geplante Alarme und Bedarfsabfragen verarbeiten
- Ein CA IT Process Automation Manager r2.1 (CA IT PAM)-Server, auf dem Prozesse konfiguriert sind, die ein anderes Produkt zur Durchführung einer Routinenüberarbeitungsaktion aufrufen
- Ein Server mit einem Produkt, das vom CA IT PAM-Prozess verwendet wird, zum Beispiel ein Server mit einem Helpdesk-Produkt

Arbeiten mit Ereignis-/Alarmausgabeprozessen

Im Folgenden erhalten Sie einen Überblick über den Ablauf bei der Nutzung eines CA IT PAM-Ereignis-/Alarmausgabeprozsesses:

1. Legen Sie fest, ob Sie eine CA IT PAM-Integration mit oder ohne den Beispielprozess erstellen möchten. Wenn Sie den Beispielprozess verwenden, werden Ergebnisse sofort angezeigt. Sie können die Aktualisierung Ihres eigenen Prozesses verschieben, bis Sie sich mit den Integrationsergebnissen vertraut gemacht haben. Für die Verwendung des Beispielprozesses benötigen Sie CA Service Desk.
2. Führen Sie eine oder beide der folgenden Aktionen aus:
   - Importieren Sie den Beispielprozess und legen Sie die CA ServiceDesk-Verbindungsparameter fest.
   - Erstellen Sie Ereignis-/Alarmausgabeprozesse, die die Anforderungen der CA Enterprise Log Manager-Integration erfüllen.
3. Sammeln Sie über den Beispielprozess oder den von Ihnen erstellten Prozess Details zur CA IT PAM-Integration.
4. Konfigurieren Sie die CA IT PAM-Integration für die Ereignis-/Alarmausgabe.

5. Stellen Sie sicher, dass die Benutzer, die den Ereignis-/Alarmprozess im Drittanbieterprodukt überwachen, über ein Benutzerkonto in CA Enterprise Log Manager verfügen und ihre Anmeldeinformationen kennen. Sie können diesen Konten die Rolle eines Auditors zuweisen.

   Hinweis: Wenn sich Benutzer anmelden, können sie diese Seite und die entsprechenden Abfrageergebnisse nur anzeigen.

6. Vorbereitung für die Automatisierung eines Ereignis-/Alarmausgabeprozesses:

   a. Ermitteln Sie die Abfrage/n, die Daten zurückgeben, auf die das Drittanbieterprodukt entsprechend des konfigurierten CA IT PAM-Prozesses reagieren kann.

   b. Wenn die Abfrage eine Schlüsselliste verwendet, stellen Sie sicher, dass die Schlüsselliste die erforderlichen Werte enthält.

   c. Führen Sie den Ereignis-/Alarmausgabeprozess anhand der Abfrageergebnisse durch, und stellen Sie sicher, dass der Prozess erfolgreich durchgeführt wird.

7. Planen Sie einen Aktionsalarm. Halten Sie sich dabei an die angegebene Vorgehensweise und die folgenden Richtlinien.

   a. Beim Schritt "Alarmauswahl":

      - Geben Sie einen Jobnamen ein.
      - Vergewissern Sie sich, dass unter "Auswahltyp" die Auswahl "Abfragen" aktiviert ist.
      - Wählen Sie die Abfrage(n), die Sie bei der Planung festgelegt haben.

   b. Wählen Sie im Schritt "Ziel" die Registerkarte "IT PAM-Prozess", und legen Sie die Details für die Ereignis-/Alarmausgabe wie folgt fest:

      - Wählen Sie die Abfragen, auf denen der Alarm beruhen soll.
      - Legen Sie fest, ob der Prozess einmal pro Abfrage durchgeführt werden soll, die Ergebnisse zurückgibt, oder einmal pro zurückgegebener Zeile.
      - Legen Sie die Parameterwerte für den IT PAM-Prozess fest. Sie können für die Zusammenfassungs- und Beschreibungsparameterwerte nur Feldwerte und Text einfügen, wenn Sie den Prozess pro Zeile ausführen.

   c. Legen Sie die Details für die verbleibenden Schritte ähnlich wie für andere zu planende Aktionsalarme fest. Speichern Sie anschließend, und schließen Sie den Assistenten.

8. Überwachen Sie die Ergebnisse:
   a. Überprüfen Sie, ob die Liste "Aktionsalarmjobs" diesen Job enthält.
   b. Überwachen Sie selbstüberwachende Ereignisse und Ereignisbenachrichtigungsaktionen, um zu überprüfen, ob der IT PAM-Prozess erfolgreich war.
   c. (Optional) Melden Sie sich beim Drittanbieterprodukt an, das auf die Ereignis-/Alarmausgabeinformation von CA Enterprise Log Manager geantwortet hat, die vom IT PAM-Prozess übergeben wurde.

Weitere Informationen

Importieren des Ereignis-/Alarmausgabe-Beispielprozesses (siehe Seite 416)
Richtlinien zum Erstellen eines Ereignis-/Alarmausgabeprozesses (siehe Seite 424)
Beispiel: Ausführen eines Ereignis-/Alarmausgabeprozesses mit ausgewählten Abfrageergebnissen (siehe Seite 431)
Entwerfen von Ereignisabfragen, die an den Ereignis-/Alarmausgabeprozess zu senden sind (siehe Seite 435)
Festlegen von Benachrichtigungszielen (siehe Seite 496)
Beispiel: Senden eines Alarms, durch den ein IT PAM-Prozess pro Zeile ausgeführt wird (siehe Seite 437)

Funktionsweise der CA IT PAM-Integration

Gehen Sie von folgender Konfiguration aus:

- Sie haben CA IT PAM auf der Konfigurationsseite für den Berichtsserver eingerichtet und festgelegt, dass der Ereignis-/Alarmausgabeprozess ausgeführt werden soll.
- Sie haben einen Alarm mit dem Ziel "CA IT PAM" geplant, und festgelegt, dass der Prozess einmal pro Zeile ausgeführt werden soll. Für Parameter, die die Eingabe von Anweisungen für Übersicht und Beschreibung zulassen, haben Sie Anweisungen eingegeben, die CEG-Felder enthalten.
- Sie haben einen weiteren Alarm mit dem Ziel "CA IT PAM" geplant, und festgelegt, dass der Prozess einmal pro Abfrage ausgeführt werden soll. Für Parameter, die die Eingabe von Anweisungen für Übersicht und Beschreibung zulassen, haben Sie einen Text eingegeben.

An dem gesamten Prozess sind Aktionen mehrerer Quellen beteiligt:

- Die Erstellung von Rohereignissen durch Ereignisquellen
- Die Sammlung und Verfeinerung von Ereignissen durch CA Enterprise Log Manager
- Die Alarmgenerierung, wenn verfeinerte Ereignisse den Abfragekriterien von CA Enterprise Log Manager entsprechen
- Das Versenden der Ereignis- und Alarmausgabe von CA Enterprise Log Manager an CA IT PAM
- Das Ausführen des konfigurierten Ereignis-/Alarmausgabeprozesses von CA IT PAM auf einem Drittanbietersystem
- Eine der folgenden:
  - Eine Auswertung der Daten durch einen Benutzer des Drittanbietersystems, der über die entsprechende Aktion entscheidet und diese durchführt.
  - Die automatisierte Antwort dieses Drittanbietersystems auf die auftretenden Ereignisse.

Übersicht über den Prozess:

1. Ereignisquellen generieren Rohereignisse.
2. Agents erfassen einige dieser Rohereignisse basierend auf deren Connectors und übermitteln die Rohereignisse an einen Erfassungsserver.
3. Der Erfassungsserver normalisiert und klassifiziert die Rohereignisse und übermittelt die verfeinerten Ereignisse an einen Berichtsserver.

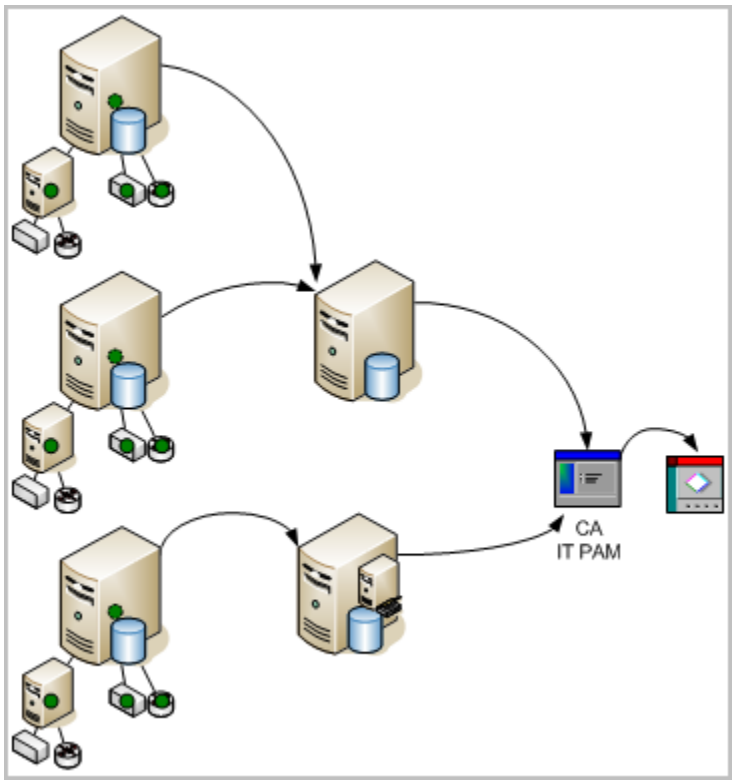
   Wenn beispielsweise in einem beliebigen System eine Konfiguration geändert wird, wird ein Protokoll erstellt und als Konfigurationsänderung klassifiziert. Das Ereignis erfasst den Zeitpunkt der Änderung, den Host, auf dem die Änderung durchgeführt wurde, den Benutzer, der die Änderung ausgeführt hat, und das Ergebnis des Änderungsversuchs.
4. Der Berichtsserver führt die Abfragen aus, die für jeden geplanten Alarm ausgewählt wurden.

5. Wenn die verfeinerten Ereignisse den Abfragekriterien entsprechen, generiert der Berichtsserver einen Alarm und übermittelt die folgenden Daten an CA IT PAM:
   - Alarmdetails
     - Angezeigte Prozessparameter und ihre Werte
     - CEG-Felder, die für nicht angezeigte Prozessparameter versendet wurden
   - Ereignisdetails
     - Pro Zeile werden Ereignisdetails durch die Einträge in den Feldern angegeben, die für Zusammenfassung und Beschreibung zur Verfügung stehen. Hier beschreiben Benutzer das Ereignis mit den CEG-Feldvariablen, aus der sich die für den Alarm ausgewählte Abfrage zusammensetzt.
     - Pro Abfrage werden Ereignisdetails durch eine URL zur CA Enterprise Log Manager-Seite angegeben. Hier werden dann die Ereignisdetails pro Zeile angegeben.
6. Wenn der Versendevorgang erfolgreich abgeschlossen wurde, setzt CA IT PAM die Verarbeitung so fort, wie sie im konfigurierten Ereignis-/Alarmausgabeprozess definiert wurde.
7. Wenn es sich bei dem Drittanbieterprodukt um CA Service Desk und bei dem Prozess um den Beispiel-Ereignis-/Alarmausgabeprozess handelt, geschieht Folgendes:
   - Es wird ein Help Desk-Ticket geöffnet, dem eine Nummer zugeordnet wird. In die Felder auf dem Ticket werden die Parameterwerte der Alarmdefinition eingetragen. Wenn eine URL empfangen wird, wird sie mit der Zusammenfassung angezeigt.
   - CA Service Desk gibt eine Ticket-Nummer an CA IT PAM zurück.
8. CA IT PAM übergibt die Ticket-Nummer zurück an CA Enterprise Log Manager.
9. CA Enterprise Log Manager zeigt die Ticket-Nummer als ein selbstüberwachendes Ereignis an.

Beispiel: Datenfluss für einen Ereignis-/Alarmausgabeprozess

Die Pfeile im folgenden Diagramm illustrieren den Datenfluss:

- Von Erfassungs- zu Berichtsservern
- Von Berichtsservern zu CA IT PAM
- Von CA IT PAM zum Produkt, an das der CA IT PAM-Prozess die CA Enterprise Log Manager-Ausgabe sendet, z. B. CA Service Desk.

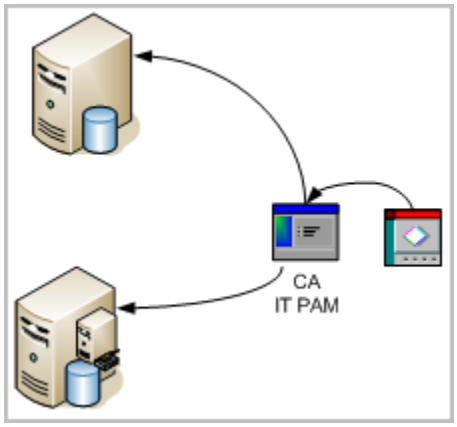


Wenn CA Enterprise Log Manager die Meldung erhält, dass der Vorgang erfolgreich war, fragt es bei CA IT PAM den Status des ausgeführten Prozesses ab. Sobald CA IT PAM den aktuellen Status gesendet hat, erstellt CA Enterprise Log Manager ein selbstüberwachendes Ereignis mit dem Ergebnis. Daraufhin werden folgende Schritte ausgeführt:

1. CA IT PAM benachrichtigt CA Enterprise Log Manager, ob der ausgeführte Prozess erfolgreich war oder fehlgeschlagen ist.
2. CA Enterprise Log Manager erstellt ein selbstüberwachendes Benachrichtigungserstellungsereignis mit den erhaltenen Ergebnissen.

Beachten Sie auch das Beispiel, in dem der CA IT PAM-Prozess ein Help Desk-Ticket mit den Prozessparameterwerten und den Ereignisdaten erstellt, die von der Abfrage ermittelt wurden. Die Pfeile im folgenden Diagramm illustrieren den folgenden Datenfluss:

- Vom Help Desk-Produkt an CA IT PAM
- Von CA IT PAM an die Quell-CA Enterprise Log Manager-Berichtsserver.



Importieren des Ereignis-/Alarmausgabe-Beispielprozesses

Damit Sie die CA IT PAM-Integration sofort testen und den Konfigurationsablauf üben können, steht ein Beispielprozess zur Verfügung. Sie finden diesen Prozess auf der DVD für die Anwendung. Für die Verwendung dieses IT PAM-Beispielprozesses wird vorausgesetzt, dass Sie als Helpdesk-Anwendung CA Service Desk verwenden.

Sie können CA IT PAM dann in CA Enterprise Log Manager konfigurieren und den CA IT PAM-Beispielprozess mit ausgewählten Abfrageergebnissen testen. Nachdem Sie sich mit dem Zusammenspiel zwischen CA Enterprise Log Manager und CA IT PAM vertraut gemacht haben, können Sie die Compliance Ihrer eigenen Prozesse sicherstellen und diese Werte in der CA IT PAM-Konfiguration mit Blick auf Ihre Produktionsintegration ersetzen.

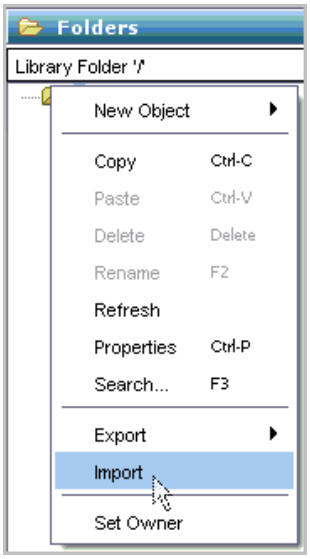
So importieren Sie einen Beispielprozess und testen die IT PAM-Integration:

1. Starten Sie CA IT PAM, und melden Sie sich an.
2. Starten Sie den ITPAM-Client.

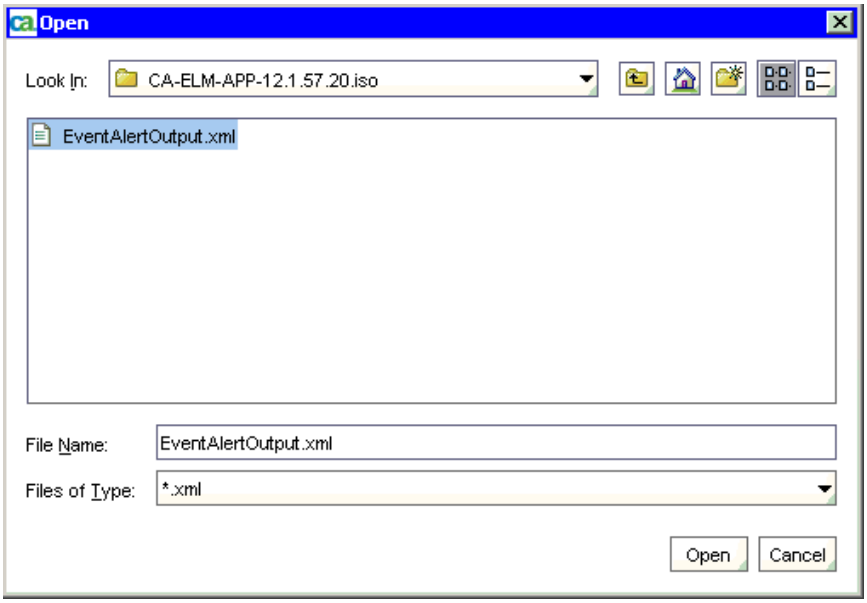
3. Importieren Sie den IT PAM-Beispielprozess "EventAlertOutput.xml", der sich auf der Anwendungs-DVD unter "CA/ITPAM" befindet. Bei diesem Beispiel sind alle erforderlichen Werte bereits definiert.

   a. Wählen Sie "File" (Datei), "Open Library Browser" (Bibliotheksbrowser öffnen) aus.

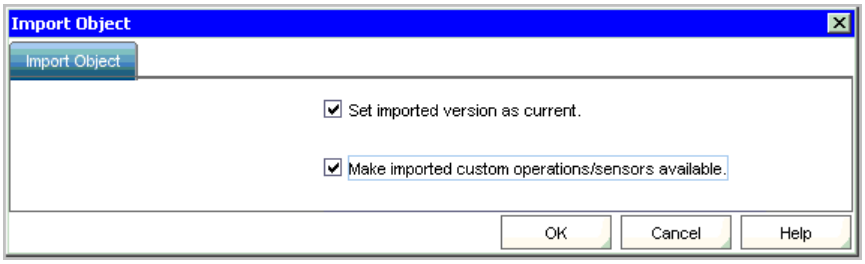
   b. Klicken Sie im linken Fenster auf "Folders" (Ordner), und klicken Sie unter dem Root-Ordner auf "Import" (Importieren).



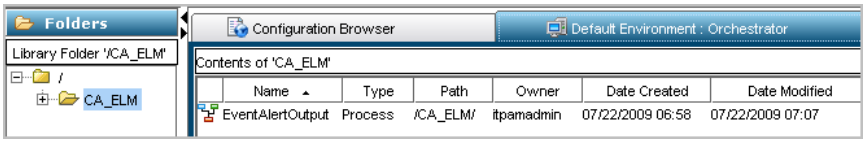
   c. Wählen Sie im extrahierten ISO-Image den IT PAM-Beispielprozess "EventAlertOutput.xml" aus, und klicken Sie auf "Open" (Öffnen).



d. Wählen Sie im Dialogfeld "Import Object" (Objekt importieren) beide Optionen aus, und klicken Sie auf "OK".



Daraufhin werden der genaue Name und Pfad eingeblendet. Hier lautet der Name beispielsweise "EventAlertOutput" und der Pfad "/CA_ELM/".



4. Legen Sie die Parameter für die Verbindung mit dem Service Desk fest.

   a. Klicken Sie für "Request_Create" auf die Registerkarte "ServiceDesk Connect Parameters" (ServiceDesk-Verbindungsparameter), um die ServiceDesk-Verbindungsparameter anzuzeigen.

   b. Geben Sie die URL für den Service Desk mit der folgenden Syntax an:

      `"http://<Servername>:8080/axis/services/USD_R11_WebService"`

   c. Geben Sie bei der Benutzer-ID und dem Kennwort für den Service Desk gültige Anmeldedaten ein.

5. (Optional) Testen Sie den importierten Prozess, um sicherzustellen, dass er ordnungsgemäß als eigenständiger Prozess ausgeführt wird.

6. Schließen Sie den ITPAM-Client, und klicken Sie auf "Sign Out" (Abmelden), um CA IT PAM zu beenden.

Anzeigen des Ereignis-/Alarmausgabebeispielprozesses

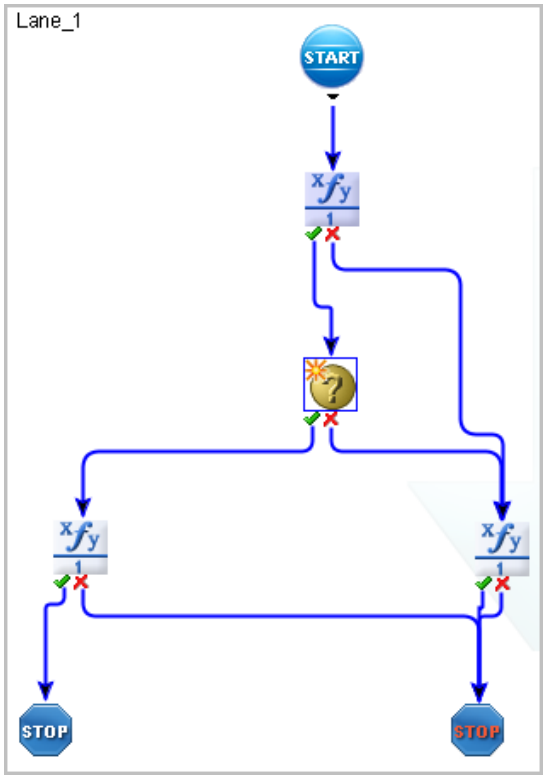
Falls Sie den Ereignis-/Alarmausgabebeispielprozess importieren, können Sie seinen Aufbau in CA IT PAM untersuchen. Folgen Sie den unten angeführten Richtlinien, um sich mit den CA Enterprise Log Manager-Voraussetzungen im Zusammenhang mit dem Beispielprozess vertraut zu machen. Sie erfahren in diesen Richtlinien, an welcher Stelle Verbindungsparameter für den Webdienst festgelegt und wie die Berechnungsoperatoren definiert werden. Ferner lernen Sie die produktspezifischen Anforderungen kennen. Wenn Sie beispielsweise CA Service Desk als Drittanbieterprodukt konfigurieren, müssen Sie den Operator "Request_Create" aus dem CA Service Desk-Modul sowie einen Vorausberechnungsoperator zur Verwaltung der Werte für den Schweregrad und die Priorität verwenden.

So machen Sie sich mit dem Ereignis-/Alarmausgabebeispielprozess vertraut:

1. Zeigen Sie das Modell Ihres Zielprozesses an.
   a. Starten Sie CA IT PAM, und melden Sie sich an.
   b. Klicken Sie auf den ITPAM-Client.
   c. Wählen Sie im Menü "File" (Datei) die Option "Open Library Browser" (Bibliotheksbrowser öffnen).
   d. Wählen Sie auf der Registerkarte "Folders" (Ordner) den Bibliotheksordner aus, der das Modell für Ihren Zielprozess enthält.

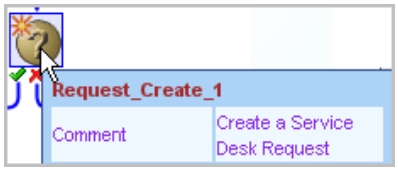
      Der Name des Prozesses sowie der Pfad werden im Hauptfenster angezeigt.
   e. Doppelklicken Sie auf die Zeile mit dem Namen und Pfad Ihres Prozesses.

Ein Modell wird angezeigt, das in etwa folgendermaßen aussieht: Dieses Beispielmodell enthält die Mindestvoraussetzungen für CA Enterprise Log Manager.



2. Beachten Sie, dass die ServiceDesk-Basisparameter die CA Enterprise Log Manager-Anforderungen erfüllen.

   a. Doppelklicken Sie auf das Symbol "Request_Create_1".

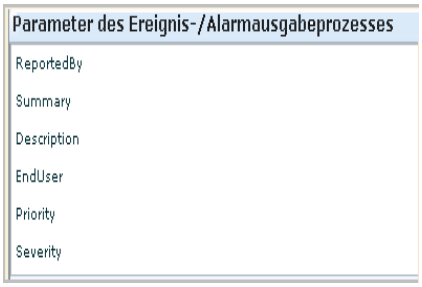


   Der Operator "Request_Create" übergibt die von der Aktionsalarmabfrage zurückgegebenen Daten an das Zielprodukt (Anwendung). Ein ähnlicher Operator ist für jeden Prozess erforderlich, der über CA Enterprise Log Manager ausgeführt werden soll.

b. Beachten Sie unter "ServiceDesk Basic Parameters" (ServiceDesk-Basisparameter), dass die lokalen Prozessparameter mit der folgenden Syntax angegeben werden:

```
BasicParameter = Prozess.LokalerParameter
```

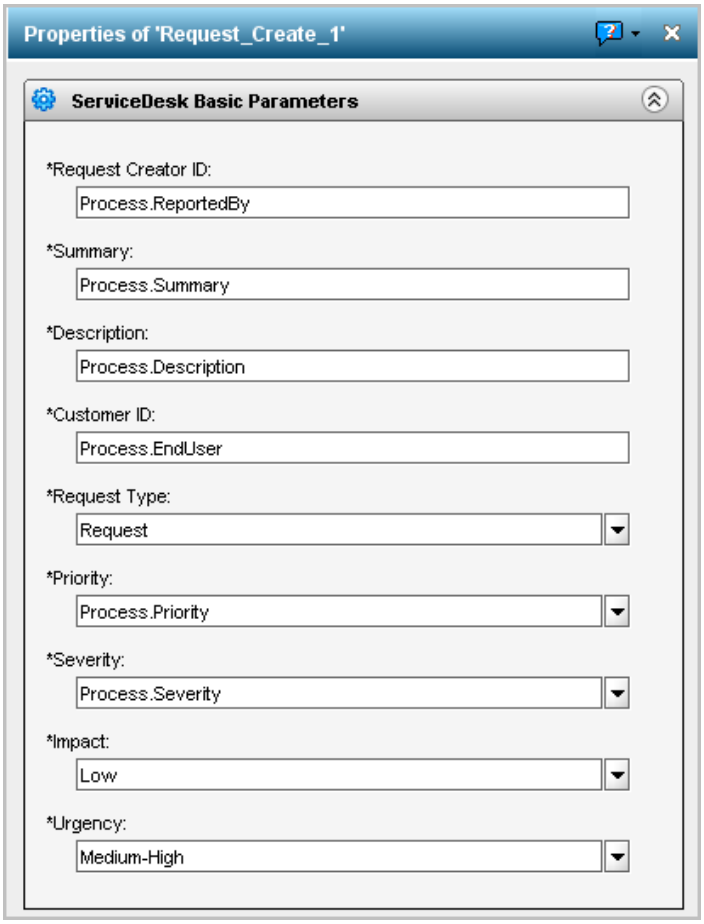
Hinweis: Bei den lokalen Prozessparametern handelt es sich um die Parameter des Ereignis-/Alarmausgabeprozesses, die Sie bei der Konfiguration von CA IT PAM zu CA Enterprise Log Manager hinzufügen.



c. Da es sich bei der Zielanwendung um CA Service Desk handelt, werden die folgenden lokalen Parameter wie in der folgenden Tabelle beschrieben definiert:

ServiceDesk-Basisparameter	Lokaler Parameter	Service Desk-Feld	Bemerkungen
Request Creator ID (ID des Erstellers der Anforderung)	Process.ReportedBy	Assignee,Reported By (Bearbeiter, Gemeldet von)	ein gültiger "Kontakt" in CA Service Desk
Summary (Zusammenfassung)	Process.Summary	Summary (Zusammenfassung)	(leer lassen)
Description (Beschreibung)	Process.Description	Description (Beschreibung)	(leer lassen)
Customer ID (Kunden-ID)	Process.EndUser	Affected End User (Betroffener Endbenutzer)	Ein gültiger "Kontakt" in CA Service Desk
Priority (Priorität)	Process.Priority	Priority (Priorität)	1-5
Severity (Schweregrad)	Process.Severity	Severity (Schweregrad)	1-5

Im folgenden Beispiel sehen Sie gültige lokale Parameter für die ServiceDesk-Basisparameter. Bei den Einträgen muss auf die Groß-/Kleinschreibung geachtet werden. Das heißt, dass "Process.ReportedBy" beispielsweise genau wie angegeben mit einem großen "R" und einem großen "B" eingegeben werden muss.

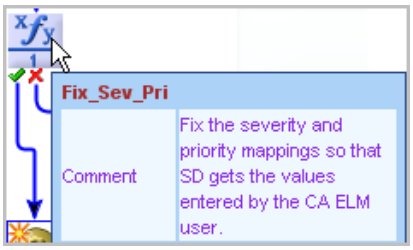


3. Klicken Sie für "Request_Create" auf die Registerkarte "ServiceDesk Connect Parameters" (ServiceDesk-Verbindungsparameter), um die ServiceDesk-Verbindungsparameter anzuzeigen.

   - Service Desk-URL:"http://<Servername>:8080/axis/services/USD_R11_WebService"
   - Service Desk-Benutzer-ID: "<SD-Benutzer>"
   - Kennwort: "<SD-Kennwort>"

4. Hinweis: Bei CA Service Desk muss eine Anpassung vorgenommen werden, damit sichergestellt ist, dass die in CA Enterprise Log Manager eingegebenen Werte für den Schweregrad und die Priorität von CA Service Desk richtig interpretiert werden.

   a. Nach "Start" und vor dem Operator "Create_Process" wird ein Operator für die Vorausberechnung angezeigt. Im folgenden Beispiel heißt dieser Operator "Fix_Sev_Pri".

   b. Unter "Properties" (Eigenschaften), "Calculate" (Berechnen) sind die folgenden Zuordnungen definiert:

```
if (Process.Priority == 1) Process.Priority = "pri:504";
else if (Process.Priority == 2) Process.Priority = "pri:503";
else if (Process.Priority == 3) Process.Priority = "pri:502";
else if (Process.Priority == 4) Process.Priority = "pri:501";
else if (Process.Priority == 5) Process.Priority = "pri:500";

if (Process.Severity == 1) Process.Severity = "sev:800";
else if (Process.Severity == 2) Process.Severity = "sev:801";
else if (Process.Severity == 3) Process.Severity = "sev:802";
else if (Process.Severity == 4) Process.Severity = "sev:803";
else if (Process.Severity == 5) Process.Severity = "sev:804";
```

5. Beachten Sie, dass die folgenden Parameter für den Rückgabewert (Ausgabeschnittstelle) wie erforderlich von CA Enterprise Log Manager formatiert werden:

   - ResultString
   - FaultString

6. Sehen Sie sich den Berechnungsoperator für die erfolgreiche Anforderungserstellung an. Dieses Format muss bei allen Ereignis-/Alarmausgabeprozessen verwendet werden, die über CA Enterprise Log Manager ausgeführt werden sollen.

   a. Klicken Sie auf das Symbol für den Berechnungsoperator für die erfolgreiche Anforderungserstellung.

   b. Wählen Sie die Registerkarte "Calculate" (Berechnen) aus, und klicken Sie im Feld für den Quellcode auf "...".

   c. Beachten Sie, wie der Berechnungsoperator für die erfolgreiche Erstellung im Quellcode definiert wurde:

   ```
   Process.ResultString = "Request " + Request_Create_1.newRequestNumber + "
   created in CA Service Desk.";
   ```

7. Sehen Sie sich den Berechnungsoperator für die fehlerhafte Erstellung an. Dieses Format muss bei allen Ereignis-/Alarmausgabeprozessen verwendet werden, die über CA Enterprise Log Manager ausgeführt werden sollen.

   a. Klicken Sie auf das Symbol für den Berechnungsoperator für die fehlerhafte Anforderungserstellung.

   b. Wählen Sie die Registerkarte "Calculate" (Berechnen) aus, und klicken Sie im Feld für den Quellcode auf "...".

   c. Beachten Sie, wie der Berechnungsoperator für eine fehlerhafte Erstellung im Quellcode definiert ist, wobei "Process.FaultString" der entsprechenden SOAP-Variablen zugeordnet ist:

   ```
   Process.FaultString = Request_Create_1.SoapErrorResponse;
   ```

Richtlinien zum Erstellen eines Ereignis-/Alarmausgabeprozesses

Damit ein CA IT PAM-Prozess aus CA Enterprise Log Manager ausgeführt werden kann, müssen bestimmte Richtlinien erfüllt werden. Bevor Sie versuchen, einen CA IT PAM-Prozess aus CA Enterprise Log Manager auszuführen, vergewissern Sie sich, dass der Prozess folgende Elemente umfasst:

- Webservice-Verbindungsparameter
- Erfolgsberechnungsoperator, der "Process:ResultString" einer Anweisung mit Zeichen und Variablen zuordnet, die die Antwort des Drittanbieterprodukts ausdrückt
- Fehlerberechnungsoperator, der "Process:FaultString" einer entsprechenden SOAP-Antwortvariablen zuordnet

Wenn sich Ihr Ziel-IT PAM-Prozess an ein Help Desk-Produkt eines Drittanbieters richtet, vergewissern Sie sich, dass der Prozess auch die folgenden Elemente umfasst:

- produktspezifischen Operator

  Beispiel: Ein Prozess mit den BMC Remedy-Modul als Ziel würde mit dem Operator "Create_Help_Desk_Case" definiert werden.

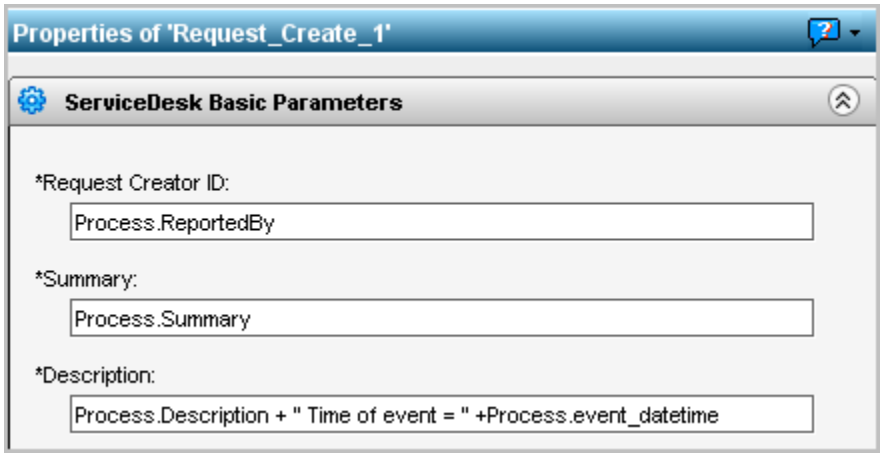
- produktspezifische Parameter, die lokalen Prozessparametern zugeordnet sind: "ReportedBy", "Summary", "Description", "EndUser", "Priority" und "Severity"

  Beispiel: Ein Prozess mit den BMC Remedy-Modul als Ziel würde mit den lokalen Parametern "Create_Help_Desk_Case" definiert werden.

Normalerweise umfasst ein CA IT PAM-Prozess nur die Standardprozessparameter, die jeweils einem Feld im Drittanbieterprodukt zugeordnet sind. Optional können Sie CEG-Felder als Prozessparameter für einen bestimmten Prozess hinzufügen. Im folgenden Beispiel werden die folgenden CEG-Felder im Datensatz angezeigt:

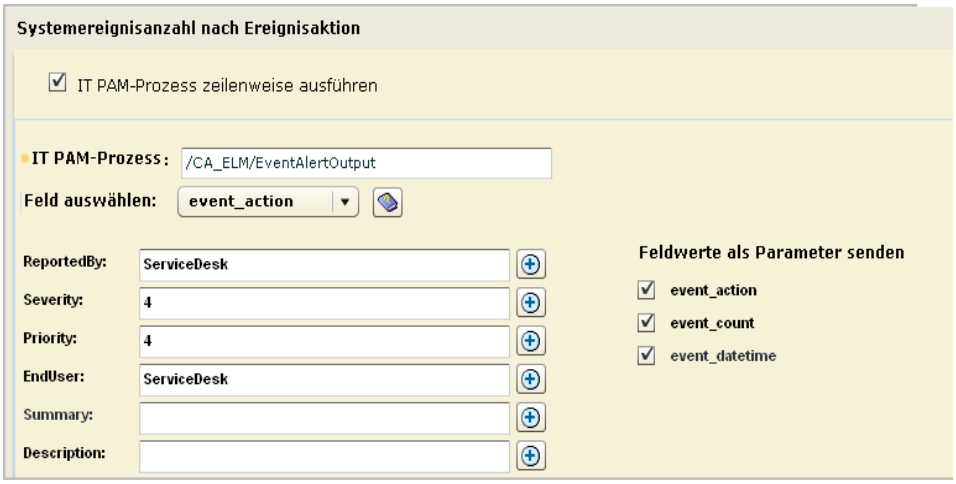
- event_severity
- event_count
- event_datetime

Jeder Basisparameter ist einem Service Desk-Feld zugeordnet. Der Prozessparameter "ReportedBy" ist beispielsweise dem CA Service Desk-Feld "Zuständiger" zugeordnet. Wenn CEG-Felder als Prozessparameter hinzugefügt werden, können sie als Werte in einem Basisparameter referenziert werden. Es kann beispielsweise für den Wert des CEG-Feldes "event_datetime" definiert werden, dass er im CA Service Desk standardmäßig im Feld "Beschreibung" angezeigt wird. Hierzu fügen Sie unter den Service Desk-Basisparametern im Feld "Beschreibung" den Wert "Process.event_datetime" hinzu.

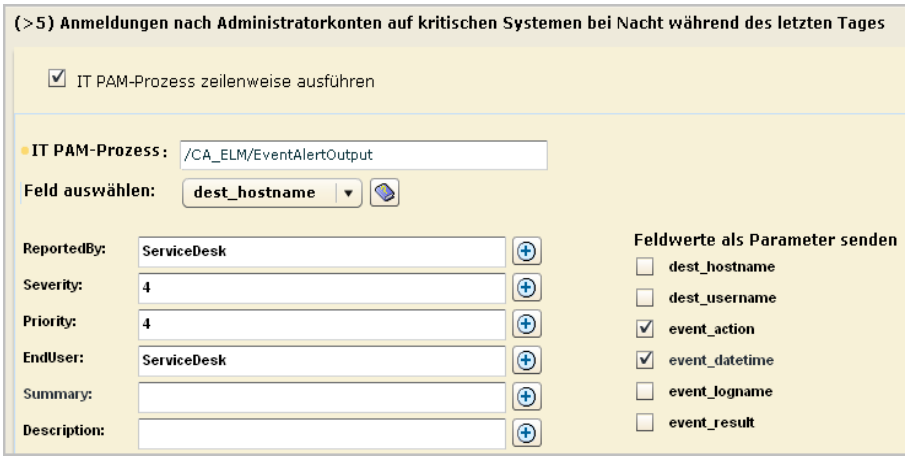


Wenn Sie einen Alarm erstellen, durch den dieser Prozess ausgeführt wird, überprüfen Sie die unter "Feldwerte als Parameter senden" aufgeführten CEG-Felder. Falls es sich bei einem der aufgelisteten Parameter um ein CEG-Feld handelt, das Sie als Prozessparameter definiert haben, wählen Sie dieses Feld aus. Betrachten Sie die folgenden Beispiele:

- Alle drei im Datensatz definierten CEG-Felder werden für die Abfrage "Systemereignisanzahl nach Ereignisaktion" angezeigt. In diesem Fall wählen Sie alle drei Felder, um sie als Parameter an CA IT PAM zu senden.



- Zwei der drei im Datensatz definierten CEG-Felder werden für die Abfrage "(>5) Anmeldungen nach Administratorkonten" angezeigt. In diesem Fall wählen Sie diese beiden Felder, um sie als Parameter an CA IT PAM zu senden.



Weitere Informationen:

Anzeigen des Ereignis-/Alarmausgabebeispielprozesses (siehe Seite 419)

Zusammentragen der Informationen für die CA IT PAM-Integration

Die meisten der für die CA IT PAM-Integration notwendigen Informationen sind Teil der Produkt- und Prozesskonfigurationen für CA IT PAM. Sie können CA IT PAM starten und dann im Laufe der Konfiguration nach den erforderlichen Informationen suchen, oder Sie können die Daten zuerst zusammentragen, notieren und dann die notierten Werte bei der Konfiguration von CA IT PAM eintragen.

Dabei haben Sie die Möglichkeit, auf die importierten Beispielprozesse oder Ihre eigenen, an die CA Enterprise Log Manager-Anforderungen angepassten Prozesse zu verweisen.

So tragen Sie die Informationen für die CA IT PAM-Integration zusammen:

1. Melden Sie sich bei Ihrem lokalen CA IT PAM-Server an, und vergewissern Sie sich, dass Sie mit CA IT Process Automation Manager 2.1 arbeiten.
2. Klicken Sie auf den Link für den ITPAM-Client.

3. Notieren Sie sich die Daten für die ersten vier Felder der IT PAM-Konfiguration.
   a. Klicken Sie auf "Configuration Browser" (Konfigurationsbrowser).
   b. Klicken Sie auf die Registerkarte "Eigenschaften“.
   c. Notieren Sie sich den Servernamen als Wert für den IT PAM-Server.
   d. Übernehmen Sie Port 8080 als IT PAM-Port.
   e. Lassen Sie sich vom zuständigen CA IT PAM-Administrator die Anmeldeinformationen für CA Enterprise Log Manager geben, und verwenden Sie diese als Benutzername und Kennwort.

IT PAM-Konfigurationsfeld	Beschreibung	Ihr Wert
IT PAM-Server	Der voll qualifizierte Hostname des Servers, auf dem CA IT PAM installiert ist. Dieser Wert wird im Feld "Server Name" (Servername) auf der Registerkarte "Properties" (Eigenschaften) des Konfigurationsbrowsers angezeigt.	
IT PAM-Port	Der Standard ist Port 8080. Dieser Wert wird im Feld "Domain URL" (URL der Domäne) auf der Registerkarte "Properties" (Eigenschaften) des Konfigurationsbrowsers angezeigt.	8080
Benutzername	Die Benutzer-ID, mit der sich CA Enterprise Log Manager bei IT PAM anmeldet und Prozesse ausführt. Sie erhalten diese ID von Ihrem CA IT PAM-Administrator. Beispiel: itpamadmin	
Kennwort	Das Kennwort, das mit dem Benutzernamen verknüpft ist. Sie erhalten dieses Kennwort von Ihrem CA IT PAM-Administrator.	

4. Notieren Sie sich die Pfade und Namen der Prozesse, die über CA Enterprise Log Manager ausgeführt werden sollen.
   a. Wählen Sie im Menü "File" (Datei) des ITPAM-Clients die Option "Open Library Browser" (Bibliotheksbrowser öffnen).
   b. Wählen Sie auf der Registerkarte "Folders" (Ordner) den Bibliotheksordner mit dem Ereignis-/Alarmausgabeprozess.
   c. Notieren Sie sich den Pfad und Namen des Ereignis-/Alarmausgabeprozesses.
   d. Falls dieser unterschiedlich ist, wählen Sie den Bibliotheksordner mit dem Prozess, der aktuelle Werte für einen bestimmten Schlüssel zurückgibt.
   e. Notieren Sie sich den Pfad und Namen für den Prozess mit dynamischen Werten.

IT PAM-Prozess-spezifisches Feld	Beschreibung und Beispiel	Ihr Wert
Ereignis-/Alarmausgabeprozess	Pfad und Prozessname Identifiziert den Prozess, der die mit dem Alarm konfigurierten Details bzw. eine URL an ein externes Produkt wie etwa CA Service Desk übergibt. Beispiel: /CA_ELM/EventAlertOutput	
Prozess mit dynamischen Werten	Pfad und Prozessname Identifiziert den Prozess, der Werte für den Eingabeschlüssel erfasst und diese für die Analyse in einer CSV-Datei zurückgibt. Beispiel: /CA_ELM/ValuesList	

5. Tragen Sie die Parameter des Ereignis-/Alarmausgabeprozesses zusammen:
   a. Doppelklicken Sie auf den Ereignis-/Alarmausgabeprozess, auf den Sie zum Öffnen des Prozesses verwiesen haben.
   b. Klicken Sie auf der Registerkarte "Main Editor" (Haupteditor) auf das Symbol "Request_Create", um die Eigenschaften anzuzeigen.
   c. Zeigen Sie die "ServiceDesk Basic Parameters" (ServiceDesk-Basisparameter) an.
   d. Notieren Sie sich die unten in der ersten Spalte angeführten Parameter (mit dem Präfix "Process:"), falls diese nicht exakt mit den vorliegenden Angaben übereinstimmen.
   e. Klicken Sie auf die Registerkarte "Dataset" (Datensatz).
   f. Klicken Sie auf jeden Parameter für "Local_Dataset", und notieren Sie sich den Standardwert (sofern vorhanden).

Parameter des Ereignis-/Alarmausgabeprozesses	Beschreibung und Beispiel	Ihr Wert
Berichtet von	Geben Sie einen gültigen ServiceDesk-Benutzernamen ein.	
Zusammenfassung	Dieser Text wird im Feld "Zusammenfassung" der Service Desk-Anfrage angezeigt. Zum Beispiel "Anfrage aus CA ELM erstellt".	---
Beschreibung	Dieser Text wird im Feld "Beschreibung" der Service Desk-Anfrage angezeigt.	---
Endbenutzer	Geben Sie einen gültigen ServiceDesk-Benutzernamen ein.	
Priorität	Legt die Standardpriorität fest. Falls kein Standardwert konfiguriert ist, notieren Sie sich einen Wert zwischen 1 und 5. Beispiel: 3	
Schweregrad	Legt den Standardschweregrad fest. Falls kein Standardwert konfiguriert ist, notieren Sie sich einen Wert zwischen 1 und 5. Beispiel: 4	

Beispiel: Ausführen eines Ereignis-/Alarmausgabeprozesses mit ausgewählten Abfrageergebnissen

Alle Benutzer sind berechtigt, auf Anforderung einen CA IT PAM-Prozess auszuführen. Sie können den konfigurierten CA IT PAM-Ereignis-/Alarmausgabeprozess mit ausgewählten Abfrageergebnissen zu folgenden Zwecken ausführen:

- Zur Durchführung eines Ereignis-/Alarmausgabeprozesses auf Basis der aktuellen Anforderungen.
- Zum Testen der Verarbeitungsergebnisse vor Erstellung eines geplanten Alarms für diese Abfrage mit dem Ziel des CA IT PAM-Prozesses.

Sie können einen CA IT PAM-Prozess aus einer in der Anzeige enthaltenen Abfrageergebniszeile ausführen. Hierbei wird vorausgesetzt, dass die Ergebnisse als Tabelle und nicht in einem Diagramm dargestellt werden. Abfrageergebniszeilen können auf folgende Weise dargestellt werden:

- Wählen Sie aus der Abfrageliste eine Abfrage aus, die Ergebnisse zurückgibt.
- Wählen Sie einen Bericht aus der Berichtsliste sowie eine Abfrage mit Ergebnissen aus.
- Geben Sie Werte für eine Eingabeaufforderung ein, die Ergebnisse zurückliefert.

Hinweis: Im folgenden Thema wird davon ausgegangen, dass eine Abfrageergebniszeile angezeigt wird, wenn Sie die Abfrage aus der Abfrageliste auswählen.

Informationen zu den für die CEG-Felder zurückgegebenen Daten finden Sie in der Online-Hilfe im Referenzhandbuch zur *ELM-Schemadefinition (CEG)*.

So führen Sie den konfigurierten CA IT PAM-Prozess manuell auf der Basis einer angezeigten Abfrageergebniszeile aus:

1. Klicken Sie auf die Registerkarte "Abfragen und Berichte" und auf die Unterregisterkarte "Abfragen".

   Der Abfragekennungsfilter und die Abfrageliste werden angezeigt.

2. (Optional) Geben Sie Suchkriterien wie Standardkonten in der Queryliste ein.

   Ereignisse, die Anmeldungen durch Standardkonten widerspiegeln, sind besonders für die Weitergabe an den CA IT PAM-Ereignis-/Alarmausgabeprozess geeignet.

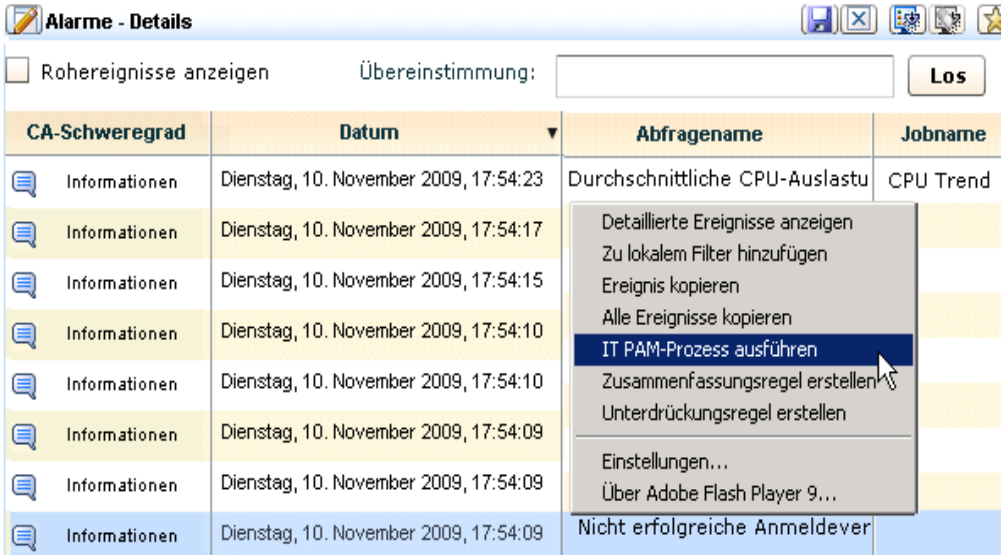
3. Wählen Sie die Abfrage aus der Abfrageliste aus, deren Ergebnisse Sie anzeigen möchten.

   Alternativ können Sie auch die Unterregisterkarte "Berichte" aufrufen, eine Option aus der Berichtsliste auswählen, zur Einzelabfragenansicht wechseln und die Abfrage aus dieser Ansicht auswählen.

4. Wenn die Ergebnisse in einem Diagramm dargestellt werden, wählen Sie aus der Dropdown-Liste für den Abfragenamen die Option "Visualisierung" und anschließend "Tabelle" aus.

5. Wählen Sie die Abfrageergebniszeile aus, für die Sie den CA IT PAM-Prozess ausführen möchten.

6. Klicken Sie mit der rechten Maustaste auf diese Abfrageergebniszeile, und wählen Sie aus der Dropdown-Liste die Option "IT PAM-Prozess ausführen" aus.



Das Dialogfeld "IT PAM-Prozess ausführen" wird angezeigt. Es enthält den Prozessnamen und die Prozessparameter, die in der IT PAM-Konfiguration des Berichtsserver-Services definiert sind. Darüber hinaus verfügt das Dialogfeld über eine Dropdown-Liste "Feld auswählen", die Ihnen die Möglichkeit bietet, Variablendaten einzugeben, die an das ausgewählte CEG-Feld zurückgegeben wurden.

7. Füllen Sie die Felder wie folgt aus:

   a. Überprüfen Sie die vorhandenen Standardwerte für die angezeigten Prozessparameter, und stellen Sie fest, ob Werte geändert werden müssen.

      Diese Parameter und ihre Werte werden anhand der Konfiguration der CA IT PAM-Integration ermittelt.

   b. Zum Ändern des angezeigten Standardwerts geben Sie den neuen Wert ein.

   c. Um einen Variablenwert anzugeben, wählen Sie oben im Dialogfeld in der Dropdown-Liste "Feld auswählen" das betreffende CEG-Feld aus, und klicken Sie dann neben dem Textfeld, auf das es sich bezieht, auf "Feld hinzufügen".

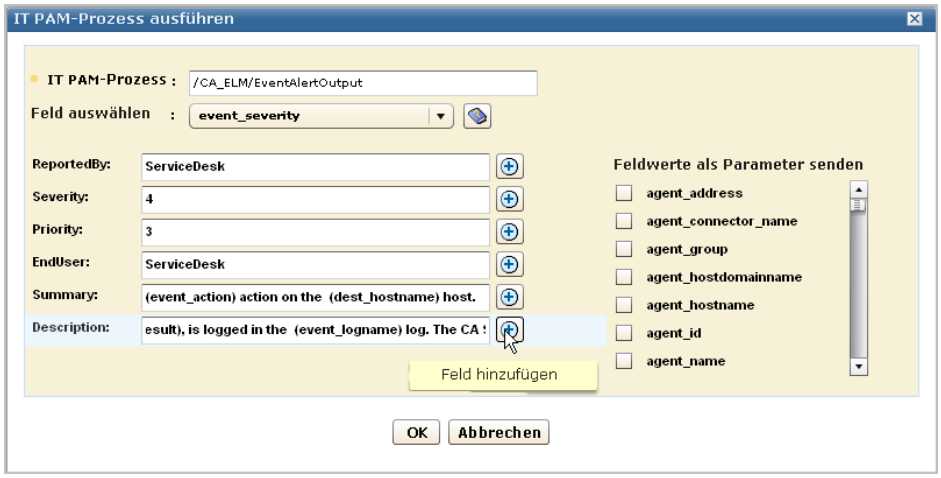
   d. Geben Sie für jedes leere Feld einen Wert ein, wählen Sie eine Variable aus, und fügen Sie sie hinzu, oder geben Sie einen Satz ein, der ausgewählte Variablen enthält.

      Übersicht des Beispiels: Für (event_datetime), wurde vom Konto (dest_username) eine Aktion (event_action) auf dem Host (dest_hostname) ausgeführt.

      Beschreibung des Beispiels: Das Aktionsergebnis (event_result) wird im Protokoll (event_logname) erfasst. Der CA-Schweregrad ist (event_severity).

   e. Wenn der CA IT PAM-Prozess Parameter angibt, die sich auf weitere CEG-Felder beziehen, wählen Sie die betreffenden Felder aus der angezeigten Liste aus, damit sie als Parameter gesendet werden.

   Beispiel: Ihre Anzeige enthält möglicherweise weitere Felder, die im benutzerdefinierten Ereignis-/Alarmausgabeprozess von IT PAM definiert sind.



8. Klicken Sie auf "OK".

   Das Statusdialogfeld wird angezeigt, gefolgt von einer Meldung, die angibt, ob der CA IT PAM-Prozess erfolgreich ausgeführt wurde. Wenn dies der Fall ist, werden auch die Ergebnisse der Prozessausführung ausgegeben.

   Im folgenden Beispiel ist das Ergebnis die Erstellung einer Anforderung Nr. 4590 in Service Desk.

9. Klicken Sie auf "OK".

10. Um die Ergebnisse in CA Service Desk anzuzeigen, melden Sie sich an, und suchen Sie nach der Anforderung mit der in der Meldung angegebenen Nummer.

    Wählen Sie beispielsweise "Anforderung" aus, und geben Sie "4590" ein.

11. Daraufhin werden Service Desk-Ergebnisse angezeigt, die in etwa der folgenden Darstellung entsprechen.

12. Vergleichen Sie die in Schritt 7 ermittelten geplanten Übersichts- und Beschreibungsdaten mit den entsprechenden Daten, die unter den zusammengefassten Informationen angezeigt werden. Sie enthalten auch die Informationen zum CA-Schweregrad.

Entwerfen von Ereignisabfragen, die an den Ereignis-/Alarmausgabeprozess zu senden sind

Nachdem Sie die CA IT PAM-Integration eingerichtet haben, können Sie den ersten Schritt zur Planung von Alarmen für die Ereignis-/Alarmausgabe durchführen: Erstellen Sie eine Liste mit Abfragen, auf denen die Alarme basieren sollen. Hierbei handelt es sich üblicherweise um Ereignisabfragen, die auf eine Richtlinienverletzung hinweisen. Sie können auf unterschiedliche Weise vorgehen:

- Analysieren Sie die aktuell geplanten Alarme, um Alarme zu ermitteln, bei denen der Ereignis-/Alarmausgabeprozess ausgeführt werden sollte. Wenn durch den Ereignis-/Alarmausgabeprozess beispielsweise eine Helpdesk-Anwendung benachrichtigt wird, geben Sie Alarme an, die das Öffnen eines Helpdesk-Tickets veranlassen sollten.
- Analysieren Sie Ihre Richtlinien, um diejenigen zu identifizieren, bei denen eine Verletzung auf ein protokolliertes Ereignis zurückgeführt werden konnte, und erstellen Sie dann eine Abfrage für ein solches Ereignis.
- Untersuchen Sie die Ergebnisse anderer vordefinierter Abfragen, um nach Daten zu suchen, die ein Drittanbieterprodukt wie z. B. eine Helpdesk-Anwendung für Hilfsmaßnahmen nutzen könnte.
- Wenn der CA IT PAM-Ereignis-/Alarmausgabeprozess in einem Helpdesk-Produkt eines Drittanbieters Tickets erstellt, überprüfen Sie die üblicherweise erstellten Helpdesk-Tickets auf Ursachen, die in Form von Ereignisprotokollen erfasst werden könnten.

So bestimmen und definieren Sie Abfragen, auf denen Alarme zur Ausführung des CA IT PAM-Ereignis-/Alarmausgabeprozesses beruhen:

1. Identifizieren, ändern oder erstellen Sie für jeden Ereignistyp, der ein Helpdesk-Ticket erfordert, eine oder mehrere Abfragen, die Daten für ein solches Ereignis erfassen.
   - Identifizieren Sie sämtliche vordefinierten Abfragen, die Ereignisse unter solchen Umständen erfassen.
   - Wenn eine vordefinierte Abfrage angepasst werden muss, kopieren Sie sie, und ändern Sie die Kopie entsprechend Ihren Anforderungen.
   - Sofern keine vordefinierten Abfragen zur Erfassung eines bestimmten Ereignistyps, der eine Helpdesk-Benachrichtigung erfordert, vorhanden sind, erstellen Sie die Abfrage oder Abfragen entsprechend Ihrer Anforderungen.

2. Bei jeder Abfrage, die nach einem IT-Ereignis suchen soll, bei dem eines der Felder einen von mehreren bekannten Werten aufweisen kann, verwenden Sie entweder eine vordefinierte Schlüsselliste, passen Sie eine Schlüsselliste an, oder erstellen Sie eine neue Schlüsselliste. Wenn die Werte für eine solche Schlüsselliste in einer CSV-Datei gespeichert sind, importieren Sie sie. Wenn eine Liste von einem IT PAM-Prozess generiert wird, konfigurieren Sie diesen Prozess als Prozess mit dynamischen Werten, erstellen Sie den Schlüssel, und importieren Sie anschließend die Werte aus CA IT PAM.
3. Bestimmen Sie, ob der CA IT PAM-Ereignis-/Alarmausgabeprozess jeweils pro Abfrage, die Ergebnisse liefert, oder pro Ergebniszeile ausgeführt werden soll.
4. Testen Sie die Abfrage.
    a. Sorgen Sie dafür, dass die Bedingung eintritt, die zu dem Ereignis führt, das erfasst werden soll.
    b. Führen Sie die Abfrage oder den Abfragesatz manuell aus.
    c. Prüfen Sie, ob die Abfrageergebnisse für die Helpdesk-Mitarbeiter zur weiteren Bearbeitung ausreichen.
    d. Wenn dies nicht der Fall ist, ändern Sie die Abfrage oder den Abfragesatz so ab, dass die erforderlichen Informationen bereitgestellt werden, und wiederholen Sie den Test.

Mit dieser Vorbereitung stellen Sie sicher, dass bei der Planung eines Alarms, der diese Abfrage bzw. diesen Abfragesatz ausführt, die zurückgelieferte Ereignis-/Alarmausgabe die zur Problemlösung benötigten Daten enthält.

Weitere Informationen

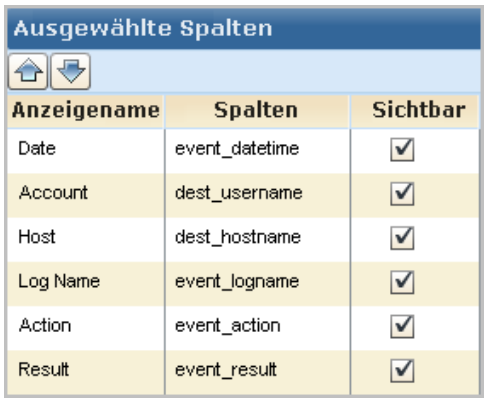
Anpassen von Abfragen für Aktionsalarme (siehe Seite 392)

Beispiel: Senden eines Alarms, durch den ein IT PAM-Prozess pro Zeile ausgeführt wird

Sie können einen Alarm senden, durch den der CA IT PAM-Ereignis-/Alarmausgabeprozess pro Zeile oder pro Abfrage ausgeführt wird. In diesem Beispiel wird die Ausführung pro Zeile vorgestellt. Hierbei erfahren Sie auch, welche Elemente für diese Art von Alarm von Mitarbeitern angezeigt werden können, die sowohl mit CA IT PAM als auch mit dem Drittanbieterprodukt, an das CA IT PAM die Informationen sendet, arbeiten.

Bevor Sie einen Alarm erstellen, durch den ein IT PAM-Prozess für eine bestimmte Abfrage ausgeführt wird, sollten Sie die Spalten der ELM-Schemadefinition (CEG-Spalten) ermitteln, die Daten zurückgeben. Dies sind die Spalten, die ausgewählt werden müssen, wenn Sie für den Alarm eine Zusammenfassungs- und Beschreibungsanweisung erstellen.

Hinweis: Kopieren Sie die Abfrage, und klicken Sie auf den Schritt "Abfragespalten". Bei sichtbaren Feldern entspricht der Spaltenname dem Anzeigenamen. So wird beispielsweise die Spalte für das Konto über das CEG-Feld "dest_username" gefüllt.


Ausgewählte Spalten

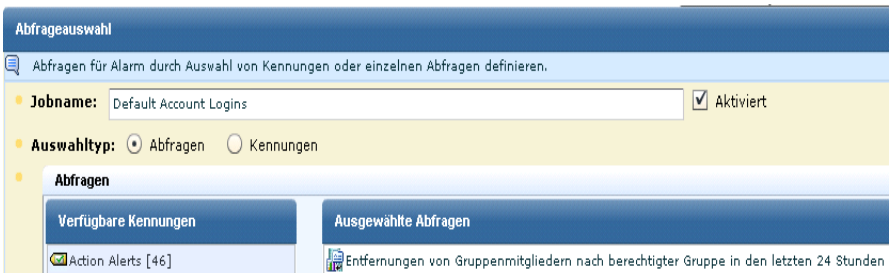
Anzeigename	Spalten	Sichtbar
Date	event_datetime	☑
Account	dest_username	☑
Host	dest_hostname	☑
Log Name	event_logname	☑
Action	event_action	☑
Result	event_result	☑

So erstellen Sie einen Alarm für eine erfolgreiche Anmeldung eines Standardkontomitglieds:

1. Klicken Sie zunächst auf die Registerkarte "Alarmverwaltung", dann auf die Unterregisterkarte "Alarmplanung".
2. Klicken Sie auf "Aktionsalarm planen".

   Der Assistent "Aktionsalarme planen" wird eingeblendet.

3. Nehmen Sie die Alarmauswahl folgendermaßen vor:
   a. Geben Sie den Jobnamen ein, z. B. "Standardkontoanmeldungen".
   b. Klicken Sie auf die Kennung "Aktionsalarme".
   c. Wählen Sie die Abfrage "Erfolgreiche Anmeldung nach Standardkonto in den letzten 24 Stunden", und verschieben Sie sie in die Liste "Ausgewählte Abfragen".



4. Wählen Sie einen Zeitraum für die Ausführung der Abfrage und die Anzahl der maximal anzuzeigenden Zeilen aus.
   a. Klicken Sie auf "Ergebnisbedingungen".
   b. Wählen Sie einen Zeitraum wie etwa "Jetzt" und "Jetzt" "-1 Stunden" aus.
   c. Wählen Sie Parameter für die Ergebnisanzeige wie etwa eine Zeilenbegrenzung von 10 und die Zeitgranularität "event_datetime" aus.
   d. Überspringen Sie gruppierte Ereignisse.
5. Definieren Sie den Zeitplan.
6. Legen Sie die Alarmdaten fest, die mit den von der Abfrage abgerufenen Ereignisdaten an den IT PAM-Prozess übergeben werden sollen.
   a. Klicken Sie auf den Schritt "Ziel".
   b. Wählen Sie die Registerkarte "IT PAM-Prozess" aus.
   c. Wählen Sie die Option "Erfolgreiche Anmeldung nach Standardkonten in den letzten 24 Stunden" aus.
   d. Wählen Sie die Option "IT PAM-Prozess zeilenweise ausführen" aus.
   e. Falls nicht der konfigurierte IT PAM-Prozess ausgeführt werden soll, ändern Sie den Pfad für den IT PAM-Prozess. Der IT PAM-Prozess muss den vollständigen Pfad beginnend mit einem Schrägstrich (/) enthalten.

f. (Optional) Erstellen Sie eine Zusammenfassungsanweisung mit wörtlichem Text und Variablen. Die Variablen werden in diesem Fall von CEG-Feldern abgeleitet, wenn die erfassten Daten für eine Zeile verfeinert werden. Im Folgenden sehen Sie eine Beispielzusammenfassungsanweisung mit Variablen.

```
The  (dest_username) account performed the (event_action) action on
(dest_hostname)
```

Die erste Anweisung wird wie folgt erstellt:

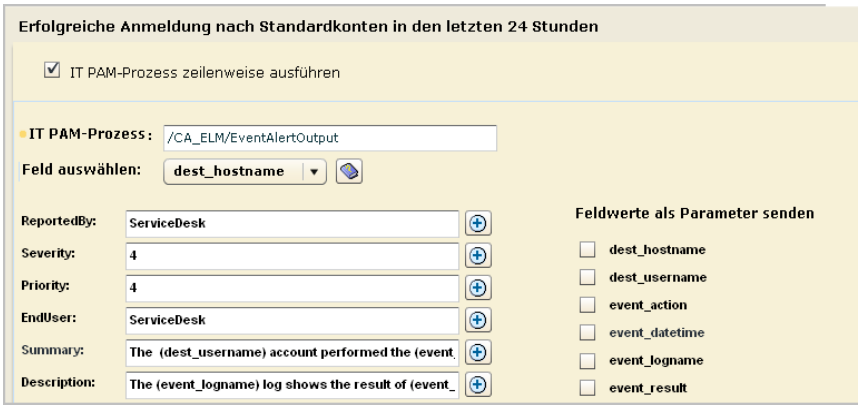
- Geben Sie das Wort "The" (Das) ein.
- Wählen Sie in der Dropdownliste "Feld auswählen" den Eintrag "dest_username" aus, und klicken Sie neben dem Feld "Übersicht" auf das Pluszeichen (+).
- Geben Sie den Ausdruck "account performed the" (Konto führte die) ein.
- Wählen Sie in der Dropdownliste "Feld auswählen" den Eintrag "event_action" aus, und klicken Sie neben dem Feld "Übersicht" auf das Pluszeichen (+).
- Geben Sie den Ausdruck "action on" (Aktion aus für) ein.
- Wählen Sie in der Dropdownliste "Feld auswählen" den Eintrag "dest_hostname" aus, und klicken Sie neben dem Feld "Übersicht" auf das Pluszeichen (+).

g. (Optional) Erstellen Sie eine Beschreibung mit wörtlichem Text und aus CEG-Feldern abgeleitetem Text. Wählen Sie in der Dropdown-Liste "Feld auswählen" das gewünschte Feld aus, und klicken Sie auf das Pluszeichen (+). Beispiel:

```
The (event_logname) log shows the result of (event_result) on
(event_datetime)

The(event_result) of the (event_action) is logged in the (event_logname)
log.

The (event_logname) log shows the (event_action) action had a result of
(event_result).
```

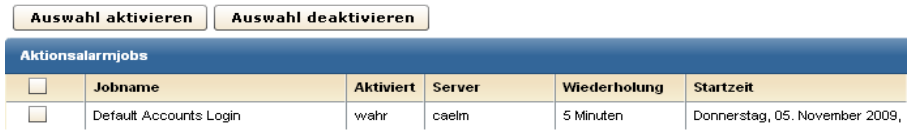
h. Wählen Sie unter "Feldwerte als Parameter senden" alle CEG-Felder aus, die von dem angegebenen IT PAM-Prozess als Prozessparameter verwendet werden.

Hinweis: Da der ausgewählte Prozess in diesem Beispiel keine CEG-Feldnamen verwendet, sind keine Felder aktiviert. Um festzustellen, ob ein benutzerdefinierter Prozess solche Parameter verwendet, rufen Sie die Registerkarte "Dataset" (Datensatz) im CA IT PAM-Ereignis-/Alarmausgabeprozess auf.



7. Wählen Sie einen Server aus.

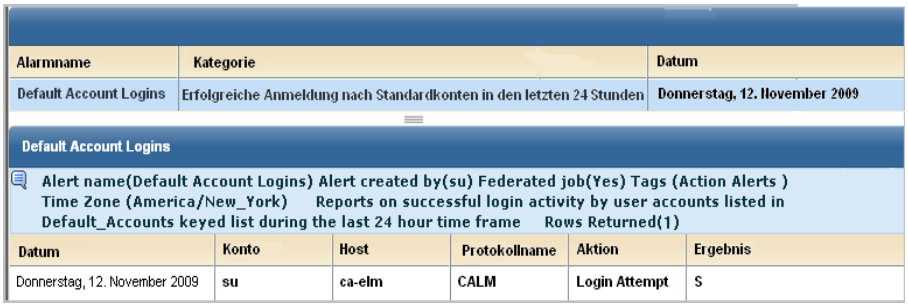
8. Klicken Sie auf "Speichern und schließen".
Der Job wird in der Liste "Aktionsalarmjobs" angezeigt.



9. Klicken Sie zum Anzeigen der Ergebnisse auf "Alarmverwaltung", "Selbstüberwachende Ereignisse". Im Folgenden sehen Sie einen Auszug der Datenzeilen:

Aktion	Ergebnis	Ergebnisbeschreibung
Resource Modify	S	Update RSSFeed Alert Name [login attempts] on reportServer [ca-elm] recurrence [5] recurrenceType [Minutes] was Successful.
Alert Creation	S	Alert job [Default Account Logins] created successfully.
Alert Job Setup	S	Schedule Action Query Alert Name [Default Account Logins] on reportServer [ca-elm] was Successful.

10. Klicken Sie auf die Registerkarte "Alarmverwaltung", und wählen Sie die Unterregisterkarte "Aktionsalarme" aus. Wählen Sie den geplanten Alarm aus, um die Abfrageergebnisse anzuzeigen.



Alarmname	Kategorie	Datum
Default Account Logins	Erfolgreiche Anmeldung nach Standardkonten in den letzten 24 Stunden	Donnerstag, 12. November 2009

Default Account Logins

Alert name(Default Account Logins) Alert created by(su) Federated job(Yes) Tags (Action Alerts) Time Zone (America/New_York) Reports on successful login activity by user accounts listed in Default_Accounts keyed list during the last 24 hour time frame Rows Returned(1)

Datum	Konto	Host	Protokollname	Aktion	Ergebnis
Donnerstag, 12. November 2009	su	ca-elm	CALM	Login Attempt	S

11. Überprüfen Sie auf der Registerkarte "Selbstüberwachende Ereignisse" die von CA IT PAM zurückgegebenen Ergebnisse.

    Im Folgenden sehen Sie einen Auszug einer Erfolgsmeldung, wobei diese Meldung in den selbstüberwachenden Ereignissen für den Berichtsserver erscheint. Achten Sie auf die Ticketnummer hinter "Results =".

Aktion	Ergebnis	Ergebnis-Beschreibung
Notification Creation	S	IT PAM process ran successfully. Results = [Request 631 created in CA Service Desk.]

12. (Optional) Zeigen Sie die Ergebnisse wie folgt in CA Service Desk an:

    a. Melden Sie sich bei CA Service Desk an.

    b. Wählen Sie "Request" (Anforderung) aus, und geben Sie die Fallnummer ein.

    c. Klicken Sie auf den Link für die Anforderungsnummer, und zeigen Sie Detailinformationen zum Problem und eine Übersicht an.

Weitere Informationen:

Richtlinien zum Erstellen eines Ereignis-/Alarmausgabeprozesses (siehe Seite 424)

Beispiel: Senden eines Alarms, der einen IT PAM-Prozess pro Abfrage ausführt

Sie können einen Alarm senden, durch den der CA IT PAM-Ereignis-/Alarmausgabeprozess pro Zeile oder pro Abfrage ausgeführt wird. In diesem Beispiel wird ein Prozess pro Abfrage ausgeführt. Dabei wird gezeigt, was für diesen Alarmtyp Benutzern der Drittanbieterprodukte angezeigt wird, an die CA IT PAM die Details sendet.

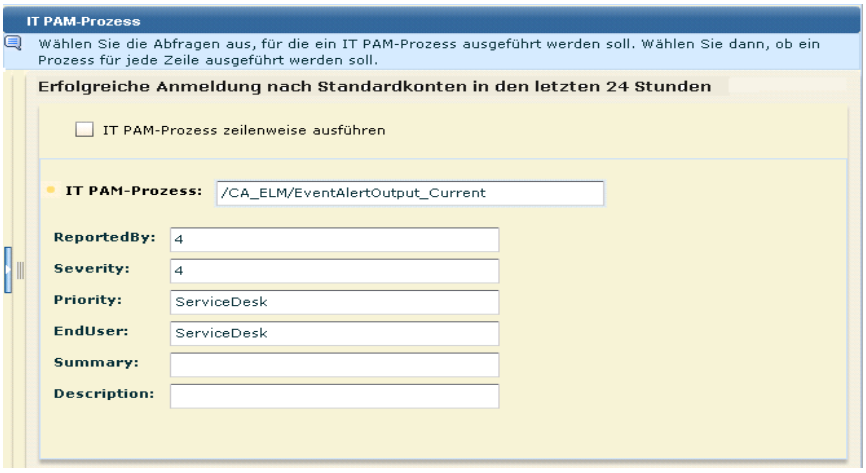
So senden Sie einen Alarm, der den CA IT PAM Ereignis-/Alarmausgabeprozess pro Zeile oder pro Abfrage ausführt.

1. Klicken Sie zunächst auf die Registerkarte "Alarmverwaltung", dann auf die Unterregisterkarte "Alarmplanung".
2. Klicken Sie auf "Aktionsalarm planen".

   Der Assistent "Aktionsalarme planen" wird eingeblendet.
3. Nehmen Sie die Alarmauswahl folgendermaßen vor:
   a. Geben Sie den Jobnamen ein.
   b. Wählen Sie eine Abfrage aus.
4. (Optional) Wählen Sie einen Datumsbereich für die Abfrage und die maximal angezeigte Anzahl von Zeilen aus.
   a. Klicken Sie auf "Ergebnisbedingungen".
   b. Wählen Sie einen Zeitraum wie etwa "Jetzt" und "Jetzt" "-1 Stunden" aus.
   c. Wählen Sie die Parameter für die Ergebnisansicht aus.
5. Definieren Sie den Zeitplan.
6. Legen Sie die Alarmdaten fest, die mit den von der Abfrage abgerufenen Ereignisdaten an den IT PAM-Prozess übergeben werden sollen.
   a. Klicken Sie auf den Schritt "Ziel".
   b. Wählen Sie die Registerkarte "IT PAM-Prozess" aus.
   c. Wählen Sie die sendende Abfrage aus.

d. Wenn Sie einen Ergebnisbericht pro Abfrage wünschen, lassen Sie den Eintrag "IT PAM-Prozess zeilenweise ausführen" leer.

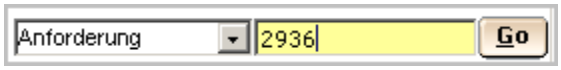
e. Optional können Sie in den Feldern "Zusammenfassung" und "Beschreibung" Text eingeben.



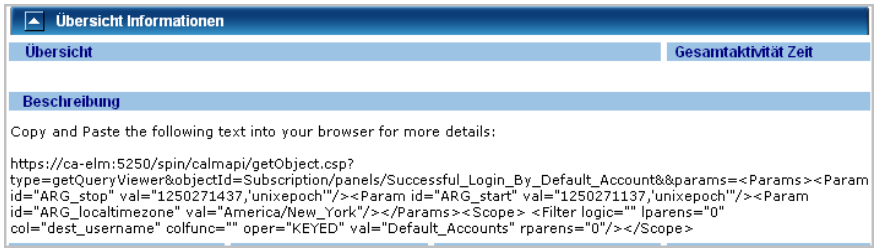
7. Wählen Sie einen Server aus.
8. Klicken Sie auf "Speichern und schließen".
   Der Job wird in der Liste "Aktionsalarmjobs" angezeigt.
9. Klicken Sie auf die Registerkarte "Alarmverwaltung", und wählen Sie die Unterregisterkarte "Aktionsalarme" aus. Wählen Sie den geplanten Alarm aus, um die Abfrageergebnisse anzuzeigen.
10. Suchen Sie auf der Registerkarte "Selbstüberwachende Ereignisse" die Benachrichtigungserstellung mit Ergebnissen aus CA IT PAM. Eine Erfolgsmeldung enthält die Nummer der Anfrage, die in der Drittanbieteranwendung erstellt wurde, sofern es sich dabei um ein Help Desk-Produkt handelt.

Aktion	Ergebnis	Ergebnis-Beschreibung
Notification Creation	S	IT PAM process ran successfully. Results = Request 2936 created in CA Service Desk.

11. (Optional) Um zu sehen, was den Help Desk-Mitarbeitern angezeigt wird, überprüfen Sie die Ergebnisse folgendermaßen in CA Service Desk:
    a. Melden Sie sich bei CA Service Desk an.
    b. Wählen Sie die Anfrage, und geben Sie die Nummer ein, die in der Ergebnisbeschreibung der Benachrichtigungserstellung angezeigt wird. Klicken Sie auf "Los".



c. Kopieren Sie die URL, die in der Zusammenfassung angezeigt wird, und fügen Sie sie in Ihrem Browser ein.



Das CA Enterprise Log Manager-Anmeldedialogfeld wird angezeigt.

d. Melden Sie sich bei CA Enterprise Log Manager an. Sie können ein Konto mit eingeschränkten Rechten verwenden, beispielsweise ein Auditor-Konto.

Die Ereignisdaten, die von der Abfrage zurückgegeben werden, werden im Format der Standardansicht der Abfrage angezeigt, also Tabelle oder Diagramm.

Bei Anzeige im Tabellenformat können Sie Rohereignisdaten anzeigen.

Weitere Informationen

Festlegen von Benachrichtigungszielen (siehe Seite 496)

Arbeiten mit SNMP-Traps

Fehlermanagementsysteme und Network Operations Center (NOCs) erhalten normalerweise SNMP-Traps. Alarme können Sie an solche Systeme je nach Zielprodukt als SNMP v2-Traps oder SNMP v3-Traps senden.

Die einzigen erforderlichen Aufgaben, um mit SNMP-Traps arbeiten zu können, sind folgende:

- Erstellen Sie eine benutzerdefinierte MIB für jeden für CA NSM bestimmten Aktionsalarm.
- Bereiten Sie die Zielprodukte für den Empfang von SNMP-Traps aus CA Enterprise Log Manager vor.
- Planen Sie Alarme mit einem oder mehreren SNMP-Trap-Zielen.

Ein Standard-SNMP-Trap-Ziel zu konfigurieren ist optional.

Info zu SNMP-Traps

SNMP ist das Akronym für Simple Network Management Protocol. Dabei handelt es sich um einen offenen Standard zum Versenden von Alarmmeldungen an ein angegebenes Ziel. Es gibt drei Versionen von SNMP: SNMPv1, SNMPv2 und SNMPv3. CA Enterprise Log Manager verwendet entweder SNMPv2 oder SNMPv3, um ein oder mehrere Drittanbieter-Verwaltungssysteme zu warnen, sobald ein Ereignis eintritt, das einen Alarm generiert.

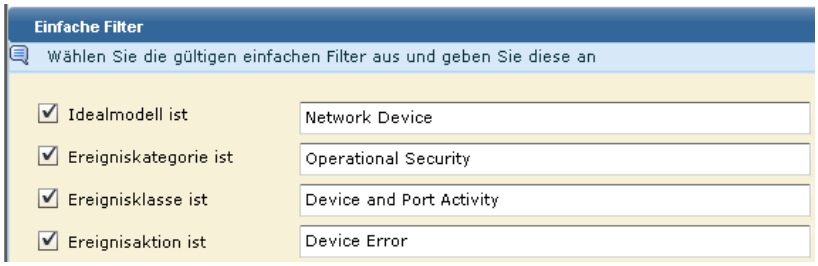
In CA Enterprise Log Manager, wird ein Alarm generiert, wenn eine geplante Abfrage Ergebnisse aus der Ereignisprotokolldatenbank kürzlich verfeinerter Ereignisse zurückgibt. Eine geplante Abfrage kann mit einem SNMP-Trap als Ziel konfiguriert werden. Trap-Empfänger (Zielverwaltungssysteme) können Traps mit einer Rate von maximal 200 Traps pro Sekunde verarbeiten. Trap-Empfänger hören normalerweise den UDP-Port 162 ab, den typischen Port für snmptrap.

Mit CA Enterprise Log Manager können Sie flexibel eigene benutzerdefinierte Alarme erstellen, die als SNMP-Traps gesendet werden. Sie können beispielsweise Alarme definieren, bei denen eine Benachrichtigung gesendet wird, dass ein kritisches Ereignis eingetreten ist. Darüber hinaus können Sie Alarme für Ereignisse wie Konfigurationsänderungen definieren. Welche Alarme als SNMP-Traps gesendet werden, legen Sie fest.

Beispiel: Einfache Filter für Alarme als Traps senden

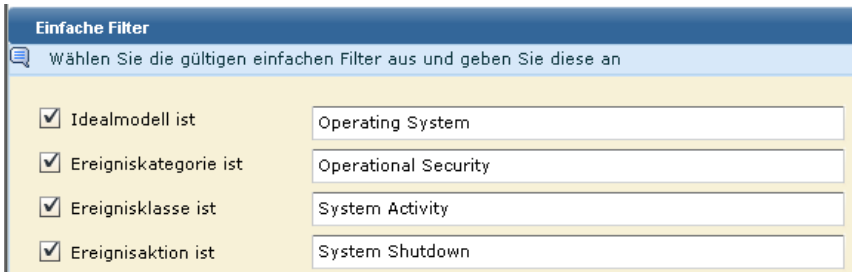
Ereignisse wie das Herunterfahren von Services, Fehler an Geräten und die Löschung von Ressourcen, die sich negativ auf Vorgänge auswirken, sind von Interesse für das Network Operations Center (NOCs). Wenn solche Ereignisse auftreten, können Sie Aktionsalarme erstellen und sie an Ihr NOC weiterleiten. Sie können zu diesem Zweck unter Verwendung eines einfachen Filters in einer benutzerdefinierten Abfrage benutzerdefinierte Alarme erstellen. Betrachten Sie folgende einfachen Filterbeispiele.

- Gerätefehler



- Ressourcenlöschung

- System herunterfahren



Wissenswertes über MIB-Dateien

SNMP-Traps sind entweder in Management Information Base-Dateien (MIB-Dateien) oder in Enterprise-spezifischen MIB-Dateien definiert.

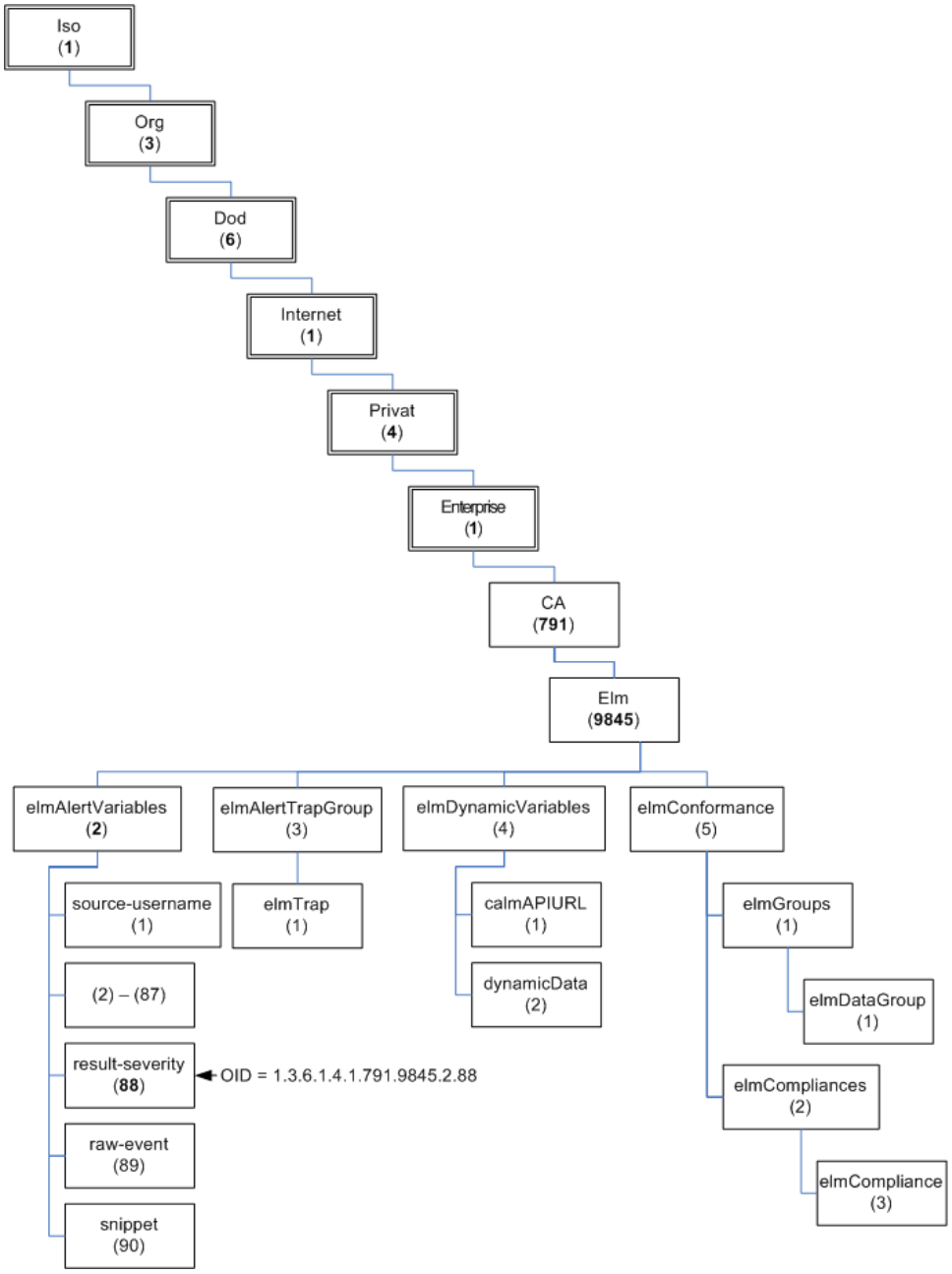
Jedes Private Enterprise im MIB-Baum hat eine eindeutige Nummer, der die Nummern des übergeordneten Knotens vorangestellt ist. CA, Inc. wurde von IANA die Private Enterprise-Nummer 791 zugeteilt. Alle Daten, die von einer beliebigen CA-Anwendung in SNMP-Traps gesendet werden, erhalten Objekt-IDs, die mit 1,3.6,1.4,1.791 beginnen. Die CA Enterprise Log Manager-Anwendung von CA hat die ID 9845. Alle SNMP-Trap-Daten, die von CA Enterprise Log Manager-Aktionsalarmen gesendet werden, erhalten Objekt-IDs (OIDs), die mit 1.3.6.1.4.1.791.9845 beginnen.

CA Enterprise Log Manager stellt eine MIB-Datei bereit. Der Name dieser MIB-Datei lautet CA-ELM.MIB. In dieser MIB-Datei sind sämtliche Felder definiert, die von Aktionsalarmen mit einem Trap gesendet werden können. Dieser Trap enthält alle in CA Enterprise Log Manager verfügbaren CEG-Felder.

Wenn ein Aktionsalarm an ein SNMP-Trap-Ziel gesendet wird, beinhalten die übermittelten Daten eine URL. Die eingehenden Traps zur individuellen Überwachung können die vom Aktionsalarm gesendete URL durchsuchen. Mit dem Durchsuchen der URL wird eine CA Enterprise Log Manager-Seite geöffnet, auf der die Abfrageergebnisse in einem leicht lesbaren Format angezeigt werden. Durch diese Funktion ist es nicht mehr erforderlich, MIB-Dateien zu verwenden, um in Form von SNMP-Traps gesendete Daten zu interpretieren.

Der CA-ELM MIB-Baum

Sie können die Struktur der CA-ELM.MIB-Datei im MIB-Baumformat anzeigen. CEG-Felder werden unter "elmAlertVariables" durch eindeutige SNMP-Objekt-IDs definiert. Beispiel: "result_severity" hat die OID "1.3.6.1.4.1.791.9845.2.88".



Die Datei "CA-ELM.MIB"

Die Datei für die CA Enterprise Log Manager-MIB "CA-ELM.MIB" befindet sich auf der Installations-DVD. Die CA Enterprise Log Manager-MIB wird anhand des Quelldokuments für die ELM-Schemadefinition erzeugt, das die OIDs für die einzelnen Felder der ELM-Schemadefinition (CEG-Felder, elmAlertVariables) enthält.

Die Datei "CA-ELM.MIB" beginnt wie folgt mit dem Abschnitt "Imports":

```
CAELM-MIB DEFINITIONS ::= BEGIN

  IMPORTS
        MODULE-IDENTITY, OBJECT-TYPE, Integer32, NOTIFICATION-TYPE
                FROM SNMPv2-SMI
        MODULE-COMPLIANCE, OBJECT-GROUP,NOTIFICATION-GROUP
                FROM SNMPv2-CONF                        DisplayString
                FROM SNMPv2-TC;
```

Die folgende Darstellung dient dazu, die Struktur der CA Enterprise Log Manager-MIB-Baumstruktur zu zeigen, wo die obersten Knoten iso(1) org(3) dod(6) internet(1) private(4) enterprises(1) einschließen. Die eigentliche CA-ELM.MIB ist nicht wie in dieser Darstellung formatiert.

```
ca OBJECT IDENTIFIER::= { enterprises 791 }
        elm MODULE-IDENTITY...::= { ca 9845 }
                elmAlertVariables       ::= { elm 2 }
                        source-username     ::= { elmAlertVariables 1 }
                        source-domainname   ::= { elmAlertVariables 2 }
                        source-groupname    ::= { elmAlertVariables 3 }
                     ...
                        result-severity     ::= { elmAlertVariables 88 }
                        raw-event           ::= { elmAlertVariables 89 }
                        snippet             ::= { elmAlertVariables 90 }
                elmAlertTrapGroup       ::= { elm 3 }
                        elmTrap             ::= { elmAlertTrapGroup 1 }

                elmDynamicVariables     ::= { elm 4 }
                        calmAPIURL          ::= { elmDynamicVariables 1 }
                        dynamicData         ::= { elmDynamicVariables 2 }
                elmConformance          ::= { elm 5 }
                        elmGroups           ::= { elmConformance 1 }
                                elmDataGroup    ::= { elmGroups 1 }
                        elmCompliances      ::= { elmConformance 2 }
                                elmCompliance   ::= { elmCompliances 3 }
```

Die CA-ELM.MIB-Datei definiert eine Trap. Diese Trap wird folgendermaßen angegeben:

```
elmTrap NOTIFICATION-TYPE
    OBJECTS {  source-username,source-domainname,source-groupname,source-
uid,source-gid,source-hostname,source-hostdomainname,source-address,source-mac-
address,source-port,source-processname,source-objectname,source-
objectattr,source-objectid,source-objectclass,source-objectvalue,dest-
username,dest-domainname,dest-groupname,dest-uid,dest-gid,dest-hostname,dest-
hostdomainname,dest-address,dest-mac-address,dest-port,dest-objectname,dest-
objectattr,dest-objectid,dest-objectclass,dest-objectvalue,agent-name,agent-
address,agent-hostname,agent-hostdomainname,agent-version,agent-id,agent-
connector-name,agent-group,event-source-hostname,event-source-
hostdomainname,event-source-address,event-source-processname,receiver-
name,receiver-hostname,receiver-hostaddress,receiver-hostdomainname,receiver-
port,receiver-time-gmt,receiver-timezone,receiver-version,event-protocol,event-
logname,event-euuid,event-count,event-summarized,event-duration,event-time-
year,event-time-month,event-time-monthday,event-time-weekday,event-time-
hour,event-time-minute,event-time-gmt,event-datetime,event-year-datetime,event-
month-datetime,event-day-datetime,event-hour-datetime,event-quarterhour-
datetime,event-minute-datetime,event-timezone,event-sequence,event-trend,event-
action,event-id,event-category,event-class,ideal-model,event-severity,event-
result,result-string,result-signature,result-code,result-version,result-
priority,result-scope,result-severity,raw-event,snippet }
    STATUS  current
    BESCHREIBUNG
            "The ELM SNMP Trap."
    ::= { elmAlertTrapGroup 1 }
```

Die elmAlertTrapGroup ist 1.3.6.1.4.1.791.9845.3 und das elmTrap wird von dem nächsten Knoten angegeben. Die standardmäßige elmTrap-ID lautet 1.3.6.1.4.1.791.9845.3.1. Benutzerdefinierte Trap-IDs liegen im Bereich von 1.3.6.1.4.1.791.9845.3.2 bis 1.3.6.1.4.1.791.9845.3.999.

Wichtig! Zum Versenden von Traps an CA Spectrum wird empfohlen, die Standard-elmTrap-ID zu verwenden. Zum Versenden von Traps an CA NSM wird empfohlen, eine Standard-Trap-ID festzulegen, die sich auf eine elmTrap-ID in einer benutzerdefinierten MIB bezieht.

Zuordnung von Objekt-IDs (OIDs) zu CEG-Feldern

Die folgende Tabelle zeigt die CEG-Felder, die den einzelnen Objekt-IDs (OIDs) im Abschnitt "elmAlertVariables"; der MIB-Struktur entsprechen. Dieser Teil der Struktur wächst, wenn neue Felder zur ELM-Schemadefinition hinzugefügt werden. Suchen Sie regelmäßig nach Updates für die MIB, und vergewissern Sie sich, dass Ihren SNMP-Trap-Zielprodukten die neueste Version zur Verfügung steht.

Objekt-ID (OID)	CEG-Feld
1.3.6.1.4.1.791.9845.2.1	source-username
1.3.6.1.4.1.791.9845.2.2	source-domainname
1.3.6.1.4.1.791.9845.2.3	source-groupname
1.3.6.1.4.1.791.9845.2.4	source-uid
1.3.6.1.4.1.791.9845.2.5	source-gid
1.3.6.1.4.1.791.9845.2.6	source-hostname
1.3.6.1.4.1.791.9845.2.7	source-hostdomainname
1.3.6.1.4.1.791.9845.2.8	source-address
1.3.6.1.4.1.791.9845.2.9	source-mac-address
1.3.6.1.4.1.791.9845.2.10	source-port
1.3.6.1.4.1.791.9845.2.11	source-processname
1.3.6.1.4.1.791.9845.2.12	source-objectname
1.3.6.1.4.1.791.9845.2.13	source-objectattr
1.3.6.1.4.1.791.9845.2.14	source-objectid
1.3.6.1.4.1.791.9845.2.15	source-objectclass
1.3.6.1.4.1.791.9845.2.16	source-objectvalue
1.3.6.1.4.1.791.9845.2.17	dest-username
1.3.6.1.4.1.791.9845.2.18	dest-domainname
1.3.6.1.4.1.791.9845.2.19	dest-groupname
1.3.6.1.4.1.791.9845.2.20	dest-uid
1.3.6.1.4.1.791.9845.2.21	dest-gid
1.3.6.1.4.1.791.9845.2.22	dest-hostname

Objekt-ID (OID)	CEG-Feld
1.3.6.1.4.1.791.9845.2.23	dest-hostdomainname
1.3.6.1.4.1.791.9845.2.24	dest-address
1.3.6.1.4.1.791.9845.2.25	dest-mac-address
1.3.6.1.4.1.791.9845.2.26	dest-port
1.3.6.1.4.1.791.9845.2.27	dest-objectname
1.3.6.1.4.1.791.9845.2.28	dest-objectattr
1.3.6.1.4.1.791.9845.2.29	dest-objectid
1.3.6.1.4.1.791.9845.2.30	dest-objectclass
1.3.6.1.4.1.791.9845.2.31	dest-objectvalue
1.3.6.1.4.1.791.9845.2.32	agent-name
1.3.6.1.4.1.791.9845.2.33	agent-address
1.3.6.1.4.1.791.9845.2.34	agent-hostname
1.3.6.1.4.1.791.9845.2.35	agent-hostdomainname
1.3.6.1.4.1.791.9845.2.36	agent-version
1.3.6.1.4.1.791.9845.2.37	agent-id
1.3.6.1.4.1.791.9845.2.38	agent-connector-name
1.3.6.1.4.1.791.9845.2.39	agent-group
1.3.6.1.4.1.791.9845.2.40	event-source-hostname
1.3.6.1.4.1.791.9845.2.41	event-source-hostdomainname
1.3.6.1.4.1.791.9845.2.42	event-source-address
1.3.6.1.4.1.791.9845.2.43	event-source-processname
1.3.6.1.4.1.791.9845.2.44	receiver-name
1.3.6.1.4.1.791.9845.2.45	receiver-hostname
1.3.6.1.4.1.791.9845.2.46	receiver-hostaddress
1.3.6.1.4.1.791.9845.2.47	receiver-hostdomainname
1.3.6.1.4.1.791.9845.2.48	receiver-port
1.3.6.1.4.1.791.9845.2.49	receiver-time-gmt
1.3.6.1.4.1.791.9845.2.50	receiver-timezone

Objekt-ID (OID)	CEG-Feld
1.3.6.1.4.1.791.9845.2.51	receiver-version
1.3.6.1.4.1.791.9845.2.52	event-protocol
1.3.6.1.4.1.791.9845.2.53	event-logname
1.3.6.1.4.1.791.9845.2.54	event-euuid
1.3.6.1.4.1.791.9845.2.55	event-count
1.3.6.1.4.1.791.9845.2.56	event-summarized
1.3.6.1.4.1.791.9845.2.57	event-duration
1.3.6.1.4.1.791.9845.2.58	event-time-year
1.3.6.1.4.1.791.9845.2.59	event-time-month
1.3.6.1.4.1.791.9845.2.60	event-time-monthday
1.3.6.1.4.1.791.9845.2.61	event-time-weekday
1.3.6.1.4.1.791.9845.2.62	event-time-hour
1.3.6.1.4.1.791.9845.2.63	event-time-minute
1.3.6.1.4.1.791.9845.2.64	event-time-gmt
1.3.6.1.4.1.791.9845.2.65	event-datetime
1.3.6.1.4.1.791.9845.2.66	event-year-datetime
1.3.6.1.4.1.791.9845.2.67	event-month-datetime
1.3.6.1.4.1.791.9845.2.68	event-day-datetime
1.3.6.1.4.1.791.9845.2.69	event-hour-datetime
1.3.6.1.4.1.791.9845.2.70	event-quarterhour-datetime
1.3.6.1.4.1.791.9845.2.71	event-minute-datetime
1.3.6.1.4.1.791.9845.2.72	event-timezone
1.3.6.1.4.1.791.9845.2.73	event-sequence
1.3.6.1.4.1.791.9845.2.74	event-trend
1.3.6.1.4.1.791.9845.2.75	event-action
1.3.6.1.4.1.791.9845.2.76	event-id
1.3.6.1.4.1.791.9845.2.77	event-category
1.3.6.1.4.1.791.9845.2.78	event-class

Objekt-ID (OID)	CEG-Feld
1.3.6.1.4.1.791.9845.2.79	ideal-model
1.3.6.1.4.1.791.9845.2.80	event-severity
1.3.6.1.4.1.791.9845.2.81	event-result
1.3.6.1.4.1.791.9845.2.82	result-string
1.3.6.1.4.1.791.9845.2.83	result-signature
1.3.6.1.4.1.791.9845.2.84	result-code
1.3.6.1.4.1.791.9845.2.85	result-version
1.3.6.1.4.1.791.9845.2.86	result-priority
1.3.6.1.4.1.791.9845.2.87	result-scope
1.3.6.1.4.1.791.9845.2.88	result-severity
1.3.6.1.4.1.791.9845.2.89	raw-event

Benutzerdefinierte MIBs

Sie können benutzerdefinierte MIB-Dateien aus dem zur Verfügung gestellten "Boilerplate"-Text erstellen, indem Sie ausgewählte Varbinds (variable Bindungen) aus dem CA-ELM.MIB-Dateiinhalt hinzufügen. Eine benutzerdefinierte MIB-Datei für einen einzigen Alarm enthält einen Teil der Inhalte der CA-ELM.MIB-Datei. Eine benutzerdefinierte MIB-Datei für einen Alarm unterscheidet sich von CA-ELM.MIB auf folgende Weise:

- Die benutzerdefinierte MIB definiert nur die von diesem Alarm gesendeten Felder.
- Die benutzerdefinierte MIB definiert eine Trap, die diese Felder in der Sequenz auflistet, in der sie gesendet werden.
- Die benutzerdefinierte MIB-Trap wird mit der OID 1.3.6.1.4.1.791.9845.3.x angegeben, wobei x ein Wert zwischen 1 und 999 ist.

  Hinweis: Ein Alarm, der eine benutzerdefinierte MIB verwendet, legt diese OID als den Wert für die benutzerdefinierte Trap-ID fest.
- Eine benutzerdefinierte MIB enthält *nur dann* die dynamicData-Varbind, wenn die Abfrage berechnete Felder berücksichtigt.

  Berechnungen können auf jedes beliebige Feld angewendet werden. Das Feld "event_count" ist ein Beispielfeld, auf das normalerweise Berechnungen angewendet sind, jedoch nicht immer. "Event_count" ist in der Abfrage "Systemereignisanzahl nach Ereignisaktion" ein berechnetes Feld; es wird mit "Sum" berechnet. Um zu bestimmen, ob ein Feld berechnet ist, prüfen Sie die Abfrage, in der das Feld definiert ist. Es folgt ein Beispiel einer Definition von "event_count" als berechnetes Feld:

  ```
  System_Event_Count_By_Event_Action.xml:    <Column columnname="event_count"
  datatype="I" displayname="Count" functionname="sum" resultname="event_count"
  sortdesc="true" sortorder="1" visible="true"/>
  ```

"Boilerplate"-Text für eine benutzerdefinierte MIB

"Boilerplate"-Text für eine benutzerdefinierte MIB folgt. Wenn Sie eine benutzerdefinierte MIB mit diesem Beispiel starten, können Sie in Speicherorten, die mit der Zeichenfolge ### angezeigt werden, benutzerdefinierte Daten ersetzen oder sie darin einfügen. In Abschnitten, in denen Sie Daten ändern, können Sie optional die Beschreibung ändern.

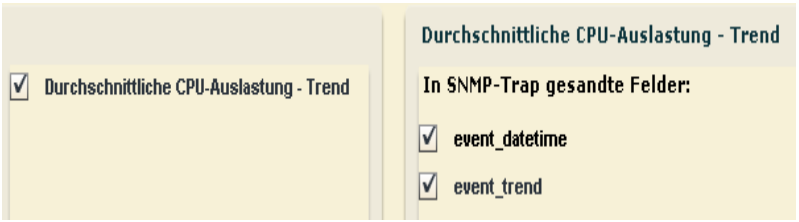
```
CAELM-MIB DEFINITIONS ::= BEGIN
  IMPORTS
        MODULE-IDENTITY, OBJECT-TYPE, Integer32, NOTIFICATION-TYPE
                FROM SNMPv2-SMI
MODULE-COMPLIANCE, OBJECT-GROUP,NOTIFICATION-GROUP
                FROM SNMPv2-CONF                        DisplayString
               FROM SNMPv2-TC;

elm MODULE-IDENTITY
    LAST-UPDATED "200907050600Z"
    ORGANIZATION "CA"
    CONTACT-INFO
        "100 Staples drive
        Framingham MA"
    DESCRIPTION
        "Contains objects describing data for ELM events"
    REVISION "200907050600Z"
    DESCRIPTION
        "Custom MIB <###>."
    ::= { ca 9845 }

ca OBJECT IDENTIFIER ::= {enterprises 791}
elmAlertTrapGroup OBJECT IDENTIFIER ::= { elm 3 }
elmAlertVariables OBJECT IDENTIFIER ::= { elm 2 }
elmDynamicVariables OBJECT IDENTIFIER ::= { elm 4 }
elmConformance OBJECT IDENTIFIER ::= { elm 5 }
elmGroups      OBJECT IDENTIFIER ::= { elmConformance 1 }
elmCompliances OBJECT IDENTIFIER ::= { elmConformance 2 }


<###-Geben Sie die elmAlertVariable-Varbind für jedes Abfragefeld ein ###>
```

```
<###-Geben Sie folgende dynamicData-Varbind nur ein, wenn die Abfrage berechnete
Felder einschließt ###>
dynamicData OBJECT-TYPE
    SYNTAX DisplayString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
" This field contains all the elm dynamic variables and data in name=value
format."
    ::= { elmDynamicVariables 2 }

calmAPIURL OBJECT-TYPE
    SYNTAX  OCTET STRING
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
"The OPEN API URL which points to the query result."
    ::= { elmDynamicVariables 1 }

elmTrap NOTIFICATION-TYPE
    OBJECTS {<### Geben Sie die Liste der Abfragefelder mit Bindestrichen ein
###>}
    STATUS  current
    DESCRIPTION
            "The ELM SNMP Trap."
    ::= {elmAlertTrapGroup-<### Geben Sie die Knotennummer der
benutzerdefinierten Trap-ID ein ###>}

elmCompliance MODULE-COMPLIANCE
    STATUS  current
    DESCRIPTION
            "The compliance information."
    MODULE  -- this module
        GROUP       elmDataGroup
        DESCRIPTION
            "This group is mandatory."
    ::= { elmCompliances 3 }
-- units of conformance

elmDataGroup    OBJECT-GROUP
    OBJECTS {<### Geben Sie die Liste der Abfragefelder mit Bindestrichen ein
###>}
    STATUS  current
    DESCRIPTION
            "A collection of objects providing information specific to
            ELM data."
    ::= { elmGroups 1 }
END
```

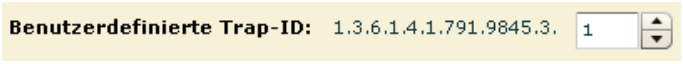
Beispiel: Erstellen von benutzerdefinierter MIB 33 für die Abfrage "Durchschnittliche CPU-Auslastung - Trend"

Erstellen Sie eine benutzerdefinierte MIB für jede Abfrage, die als SNMP-Trap an CA NSM gesendet wurde. Jede solche Abfrage ist mit einer benutzerdefinierten Trap-ID verbunden Die benutzerdefinierte MIB definiert die Felder, die ausgewählt wurden, um in der gleichen Reihenfolge wie im Aktionsalarm angezeigt in das Trap eingeschlossen zu werden.

Beachten Sie das Beispiel, in dem die für den Aktionsalarm ausgewählte Abfrage "Durchschnittliche CPU-Auslastung - Trend" lautet. Die ausgewählten Felder sind "event_datetime" und "event_trend".



Die benutzerdefinierte Trap-ID lautet 1.3.6.1.4.1.791.9845.3.33.



So erstellen Sie eine benutzerdefinierte MIB für die benutzerdefinierte Trap-ID, die auf 33 endet

1. Öffnen Sie eine Kopie von CA-ELM.MIB und kopieren Sie Text in Ihre benutzerdefinierte MIB.
2. Öffnen Sie einen Editor, kopieren Sie den "Boilerplate"-Text für die benutzerdefinierte MIB und speichern Sie die Datei unter neuem Namen ab. Speichern Sie sie zum Beispiel als benutzerdefinierte MIB n.mib, wobei "n" 33 ist, entsprechend dem letzten Knoten der benutzerdefinierten Trap-ID, die für die Abfrage im Aktionsalarm festgelegt wurde.
3. (Optional) Ersetzen Sie unter MODULE-IDENTITY <###> durch 33. Beispiel:

```
Custom MIB 33."
```

4. Ersetzen Sie folgenden "Boilerplate"-Text durch Text aus CA-ELM.MIB.

   ```
   <### Geben Sie die elmAlertVariable-Varbind für jedes Abfragefeld in Trap-
   Sequenz ein ###>
   ```

   Kopieren Sie die elmAlertVariable-Varbinds für "event_datetime" und dann für "event_trend". Diese Varbinds müssen in der MIB in der gleichen Sequenz erscheinen, in der Sie in der SNMP-Trap gesendet werden. Beispiel:

   ```
   event-datetime OBJECT-TYPE
       SYNTAX DisplayString
       MAX-ACCESS  read-only
       STATUS      current
       DESCRIPTION
   "The calendar date and time expressed in the event information"
       ::= { elmAlertVariables 65 }

   event-trend OBJECT-TYPE
       SYNTAX Integer32
       MAX-ACCESS  read-only
       STATUS      current
       DESCRIPTION
   "Trending data for this event."
       ::= { elmAlertVariables 74 }
   ```

5. Da keine der Felder in dieser Abfrage berechnete Felder sind, löschen Sie folgenden "Boilerplate"-Text:

   ```
   <###-Geben Sie folgende dynamicData-Varbind nur ein, wenn die Abfrage
   berechnete Felder einschließt ###>
   dynamicData OBJECT-TYPE
       SYNTAX DisplayString
       MAX-ACCESS  read-only
       STATUS      current
       DESCRIPTION
   " This field contains all the elm dynamic variables and data in name=value
   format."
       ::= { elmDynamicVariables 2 }
   ```

6. Ersetzen Sie folgenden "Boilerplate"-Text unter elmTrap

   ```
   OBJECTS {<### Geben Sie die Liste der Abfragefelder mit Bindestrichen ein
   ###>}
   ```

   mit der Liste der ausgewählten Abfragefelder wie folgt:

   ```
   OBJECTS { event-datetime,event-trend }
   ```

7. Ersetzen Sie folgenden "Boilerplate"-Text unter elmTrap

   ```
   ::= {elmAlertTrapGroup-<### Geben Sie die Knotennummer der
   benutzerdefinierten Trap-ID ein ###>}
   ```

   mit:

   ```
   ::= { elmAlertTrapGroup 33 }
   ```

8. Ersetzen Sie folgenden "Boilerplate"-Text unter elmDataGroup:

   ```
   OBJECTS {<### Geben Sie die Liste der Abfragefelder mit Bindestrichen ein
   ###>}
   ```

   mit:

   ```
   OBJECTS { event-datetime,event-trend }
   ```

9. Speichern Sie die Datei.

Beispiel: Custom MIB 33

Das folgende Beispiel ist eine benutzerdefinierte MIB, die für einen Aktionsalarm entwickelt wurde, der als eine SNMP-Trap mit der benutzerdefinierten Trap-ID mit der Endung 33 gesendet wurde. Die benutzerdefinierte Trap-ID lautet E 1.3.6.1.4.1.791.9845.3.33. Die ausgewählte Abfrage "Durchschnittliche CPU-Auslastung - Trend" und die Felder, die ausgewählt wurden, um in der SNMP-Trap gesendet zu werden, sind "event_datetime" und "event_trend".

```
CAELM-MIB DEFINITIONS ::= BEGIN
  IMPORTS
        MODULE-IDENTITY, OBJECT-TYPE, Integer32, NOTIFICATION-TYPE
                FROM SNMPv2-SMI
MODULE-COMPLIANCE, OBJECT-GROUP,NOTIFICATION-GROUP
                FROM SNMPv2-CONF                          DisplayString
               FROM SNMPv2-TC;

elm MODULE-IDENTITY
    LAST-UPDATED "200907050600Z"
    ORGANIZATION "CA"
    CONTACT-INFO
        "100 Staples drive
        Framingham MA"
    DESCRIPTION
        "Contains objects describing data for ELM events"
    REVISION "200907050600Z"
    DESCRIPTION
        "Custom MIB 33."
    ::= { ca 9845 }
```

```
ca OBJECT IDENTIFIER ::= { enterprises 791}
elmAlertTrapGroup OBJECT IDENTIFIER ::= { elm 3 }
elmAlertVariables OBJECT IDENTIFIER ::= { elm 2 }
elmDynamicVariables OBJECT IDENTIFIER ::= { elm 4 }
elmConformance OBJECT IDENTIFIER ::= { elm 5 }
elmGroups      OBJECT IDENTIFIER ::= { elmConformance 1 }
elmCompliances OBJECT IDENTIFIER ::= { elmConformance 2 }

event-datetime OBJECT-TYPE
    SYNTAX DisplayString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
"The calendar date and time expressed in the event information"
    ::= { elmAlertVariables 65 }

event-trend OBJECT-TYPE
    SYNTAX  Integer32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
"Trending data for this event."
    ::= { elmAlertVariables 74 }

calmAPIURL OBJECT-TYPE
    SYNTAX  OCTET STRING
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
"The OPEN API URL which points to the query result."
    ::= { elmDynamicVariables 1 }

elmTrap NOTIFICATION-TYPE
    OBJECTS { event-datetime,event-trend }
    STATUS  current
    DESCRIPTION
            "The ELM SNMP Trap."
    ::= { elmAlertTrapGroup 33 }
```

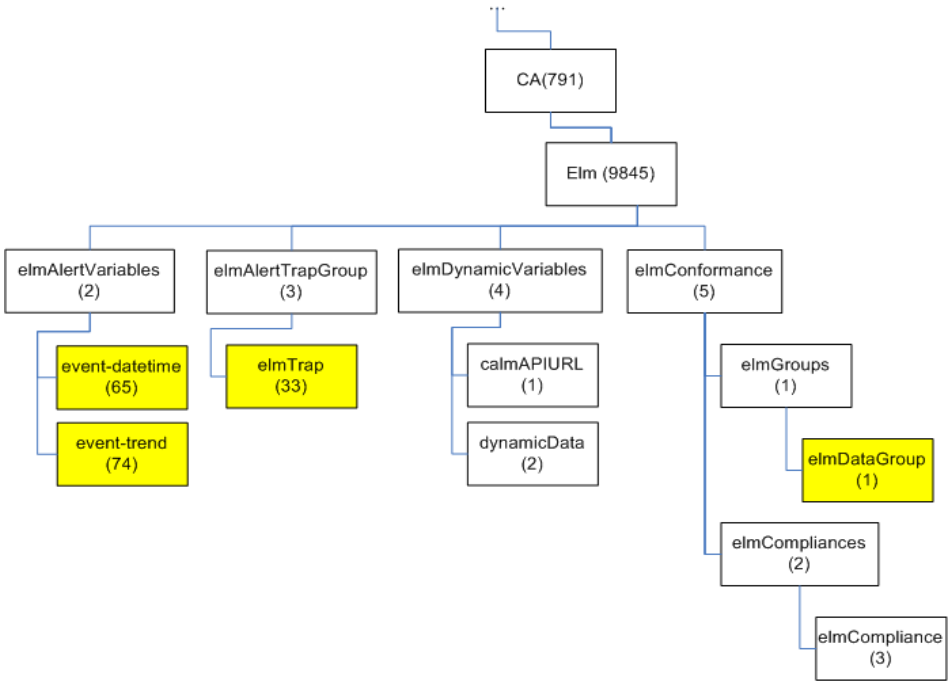
```
elmCompliance MODULE-COMPLIANCE
    STATUS  current
    DESCRIPTION
            "The compliance information."
    MODULE  -- this module
        GROUP       elmDataGroup
        DESCRIPTION
            "This group is mandatory."
    ::= { elmCompliances 3 }
-- units of conformance

elmDataGroup    OBJECT-GROUP
    OBJECTS {  event-datetime,event-trend }
    STATUS  current
    DESCRIPTION
            "A collection of objects providing information specific to
            ELM data."
    ::= { elmGroups 1 }
END
```

Beispiel: MIB-Baumstruktur für benutzerdefinierte MIB 33

Die MIB-Baumstruktur für eine benutzerdefinierte MIB unterscheidet sich von der MIB-Baumstruktur für CA-ELM.MIB auf folgende Weise:

- Die Objekte unter elmAlertVariables sind auf die Felder in der Abfrage beschränkt. Beachten Sie das Beispiel, in dem die ausgewählten Felder folgende sind:
  - event_datetime
  - event_trend
- Die elmTrap, die nur die Abfragefelder enthält, ersetzt elmTrap (1) in CA-ELM.MIB, die alle CEG-Felder enthält. Beachten Sie das Beispiel, in dem die elmTrap 33 ist. Diese elmTrap-ID bezieht sich auf den letzten Knoten der benutzerdefinierten Trap-ID, die 1.3.6.1.4.1.791.9845.3.33 lautet.

Eine Darstellung der benutzerdefinierten MIB 33 in MIB-Baumstrukturformat folgt, in der die hervorgehobenen Blöcke Unterschiede zwischen dieser benutzerdefinierten MIB und der CA-ELM.MIB anzeigen. Die benutzerdefinierte MIB definiert nur zwei Felder unter elmAlertVariables. Die benutzerdefinierte elmTrap enthält nur die beiden Abfragefelder und besitzt eine eindeutige Nummer, 33. Die elmDataGroup enthält nur die beiden Abfragefelder.



Hinweise zur MIB-Verwendung

Damit ein System eine SNMP-Trap verstehen kann, die es von CA Enterprise Log Manager unter Verwendung von MIBs erhält, muss es wissen, für was die entsprechenden OIDs stehen. Die Anforderungen lauten wie folgt:

- Importieren Sie und kompilieren Sie die CA-ELM.MIB-Datei; halten Sie diese Datei aktualisiert.
- (Nur CA NSM) Erstellen, importieren und kompilieren Sie eine benutzerdefinierte MIB für jeden geplanten Alarm, der als SNMP-Trap gesendet wurde.

  Hinweis: Dieselbe benutzerdefinierte MIB kann für Alarme verwendet werden, die auf Abfragen basieren, welche die gleichen Felder in der gleichen Reihenfolge als Trap senden.

  Zum Beispiel geben alle der folgenden Abfragen Werte für die Felder "dest_hostname" und "event_count" zurück.

  - Fünf - Fehlgeschlagener Systemzugriff nach System
  - Fehlgeschlagene Wiederherstellung in den letzten sieben Tagen nach Host - Übersicht
  - Fehlgeschlagene Sicherung in den letzten sieben Tagen nach Host - Übersicht
  - Übermäßige (25) Konfigurationsfehler in der vergangenen Stunde
  - Übermäßige (25) Konfigurationsänderungen in der vergangenen Stunde
  - Übermäßige (25) SU-Aktivität nach Host in der vergangenen Stunde
  - Kritische oder schwerwiegende Ereignisse auf kritischem Host - Übersicht

  Wenn Sie auf der Basis dieser Alarme getrennte Abfragen erstellen, würden diese Alarme die gleiche benutzerdefinierte Trap-ID angeben und mit der gleichen benutzerdefinierten MIB interpretiert werden.

Personen, die die am Zielprodukt erhaltenen SNMP-Traps überwachen, können von CA Enterprise Log Managergesendete Traps auf zwei Weisen interpretieren:

- Starten Sie die Ergebnisseite für SNMP-Traps über die in der Trap gesendeten URL.
- Verwenden Sie eine Anwendung, die sich auf importierte MIBs bezieht.

Arbeiten mit SNMP-Traps

Für die Verwendung von SNMP-Traps sind folgende Schritte erforderlich:

1. Bereiten Sie CA Enterprise Log Manager auf das Senden von SNMP-Traps vor.
   - Konfigurieren Sie das Standardziel für SNMP-Traps.
   - Ermitteln Sie die IP-Adresse und den Port für jedes zusätzliche SNMP-Trap-Ziel, das Sie angeben können, wenn Alarme als SNMP-Traps gesendet werden.
   - Ermitteln Sie Alarme, deren Abfrageergebnisse für CA Spectrum, CA NSM oder andere Empfänger von SNMP-Traps von Interesse wären.
2. Bereiten Sie die SNMP-Trap-Zielprodukte auf den Empfang der von CA Enterprise Log Manager gesendeten SNMP-Traps vor.
   - Falls CA Spectrum ein Ziel ist:
     - Erstellen Sie mit Hilfe der Dokumentation zu CA Spectrum ein Ereignismodell. Ohne Ereignismodell können Sie Trap-Ergebnisse nicht am Ziel anzeigen.
     - Vorbereiten von CA Spectrum für den Empfang von SNMP-Traps der Version 3.
   - Falls CA NSM ein Ziel ist:
     - Installieren Sie NSM r11.2 (GA-Build) auf Windows Server 2003 EE SP1, und wenden Sie den Patch an, um die Datei "aws_snmpex.dll" zu aktualisieren.
     - Konfigurieren Sie CA NSM für den Empfang von SNMP-Traps, SNMP-Traps der Version 3 eingenommen.

3. (Optional) Bereiten Sie das SNMP-Trap-Ziel auf die Interpretation der von CA Enterprise Log Manager mit MIBs gesendeten SNMP-Traps vor.
   - Laden Sie die CA Enterprise Log Manager-MIB an einen Speicherort herunter, auf den Sie von Ihrem SNMP-Trap-Zielprodukt aus zugreifen können.

     Hinweis: Die Datei "CA-ELM.MIB" befindet sich auf der Installations-DVD. Die neueste Version dieser MIB finden Sie auf der Produktseite für CA Enterprise Log Manager.
   - Importieren und kompilieren Sie die CA-ELM.MIB-Datei.
   - (Nur CA NSM.) Erstellen Sie, damit jeder Alarm als eine SNMP-Trap gesendet wird, eine benutzerdefinierte MIB mit einer mit 1.3.6.1.4.1.791.9845.3.x definierten Trap, wobei x einer Ganzzahl gleich oder kleiner 999 entspricht. Importieren und kompilieren Sie alle benutzerdefinierten MIBs.

   Wichtig! Dieser Schritt ist optional, da von CA Enterprise Log Manager erhaltene Traps durch Starten der Trap-Ergebnisseite über die in der Trap gesendeten URL interpretiert werden können.
4. Planen Sie Alarme mit SNMP-Trap-Zielen.
5. Stellen Sie sicher, dass der Alarm erfolgreich als SNMP-Trap gesendet wurde.
6. (Optional) Überwachen Sie die Ergebnisse gesendeter SNMP-Traps vom Trap-Ziel aus.
   - Zeigen Sie die SNMP-Trap-Ergebnisse am Trap-Ziel an.
   - Starten Sie die URL, um die von dem Alarm gesendeten Daten als Graphik oder Diagramm anzuzeigen.

Konfigurieren der Integration mit einem SNMP Trap-Ziel

Konfigurieren Sie die SNMP-Integration im Rahmen der Global Service-Konfiguration für den Berichtsserver. Die Konfiguration umfasst die IP-Adresse und den Port eines SNMP-Trap-Ziels.

Sie können die SNMP-Integration entweder vor oder nach der Vorbereitung des Zielprodukts für das Empfangen und Auswerten von SNMP-Traps von CA Enterprise Log Manager konfigurieren.

Wenn Sie einen Alarm für einen SNMP-Trap-Empfänger erstellen, können Sie ein oder mehrere Ziele angeben. Bei dieser Konfiguration handelt es sich um die Standardkonfiguration. Sie gilt für alle Server, die unter "Berichtsserver" aufgelistet werden.

So konfigurieren Sie die SNMP-Integration:

1. Klicken Sie auf die Registerkarte "Verwaltung" und auf die Unterregisterkarte "Services".
2. Klicken Sie auf "Alarm-Service".
3. Geben Sie die IP-Adresse oder den Hostnamen des Zielservers für die SNMP-Traps ein.
4. Übernehmen Sie den Standardport "162", oder ändern Sie ihn.
5. Klicken Sie auf "Speichern".

Vorbereiten von CA Spectrum für den Empfang von SNMP-Traps aus Alarmen

Sie können Alarme in Form von SNMP-Traps von CA Enterprise Log Manager an jedes Ziel in Ihrem Netzwerk senden, das Traps empfangen und interpretieren kann. Jeder Trap-Empfänger hat eigene Anforderungen.

Bereiten Sie CA Spektrum für den Empfang von Traps aus CA Enterprise Log Manager-Aktionsalarmen vor, durch:

- Erstellen einer CA Spectrum Southbound Gateway-Integration, ein Integrationspunkt, der jedes Datenstromformat für eingehende Alarme von Drittanbietersystemen unterstützt, darunter SNMP-Traps, wie sie von CA Enterprise Log Manager generiert werden.
- Erstellen eines Modells des CA Enterprise Log Manager-Knotens, um den Empfang von SNMP-Traps der Version 3 zu aktivieren.
- Herunterladen der CA Enterprise Log Manager-MIB.
- Importieren der CA Enterprise Log Manager-MIB in CA Spectrum.

Der Prozess für das Erstellen einer Southbound Gateway-Integration ist im Handbuch von *Spectrum Southbound Gateway Toolkit* vollständig dokumentiert. Das Erstellen einer Southbound Gateway-Integration beinhaltet die Zuordnung von SNMP-Traps zu CA Spektrum-Ereignissen in einer AlertMap-Datei, sowie das Definieren der erforderlichen Modelle. Der Southbound Gateway-Integrationspunkt akzeptiert Alarmdaten von Drittanbietersystemen und zeigt sie in OneClick an.

Um die MIB-Datei in CA Spectrum zu importieren, müssen Sie sie von der CA Enterprise Log Manager-Produktseite des Online-Supports herunterladen oder auf der Installations-DVD suchen. Weitere Informationen zum Verwenden des MIB-Tools für den Import in CA Spectrum OneClick finden Sie im *Benutzerhandbuch des CA Spectrum-Gerätemanagements*.

Konfigurieren von CA Spectrum für den Empfang von SNMPv3-Traps

Bevor Sie SNMPv3-Traps von CA Enterprise Log Manager an CA Spectrum senden können, müssen Sie in CA Spectrum ein Modell der CA Enterprise Log Manager-Anwendung erstellen. SNMPv3-Traps werden dann an den von Ihnen modellierten CA Enterprise Log Manager-Knoten weitergeleitet.

So erstellen Sie ein Modell, mit dessen Hilfe CA Spectrum SNMPv3-Traps aus Aktionsalarmen empfangen kann:

1. Melden Sie sich bei dem Windows-Server an, auf dem CA Spectrum installiert ist.
2. Rufen Sie die Spectrum OneClick-Konsole auf.
   a. Klicken Sie im Menü "Start" auf "Alle Programme", "CA" und "SPECTRUM Control Panel" (SPECTRUM-Steuerkonsole).

      Die SPECTRUM Control Panel (SPECTRUM-Steuerkonsole) wird angezeigt. Im unteren Bereich des Fensters befindet sich eine Statusanzeige.

   b. Falls unter "Status" (Status) nicht RUNNING (WIRD AUSGEFÜHRT) angezeigt wird, klicken Sie unter "Process Control" (Prozesssteuerung) auf "Start SpectroSERVER" (SpectroSERVER starten).

   c. Wird unter "Status" (Status) die Angabe RUNNING (WIRD AUSGEFÜHRT) angezeigt, klicken Sie auf "OneClick Administration" (OneClick-Administration).

      Das Fenster "OneClick Administration - SPECTRUM Control Panel" (OneClick-Administration - SPECTRUM-Steuerkonsole) wird angezeigt. Darin ist "Host" (Host) auf "localhost" und "Port" (Port) auf 80 eingestellt.

   d. Klicken Sie auf OK.

      Ein Anmeldedialogfeld wird angezeigt.

   e. Geben Sie Ihre Anmeldeinformationen ein.

      Die Seite "SPECTRUM NFM OneClick" (SPECTRUM NFM OneClick) wird angezeigt.

   f. Klicken Sie auf "Start Console" (Konsole starten).

      Das Dialogfeld "Login - SPECTRUM OneClick" (Anmeldung - SPECTRUM OneClick) wird angezeigt. Darin können Sie eine Verbindung zu SPECTRUM OneClick auf dem lokalen Host herstellen.

   g. Klicken Sie auf OK.

Das Fenster "Console - SPECTRUM OneClick" (Konsole - SPECTRUM OneClick) wird angezeigt. Es enthält einen Bereich "Navigation" (Navigation), einen Bereich "Contents" (Inhalt) und einen Bereich "Component Detail" (Komponentendetails).

3. Blenden Sie im Bereich "Navigation" (Navigation) auf der Registerkarte "Explorer" (Explorer) den obersten Knoten ein, und wählen Sie "Universe" (Universe) aus.

   Als Titel der Bereiche "Contents" (Inhalt) und "Component Detail" (Komponentendetails) wird "Universe of type Universe" (Universe vom Typ Universe) angezeigt.

4. Klicken Sie im Bereich "Contents" (Inhalt) auf die Registerkarte "Topology" (Topologie).

   Über die zweite Schaltfläche auf der Registerkarte können Sie anhand des Typs ein neues Modell erstellen und es dieser Ansicht hinzufügen.

5. Klicken Sie auf "Create a new model" (Neues Modell erstellen).

   Das Dialogfeld "Select Model Type - SPECTRUM OneClick" (Modelltyp auswählen - SPECTRUM OneClick) wird angezeigt.

6. Klicken Sie auf die Registerkarte "All Model Types" (Alle Modelltypen).

7. Geben Sie im Feld "Filter" (Filter) eine Zeichenfolge ein. Geben Sie beispielsweise "gn" ein.

   In der Liste werden Modelltypen angezeigt, die mit "Gn" beginnen.

8. Wählen Sie den gewünschten Modelltyp aus, und klicken Sie auf "OK". Wählen Sie beispielsweise "GnSNMPDev" aus, und klicken Sie auf "OK".

   Das Dialogfeld "Create Model of Type" (Modell vom Typ <ausgewählter Modelltyp> erstellen) wird geöffnet.

9. Geben Sie im Dialogfeld "Create Model of Type" (Modell vom Typ <ausgewählter Modelltyp> erstellen) folgende Daten ein:

   a. Geben Sie im Feld "Name" (Name) den Hostnamen des CA Enterprise Log Manager-Servers ein.

   b. Geben Sie im Feld "Network Address" (Netzwerkadresse) die IP-Adresse dieses Servers ein.

   c. Geben Sie im Feld "Agent Port" (Agentenport) einen Port ein, wenn der Standardwert 161 nicht Ihren Anforderungen entspricht. Geben Sie beispielsweise den Wert 162 ein.

   d. Wählen Sie unter "SNMP Communication" (SNMP-Kommunikation) die Option "SNMP v3" (SNMP v3) aus.

   e. Klicken Sie auf "Profiles" (Profile).

   Das Fenster "Edit SNMP v3 Profiles" (SNMPv3-Profile) wird mit einer Liste bestehender Profile angezeigt, sofern Profile vorhanden sind.

10. So fügen Sie ein Profil hinzu:

    a. Geben Sie den Profilnamen und die Benutzer-ID ein.

    b. Da Sie das Profil für SNMPv3 hinzufügen, wählen Sie als Authentifizierungstyp "Authentication with Privacy" (Authentifizierung mit geheimem Kennwort) aus.

    c. Geben Sie in den nächsten vier Feldern ein aus acht Zeichen bestehendes Authentifizierungskennwort und dann zweimal ein aus acht Zeichen bestehendes geheimes Kennwort ein.

    d. Klicken Sie auf "Add" (Hinzufügen), um das Profil zur Liste hinzuzufügen.

    e. Klicken Sie auf OK.

    Das hinzugefügte Profil wird im Dialogfeld "Create Model of Type" (Modell vom Typ <ausgewählter Modelltyp> erstellen) in der Dropdown-Liste "V3 Profile" (Profil für Version 3) zuoberst angezeigt.

11. Wählen Sie "Discover Connections" (Verbindungen ermitteln) aus, und klicken Sie auf "OK".

    Die Fortschrittsanzeige "Creating Model" (Modell wird erstellt) wird angezeigt. Nach Abschluss der Verarbeitung wird das erstellte Modell auf der Registerkarte "Topology" (Topologie) als Grafik mit dem Hostnamen, den Sie eingegeben haben, und dem von Ihnen ausgewählten Modelltyp angezeigt.

Herunterladen von CA Enterprise Log Manager MIB

Sie können die MIB-Datei von der CA Enterprise Log Manager-Produktseite unter "Support Online" herunterladen. Alternativ befindet sich die Datei auch auf der Installations-DVD. Nachdem Sie die CA Enterprise Log Manager-MIB heruntergeladen haben, können Sie sie in jedes Produkt importieren, das Sie als SNMP-Trap-Ziel konfiguriert haben, und dort kompilieren.

So laden Sie die CA Enterprise Log Manager-MIB herunter:

1. Melden Sie sich bei dem Server an, auf dem Sie CA Spectrum installiert haben.
2. Starten Sie "CA Support Online", und melden Sie sich an.
3. Wechseln Sie zur CA Enterprise Log Manager-Produktseite.
4. Laden Sie die CA Enterprise Log Manager MIB-Datei in Ihr Netzwerk herunter.
5. Wenn Sie SNMP-Traps an CA Spectrum senden möchten, importieren Sie die CA Enterprise Log Manager MIB in CA Spectrum.
6. Wenn Sie SNMP-Traps an CA NSM senden möchten, importieren Sie die CA Enterprise Log Manager MIB in CA NSM. Weitere Informationen hierzu finden Sie in der Dokumentation von CA NSM.

Importieren der CAELM-MIB in CA Spectrum

Bevor Sie SNMP-Traps von CA Enterprise Log Manager an CA Spectrum senden, können Sie die CA Enterprise Log Manager-MIB mit den CA Spectrum OneClick-MIB-Tools importieren und kompilieren.

Hinweis: Die SNMPv2 MIBs, die in CA-ELM.MIB referenziert werden, sind ein CA Spectrum bereits geladen.

So importieren Sie die CA-ELM.MIB in CA Spectrum:

1. Melden Sie sich bei CA Spectrum an.
2. Starten Sie die OneClick-Konsole.
3. Klicken Sie auf "Tools", "Utilities", "MIB Tools".

   Das Dialogfeld "MIB Tools: Add MIB" wird geöffnet.
4. Klicken Sie auf "Browse", navigieren Sie zu dem Speicherort, unter dem Sie die CA-ELM.MIB gespeichert haben, und wählen Sie diese Datei aus.

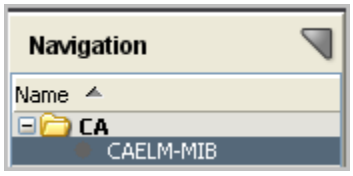
5. Klicken Sie auf "Compile".

   Eine Meldung zeigt an, dass die CA Enterprise Log Manager-MIB-Datei erfolgreich im folgenden Verzeichnis des OneClick-Webserver gespeichert wurde:

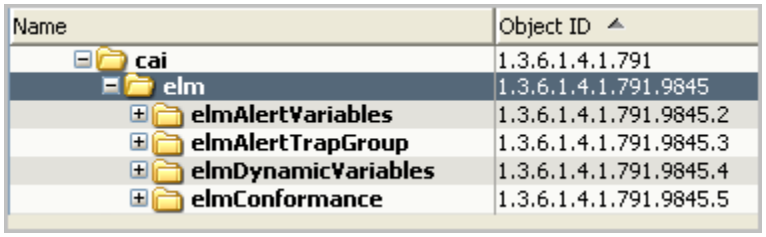
   `<$SPECROOT>/MibDatabase/userContrib`

6. Schließen Sie das Dialogfeld "MIB Tools: Add MIB".

   CAELM-MIB wird in der Navigationsleiste unter "CA" hinzugefügt.



   In der Hierarchie wird "cai" erweitert, und es wird "elm" mit den untergeordneten Strukturobjekten und den damit verknüpften OIDs angezeigt.



Beispiel: Benachrichtigung von CA Spectrum über Konfigurationsänderungen

Bevor Sie SNMP-Traps zum ersten Mal an CA Spectrum senden, empfehlen wir, die Abfragen zu identifizieren, die Ergebnisse für dieses Ziel zurückgeben. Wenn Sie Ihren ersten Alarm mit Spectrum als Ziel planen, möchten Sie möglicherweise den Fortschritt verfolgen und die Ergebnisse in CA Enterprise Log Manager mit denen in CA Spectrum vergleichen. Wenn das Versenden von Traps an CA Spectrum Routine geworden ist, sind diese Vorbereitungen meist nicht mehr notwendig.

Im folgenden Beispiel werden Sie schrittweise durch den anfänglichen Prozess geführt. Dazu gehört:

- Vorbereitungen für das Senden von SNMP-Traps an CA Spectrum
- Versenden von Traps an CA Spectrum
- Überprüfen des erfolgreichen Versendens von SNMP-Traps
- Anzeigen der von CA Spectrum empfangenen SNMP-Traps

Weitere Informationen:

Versenden von SNMPv2-Traps an CA Spectrum (siehe Seite 474)
Verfolgen des Alarmjobfortschritts (siehe Seite 476)
Anzeigen von SNMP-Traps in CA Spectrum (siehe Seite 477)

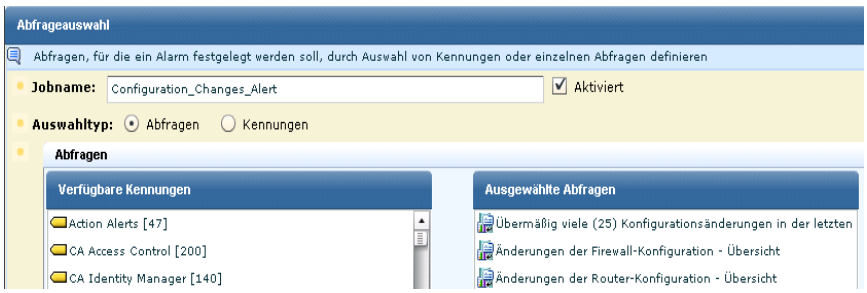
Versenden von SNMPv2-Traps an CA Spectrum

Das folgende Beispiel zeigt, wie Sie einen Alarm erstellen, der CA Spectrum mit SNMPv2-Traps über Konfigurationsänderungen informiert.

So versenden Sie SNMPv2-Traps an CA Spectrum:

1. Öffnen Sie den Assistenten für die Alarmplanung.
   a. Klicken Sie auf die Registerkarte "Alarmverwaltung" und auf die Unterregisterkarte "Alarmplanung".
   b. Klicken Sie auf die Schaltfläche "Aktionsalarm planen".
2. Vervollständigen Sie den Schritt "Alarmauswahl".
   a. Geben Sie einen Jobnamen ein. Dies ist für alle Alarme notwendig.
   b. Vergewissern Sie sich, dass unter "Auswahltyp" die Auswahl "Abfragen" aktiviert ist.

      Für Alarme, die auf Kennungen basieren, können keine SNMP-Trap-Ziele ausgewählt werden.
   c. Wenn die gewünschten Abfragen die Kennung "Aktionsalarme" verwenden, klicken Sie auf die Kennung "Aktionsalarme", um die angezeigte Liste zu filtern.
   d. Wählen Sie die ermittelten Abfragen aus.



3. (Optional) Führen Sie die Schritte "Alarmfilter", "Ergebnisbedingungen" und "Jobs planen" wie in der Online-Hilfe für diesen Assistenten beschrieben durch.

4. Legen Sie die SNMP-Trap-Details fest.
   a. Klicken Sie auf den Schritt "Ziel".
   b. Klicken Sie auf die Registerkarte "SNMP-Trap".

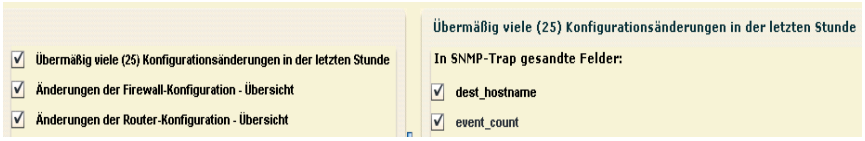
      Das konfigurierte SNMP-Trap-Ziel und die in Schritt 1 des Assistenten ausgewählten Abfragen werden angezeigt.

      Hinweis: Standardmäßig überwacht SpectroSERVER den Standard-SNMP-Trap-Port "162". Wenn Sie diesen ändern, muss der Port dem Parameter "snmp_trap_port" in der Datei "SPECTRUM.vnmrc" im "SS"-Verzeichnis entsprechen.

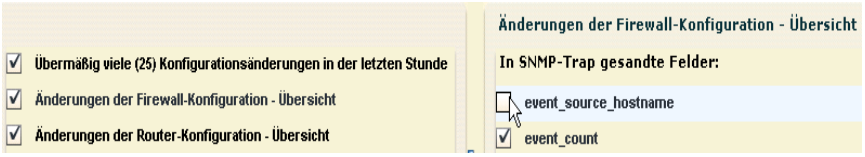
   c. (Optional). Um Traps zusätzlich zum konfigurierten Zielserver an bis zu neun weitere Server zu senden, klicken Sie auf die Schaltfläche "Hinzufügen", und geben Sie die IP-Adresse und den Port dieser Server ein.

   d. Wenn Sie alle Felder einer Abfrage in die Traps aufnehmen möchten, wählen Sie einfach die Abfrage.

      Standardmäßig werden alle Felder einer ausgewählten Abfrage verwendet. Der Name der ausgewählten Abfrage wird über der Feldliste angezeigt.



   e. Wenn Sie nur bestimmte Felder einer Abfrage in die Traps aufnehmen möchten, wählen Sie die Abfrage, und deaktivieren Sie die Felder, die nicht gesendet werden sollen.



f. Wählen Sie für Traps, die von Anwendungen empfangen werden, die SNMP-Version, die von dem ausgewählten Trap-Ziel unterstützt wird.

Hinweis: Einige Trap-Ziele akzeptieren Version 3-Traps, die direkt von Geräten gesendet werden, von Anwendungen, die Ereignisse von Geräten erfassen, jedoch nur Version 2. In diesem Beispiel verwenden wird Version 2.

5. Wählen Sie den Server, und legen Sie fest, ob die Abfrage nur Ergebnisse des/der ausgewählten Server(s) zurückgeben soll oder von diesem Server und allen untergeordneten (bei hierarchischen Servern) oder Peer- (bei Netzverbund) föderierten Servern.

6. Klicken Sie auf "Speichern und schließen".

   Der Job wird in der Liste "Aktionsalarmjobs" angezeigt. Sofern Sie das Kontrollkästchen "Aktiviert" im ersten Schritt des Assistenten nicht deaktiviert haben, wird er als aktiviert angezeigt (Wert "wahr" in der Spalte "Aktiviert"). Eine kurzes Beispiel:


Aktionsalarmjobs

	Jobname	Aktiviert	Server	Wiederholung	Startzeit	Endzeit	Zeitzone	Ersteller
☐	Configuration_Changes_Alert	wahr	ca-elm	5 Minuten	Mittwoch, 11. November 2009, 00:56:08		America/New_York	su

Verfolgen des Alarmjobfortschritts

Sie können die Ergebnisse anzeigen, die von den Abfragen zurückgegeben werden, die Sie für den erstellten Alarm ausgewählt haben. Die angezeigten Ergebnisse für das Beispiel "Configuration_Changes_Alert" werden in CA Enterprise Log Manager unter den Überschriften "Host" und "Anzahl" aufgeführt.

1. Klicken Sie auf die Registerkarte "Alarmverwaltung", und wählen Sie die Unterregisterkarte "Aktionsalarme" aus.

2. Klicken Sie auf den Namen des geplanten Alarms.

3. Zeigen Sie die Ergebnisse für diesen Alarm an.

   Im Folgenden sehen Sie Beispielergebnisse:

Alarmname	Kategorie	Datum
Configuration_Changes_Alert	Übermäßig viele (25) Konfigurationsänderungen in der letzten Stunde	Donnerstag, 12. November 2009

Configuration_Changes_Alert

Alert name(Configuration_Changes_Alert) Alert created by(su) Federated job(Yes) Tags (Action Alerts)
Time Zone (America/New_York) Lists Excessive Configuration Changes (more than 25) in last hour.
Rows Returned(1)

Host	Anzahl
ca-elm	2

Anzeigen von SNMP-Traps in CA Spectrum

Sie können die von den CA Enterprise Log Manager-Alarmen gesendeten SNMP-Traps im CA Spectrum-Ereignismodell anzeigen, das Sie für den Empfang dieser Traps erstellt haben. Empfangene Traps werden auf der Registerkarte "Ereignisse" angezeigt. Bei dem Beispiel "Configuration_Changes_Alert" werden die Ergebnisse "ca-elm" und "2" in CA Spectrum mit den Objekt-IDs (OIDs) 1.3.6.1.4.1.791.9845.2.22 und 1.3.6.1.4.1.791.9845.2.2 angezeigt.

So zeigen Sie SNMP-Traps in CA Spectrum an:

1. Melden Sie sich bei CA Spectrum mit Ihren Anmeldedaten für CA Spectrum an.
2. Rufen Sie das Spectrum-Bedienfeld auf, und starten Sie Spectroserver.

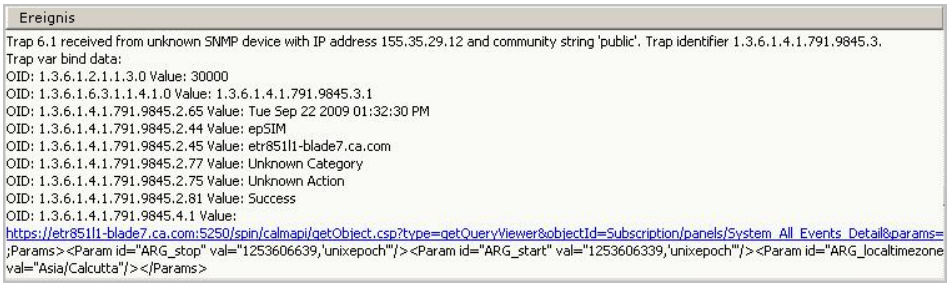
   Spectroserver wird gestartet.
3. Klicken Sie auf "OneClick Administrator", und melden Sie sich an.

   Die Anwendung Spectrum NFM OneClick wird angezeigt.
4. Klicken Sie auf "Start Console" (Konsole starten).

   Die Spectrum OneClick-Konsole wird angezeigt.
5. Erweitern Sie den für CA Enterprise Log Manager erstellten Ordner.
6. Wählen Sie unter "Universe" das Ereignismodell aus, das Sie für den Empfang der von CA Enterprise Log Manager gesendeten Traps erstellt haben.
7. Wählen Sie im rechten Fenster die Registerkarte "Events" (Ereignisse) aus, um die von CA Enterprise Log Manager gesendeten Traps einzublenden.

   Die Werte "ca-elm" und "event_count=2" entsprechen den in CA Enterprise Log Manager angezeigten Daten.

Im Folgenden sehen Sie ein Beispiel dafür, wie eine durch einen CA Enterprise Log Manager-Alarm gesendete SNMP-Trap in CA Spectrum OneClick erscheint. Der Link ist die URL, die Sie in einen Browser einfügen können, um die CA Enterprise Log Manager-Tabelle mit Details im CEG-Format (CEG = Common Event Grammar, ELM-Schemadefinition) anzuzeigen.



Weitere Informationen

Beispiel: Benachrichtigung von CA Spectrum über Konfigurationsänderungen
(siehe Seite 473)

Vorbereiten von CA NSM für den Empfang von SNMP-Traps aus Alarmen

Sie können Alarme in Form von SNMP-Traps von CA Enterprise Log Manager an jedes Ziel in Ihrem Netzwerk senden, das Traps empfangen und interpretieren kann. Jeder Trap-Empfänger hat eigene Anforderungen.

Vorbereiten von CA NSM für den Empfang von Traps aus Alarmen durch:

- Sicherstellen, dass das Ziel-CA NSM-System den Systemanforderungen für das Empfangen von SNMP-Trap-Daten aus CA Enterprise Log Manager entspricht.
- Konfigurieren von CA NSM für den Empfang von SNMP-Traps, darunter das Aktivieren der SNMP v3-Unterstützung, das Ändern von Port-Zuordnungen in verschiedenen Dateien und das Starten der erforderlichen Dienste.

Vorbereiten von CA NSM für das Interpretieren von aus Aktionsalarmen erhaltenen Traps durch:

- Erstellen einer benutzerdefinierten MIB für jeden Alarm, den Sie als SNMP-Trap an CA NSM zu senden planen.
- Importieren und Kompilieren der CA-ELM.MIB und aller benutzerdefinierten MIBs.

CA NSM-Systemvoraussetzungen

Sie können SNMP-Traps an CA NSM senden, sofern Ihr System die folgenden Anforderungen an die CA Enterprise Log Manager-Schnittstelle erfüllt:

- Sie verwenden die CA NSM-Version CA NSM r12.2 (GA-Build).
- CA NSM ist unter Windows Server 2003 EE SP1 installiert.
- Sie haben den Patch "T5MK056.caz" angewendet, durch den die Datei "aws_snmpex.dll" aktualisiert und CA NSM für den Empfang von SNMP-Traps der Version 3 von CA Enterprise Log Manager aktiviert wird.

So wenden Sie den Patch an:

1. Laden Sie den Patch von der CA-Support-Website herunter.
2. Melden Sie sich bei dem CA NSM-Server an.
3. Beenden Sie den SNMP-Trap-Dienst:
   a. Wählen Sie im Startmenü unter "Programme" die Option "Verwaltung" und anschließend die Option "Services" aus.

      Die Liste "Dienste" wird angezeigt.

   b. Wählen Sie den SNMP-Trap-Dienst aus, klicken Sie mit der rechten Maustaste auf diesen Dienst, und wählen Sie im Kontextmenü die Option "Beenden".
4. Beenden Sie alle CA NSM-Dienste:
   a. Öffnen Sie die Eingabeaufforderung.
   b. Geben Sie folgenden Befehl ein:

      ```
      Unicntrl stop all
      ```
5. Kopieren Sie die heruntergeladene Patchdatei "T5MK056.caz" in das Verzeichnis "C:\temp".
6. Entpacken Sie die Patchdatei mit "cazipxp".

   ```
   Cazipxp.exe –u T5MK056.caz
   ```

7. Sichern Sie die vorhandene Datei "aws_snmpex.dll", bevor Sie sie ersetzen.
   a. Navigieren Sie zu dem Verzeichnis "C:\Programme\CA\SC\CCS\AT\SERVICES\BIN".
   b. Klicken Sie mit der rechten Maustaste auf "aws_snmpex.dll", und wählen Sie "Kopieren" aus.

      Dem Ordner wird eine Kopie der Datei "aws_snmpex.dll" hinzugefügt.
8. Kopieren Sie die Datei "aws_snmpex.dll" aus dem Verzeichnis "temp" in das Verzeichnis "bin" (C:\Programme\CA\SC\CCS\AT\SERVICES\BIN).

   CA NSM erfüllt nun die Systemvoraussetzungen. Sie können CA NSM jetzt so konfigurieren, dass SNMP-Traps von CA Enterprise Log Manager empfangen werden.

Vorbereiten von CA NSM für den Empfang von SNMP-Traps

Bevor Sie Alarme, als SNMP-Traps an CA NSM senden können, müssen Sie CA NSM für den Empfang von Traps konfigurieren. Sie können sowohl SNMPv2- als auch SNMPv3-Traps an CA NSM senden.

So konfigurieren Sie CA NSM für den Empfang von SNMP-Traps aus CA Enterprise Log Manager-Alarmen

1. Melden Sie sich bei CA NSM an.
2. Gehen Sie folgendermaßen vor, um die Unterstützung von SNMP version3 zu aktivieren:
   a. Öffnen Sie die Eingabeaufforderung. Klicken Sie im Startmenü auf "Ausführen", geben Sie "cmd" ein, und klicken Sie auf "OK".
   b. Geben Sie Folgendes ein:

      ```
      caugui settings
      ```

      Das Fenster "EM Settings" wird angezeigt.
   c. Klicken Sie auf die Registerkarte "Event Management".
   d. Zeigen Sie folgende Beschreibung an: "SNMP - Enable SNMP version 3 support".
   e. Wählen Sie die Zeile aus, und geben Sie "Y" ein, um in der Einstellungsspalte den Eintrag "SNMP Enable SNMP version 3 support" auf "YES" zu setzen.
   f. Klicken Sie auf "Ja", um die Änderung zu bestätigen.
   g. Schließen Sie das Fenster.

3. Gehen Sie folgendermaßen vor, um den Port, den der SNMP-Dienst aktuell verwendet (z. B. 5162), auf Port 162 zu setzen:
   a. Öffnen Sie den Windows-Explorer.
   b. Navigieren Sie zum Ordner ".../System32/drivers/etc", der sich meist unter "C:\WINDOWS" befindet.
   c. Sichern Sie die Dienstedatei. Klicken Sie mit der rechten Maustaste auf die Dienste und wählen Sie "Kopieren".
   d. Öffnen Sie die Dienstedatei in einem Texteditor (z. B. Notepad), und suchen Sie einen Eintrag, der in etwa folgendermaßen aussieht:

      ```
      snmptrap      162/udp    snmp-trap   #SNMP trap
      ```

   e. Bearbeiten Sie die Zeile "snmptrap", indem Sie die Portnummer "162" durch eine andere Nummer, z. B. "5162" ersetzen. Fügen Sie die Zeile "catrapmuxd" hinzu, in der Sie Port 162 zuweisen.

      ```
      snmptrap    5162/udp
      catrapmuxd   162/udp    catrapmuxd  #CA Trap Multiplexer
      ```

   f. Speichern und schließen Sie die Datei.
4. Bearbeiten Sie die CA Trap Multiplexer-Konfigurationsdatei "catrapmux.conf" folgendermaßen:
   a. Navigieren Sie zu dem Verzeichnis "C:\Program Files\CA\SC\CCS\WVEM\CAIUSER".
   b. Öffnen Sie die Datei "CATRAPMUX.CONF" in einem Texteditor, beispielsweise Notepad.
   c. Gehen Sie zum Ende der Datei. Bearbeiten Sie die Datei, indem Sie die folgenden Einträge einfügen:

      ```
      CATRAPMUX_CMD:6161
      AWS_SNMP:6162
      catrapd:6163
      snmptrap:5162
      ```

      Hinweis: Die ersten drei Einträge stehen für Standardeinstellungen.
   d. Speichern und schließen Sie die Datei.

5. Fügen Sie in der Konfigurationsdatei "snmpv3.dat" eine Zeile hinzu, um die SNMP v3-Sicherheitsparameter zu konfigurieren.
   a. Navigieren Sie zu dem Verzeichnis "C:\Program Files\CA\SC\CCS\CommonResourcePackages\Misc".
   b. Öffnen Sie die Datei "snmpv3.dat" in einem Texteditor, und fügen Sie am Ende der Datei die folgende Zeile hinzu.

      ```
      *.*.*.* *:*                    test1234:AuthPriv:MD5:test1234:DES:test1234
      ```

      Hinweis: Dies sind dieselben Parameter, die Sie im Dialogfeld "V3 Sicherheitsparameter" des Alarmassistenten eingeben müssen, damit der SNMP-Trap von CA NSM empfangen werden kann. Hier werden der Benutzername und das Kennwort konfiguriert. Das Authentifizierungsprotokoll lautet "MD5" und das Verschlüsselungsprotokoll "DES".
   c. Speichern und schließen Sie die Datei.
6. Installieren sie den CA Trap Multiplexer-Dienst:
   a. Öffnen Sie die Eingabeaufforderung.
   b. Führen Sie den folgenden Befehl aus:

      ```
      catrapmuxd uniconfig
      ```

      CA Trap Multiplexer wird mit den Status "started" in die Diensteliste aufgenommen.
7. Überprüfen Sie, ob CA Trap Multiplexer ausgeführt wird, und starten Sie den SNMP-Trap-Dienst.
   a. Wählen Sie im Startmenü unter "Programme" die Option "Verwaltung" und anschließend die Option "Services" aus.

      Die Liste "Dienste" wird angezeigt.
   b. Überprüfen Sie den Status von CA Trap Multiplexer. Stellen Sie sicher, dass der Status "started" lautet.
   c. Wählen Sie den SNMP-Trap-Dienst aus, klicken Sie mit der rechten Maustaste darauf, und wählen Sie im Kontextmenü die Option "Starten".

8. Starten Sie alle Dienste mit dem Starttyp "Automatisch".
   a. Öffnen Sie die Eingabeaufforderung.
   b. Führen Sie den folgenden Befehl aus:

      ```
      Unicntrl start all
      ```

   CA NSM ist nun für den Empfang von SNMP v3-Traps basierend auf geplanten Alarmen von CA Enterprise Log Manager konfiguriert.

Beispiel: Warnungen für CA NSM zu Konfigurationsänderungen

Das nachfolgende Beispiel zeigt Ihnen den Prozess der Warnung von CA NSM vor Konfigurationsänderungen. Der Vorgang umfasst folgende Schritte:

- SNMP-Traps an CA NSM senden
- Sicherstellen, dass SNMP-Traps erfolgreich gesendet wurden
- Zugreifen auf die EM-Konsole von CA NSM
- Anzeigen der von CA NSM erhaltenen SNMP-Traps

SNMP-Traps der Version 3 an CA NSM senden

Wenn Sie dabei sind, zu planen, welche Alarme an CA NSM gesendet werden sollen, ermitteln Sie Abfrageergebnisse, die für das Network Operations Center von Interesse wären. Berücksichtigen Sie zum Beispiel Abfragen, die Konfigurationsänderungen erkennen. Das folgende Beispiel veranschaulicht, wie ein geplanter Alarm auf der Basis einer Abfrage "Konfigurationsänderung - Details" zu senden ist. Dieser Alarm gibt CA NSM als das SNMP-Trap-Ziel an.

So senden Sie SNMP-Traps der Version 3 an CA NSM

1. Öffnen Sie den Assistenten für die Alarmplanung.
   a. Melden Sie sich mit den Anmeldedaten eines Analysten oder Administrators bei CA Enterprise Log Manager an.
   b. Klicken Sie auf die Registerkarte "Alarmverwaltung" und auf die Unterregisterkarte "Alarmplanung".
   c. Klicken Sie auf die Schaltfläche "Aktionsalarm planen".

2. Vervollständigen Sie den Schritt "Alarmauswahl".
   a. Geben Sie einen Jobnamen ein. Beispiel: Konfigurationsänderungen für CA NSM
   b. Stellen Sie sicher, dass unter "Auswahltyp" die Auswahl "Abfragen" aktiviert ist. Für Alarme, die auf Kennungen basieren, können keine SNMP-Trap-Ziele ausgewählt werden.
   c. Wählen Sie die ermittelten Abfragen aus. Wählen Sie beispielsweise "Konfigurationsänderung - Details" aus.
3. (Optional) Führen Sie die Schritte "Alarmfilter", "Ergebnisbedingungen" und "Jobs planen" wie in der Online-Hilfe für diesen Assistenten beschrieben durch.
4. Klicken Sie auf den Schritt "Ziel" und dann auf die Registerkarte "SNMP-Trap".
5. Überprüfen Sie die Einträge für den Zielserver und Port. Geben Sie ggf. die richtige IP-Adresse für den Zielserver und Port ein. Falls Sie weitere Zielserver hinzufügen möchten, klicken Sie auf "Hinzufügen" und geben das zusätzliche Ziel ein.
6. Geben Sie die SNMP-Versionsinformationen an. Standardmäßig ist die SNMP-Version 2 ausgewählt.
   a. Klicken Sie auf "Version 3". CA NSM wird so konfiguriert, dass es SNMP-Traps der Version 3 akzeptiert.
   b. Klicken Sie auf "V3-Sicherheit".

      Das Dialogfeld "Sicherheitsparameter für SNMP-Version 3" wird angezeigt.

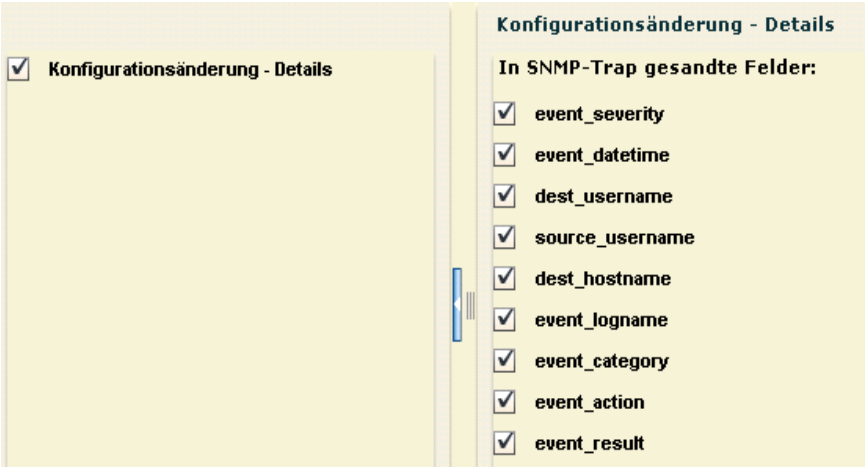
      Wichtig: Die Einträge in diesem Dialogfeld müssen den Einstellungen in der Datei "snmpv3.dat" entsprechen, die Sie konfiguriert haben, damit CA NSM SNMP-Traps von CA Enterprise Log Manager-Alarmen empfangen kann. Folgende Einstellung wird empfohlen:

      ```
      *.*.*.* *:*    <benutzername>:AuthPriv:MD5:<kennwort>:DES:<kennwort>
      ```
   c. Wählen Sie die Option "Authentifizierung" aus. Geben Sie unter "Benutzername" den konfigurierten Benutzernamen und unter "Kennwort" das konfigurierte Kennwort ein, und wählen Sie als Protokoll "MD5" aus.
   d. Aktivieren Sie die Option "Verschlüsselung". Geben Sie unter "Kennwort" das konfigurierte Kennwort ein, und wählen Sie als Protokoll "DES" aus.
   e. Klicken Sie auf "OK".

7. Wählen Sie die Abfrage aus, die als SNMP-Trap gesendet werden soll.

   Wenn Sie in diesem Beispiel die Option "Konfigurationsänderung - Details" auswählen, werden die ausgewählten Felder für diese Abfrage angezeigt. Sie können ggf. Felder deaktivieren, die nicht als Trap einbezogen werden sollen.

   Wichtig! Wenn Sie eine benutzerdefinierte MIB für diesen Alarm erstellen, vergewissern Sie sich, dass Sie eine Trap mit den Feldern definieren, die Sie hier auswählen und dabei die angezeigte Reihenfolge beachten.



8. Wählen Sie die Anzahl für den letzten Knoten, x, der zugeordneten elmTrap-OID aus, wobei alle elmTrap-OIDs als 1.3.6.1.4.1.791.9845.3.x. definiert sind.

   Die Anfangsknoten der benutzerdefinierten Trap-ID werden in CA-ELM.MIB vordefiniert. Die letzte Knotennummer entspricht eindeutig einer Trap, die in einer benutzerdefinierten MIB festgelegt ist, wobei die Trap eine Reihe von eindeutigen Feldern wiedergibt. Eine benutzerdefinierte MIB-Datei gibt die Traps an, die von den von Ihnen festgelegten CA Enterprise Log Manager-Alarmen gesendet wurden. In der von der benutzerdefinierten Trap-ID referenzierten benutzerdefinierten Trap werden die Felder in der gleichen Reihenfolge aufgelistet wie die von dem Alarm gesendeten Felder. Wenn die OID für die Trap in der benutzerdefinierten MIB 1.3.6.1.4.1.791.9845.3.63 lautet, wählen Sie aus der Nummernauswahl für die benutzerdefinierte Trap-ID die 63 aus. Wenn Sie jedoch den Alarm zuerst definieren, fügen Sie in Ihrer benutzerdefinierten MIB eine Trap für 1.3.6.1.4.1.791.9845.3.63 hinzu, die die von Ihnen ausgewählten Abfragefelder definiert.

9. (Optional) Wählen Sie die Option "Server" aus.

10. Klicken Sie auf "Speichern und schließen".

    Der Job wird mit dem konfigurierten Jobnamen in der Liste "Aktionsalarmjobs" angezeigt.

Weitere Informationen:

Zugreifen auf die EM-Konsole in CA NSM (siehe Seite 487)

Verfolgen des Alarmjobfortschritts

Wenn Sie einen Alarm planen, empfiehlt es sich, den Fortschritt des Alarmjobs bei der ersten Ausführung nachzuverfolgen. Beim Nachverfolgen des Fortschritts können Sie überprüfen, ob der Job erfolgreich ausgeführt wird und die gemeldeten Ergebnisse der Form entsprechen, in der Sie sie versenden wollten.

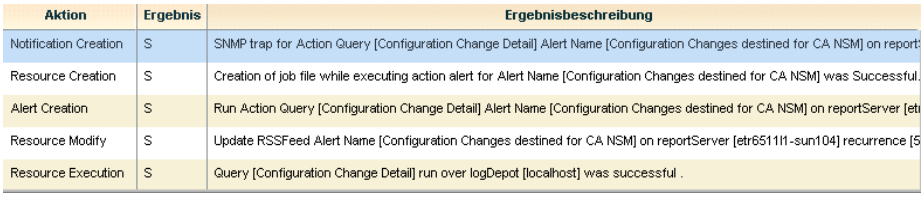
So überwachen Sie den Fortschritt von Alarmjobs und zeigen eine Vorschau der Ergebnisse an:

1. Zeigen Sie den von Ihnen erstellten Alarmjob in der Liste "Aktionsalarmjobs" an. Als Beispiel folgt ein Auszug aus dieser Liste:

Aktionsalarmjobs

	Jobname	Aktiviert	Server	Wiederholung	Startzeit
☐	Configuration Changes destined for CA NSM	wahr	ca-elm	5 Minuten	Dienstag, 01. Dezember 2009, 07:12:57

2. (Optional) Falls Sie den Verlauf des Alarmjobs verfolgen möchten, zeigen Sie "Selbstüberwachende Ereignisse des Systems - Details" an. Doppelklicken Sie auf eine beliebige Zeile, um die Ereignisanzeige einzublenden. Blättern Sie zu "result_string", um die gesamte Meldung anzuzeigen, die in der Spalte "Ergebnisbeschreibung" angezeigt wird.



Aktion	Ergebnis	Ergebnisbeschreibung
Notification Creation	S	SNMP trap for Action Query [Configuration Change Detail] Alert Name [Configuration Changes destined for CA NSM] on report
Resource Creation	S	Creation of job file while executing action alert for Alert Name [Configuration Changes destined for CA NSM] was Successful.
Alert Creation	S	Run Action Query [Configuration Change Detail] Alert Name [Configuration Changes destined for CA NSM] on reportServer [et
Resource Modify	S	Update RSSFeed Alert Name [Configuration Changes destined for CA NSM] on reportServer [etr6511l1-sun104] recurrence [5
Resource Execution	S	Query [Configuration Change Detail] run over logDepot [localhost] was successful .

3. Zeigen Sie die von den für den erstellten Alarm ausgewählten Abfragen zurückgegebenen Ergebnisse als Vorschau an.

   a. Klicken Sie auf die Registerkarte "Alarmverwaltung", und wählen Sie die Unterregisterkarte "Aktionsalarme" aus.

   b. Klicken Sie auf den Namen des geplanten Alarms.

   c. Zeigen Sie die Ergebnisse für diesen Alarm an.

   Hinweis: In der Regel handelt es sich bei den hier angezeigten Daten um die Daten, die beim Navigieren zu der an den Zielserver gesendeten URL angezeigt werden. Falls Unterschiede zwischen den Daten bestehen und Sie möchten, dass sie identisch sind, bearbeiten Sie den Aktionsalarm, um die dynamische Endzeit für "Ergebnisbedingungen" zurückzusetzen. Stellen Sie sie beispielsweise auf 'jetzt', '-10 Minuten' ein.

Zugreifen auf die EM-Konsole in CA NSM

Sie können die von CA Enterprise Log Manager aus CA NSM gesendeten SNMP-Traps anzeigen. SNMP-Traps werden als Meldungen in der EM-Konsole angezeigt.

So greifen Sie auf die EM-Konsole in CA NSM zu:

1. Melden Sie sich bei dem Server an, auf dem das SNMP-Trap-Ziel "CA NSM" installiert ist.
2. Wählen Sie im Startmenü "Programme" und dann "CA", "Unicenter", "NSM", "Enterprise Management" und "EM Classic".

   Das Fenster "EM for Windows" wird geöffnet.
3. Doppelklicken Sie auf "Windows".

   Das Fenster <hostname> (Windows) wird geöffnet.
4. Doppelklicken Sie auf "Ereignis".

   Das Fenster Ereignis <hostname> (Windows) wird geöffnet.
5. Doppelklicken Sie auf "Konsolenprotokolle".

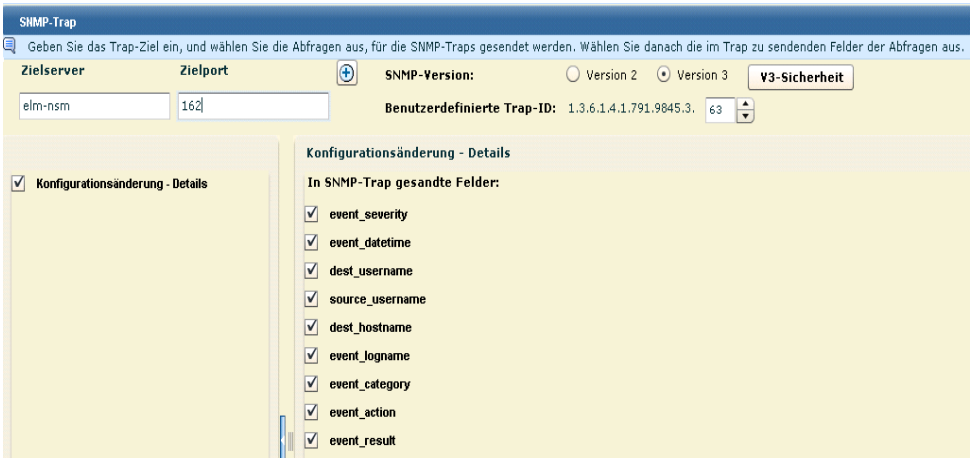
   Daraufhin wird die EM-Konsole (<Hostname>) angezeigt.

Weitere Informationen:

Anzeigen von SNMP-Traps in CA NSM (siehe Seite 488)

Anzeigen von SNMP-Traps in CA NSM

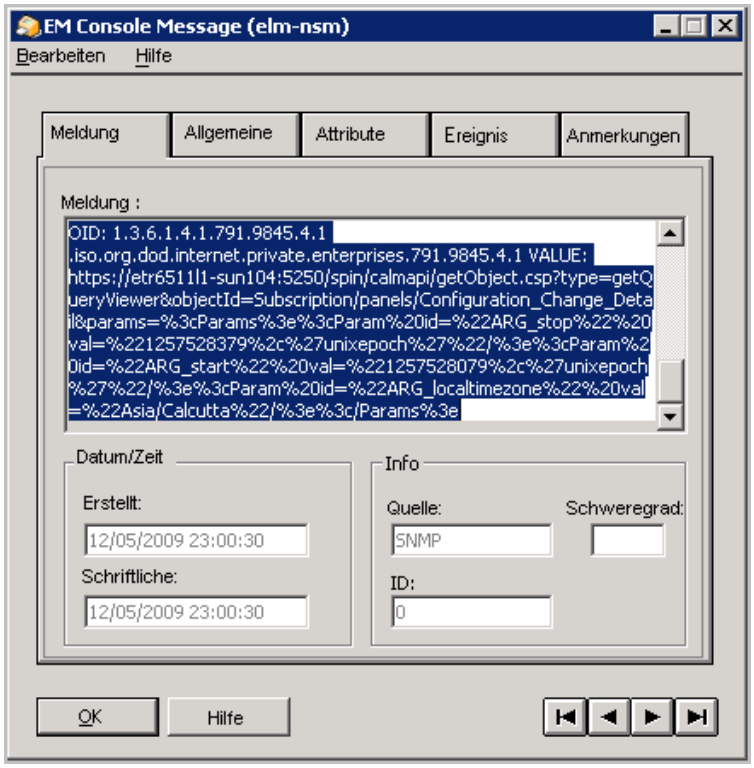
Sehen Sie sich folgendes Beispiel an, bei dem ein Alarm geplant wird, durch den die Abfrage "Konfigurationsänderung - Details" ausgeführt wird. In diesem Beispiel ist "Benutzerdefinierte Trap-ID" auf 1.3.6.1.4.1.791.9845.3.63 eingestellt. Es werden neun Felder als SNMP-Trap gesendet.



So zeigen Sie den SNMP-Trap an, der basierend auf der Abfrage "Konfigurationsänderung - Details" von einem Alarm gesendet wird:

1. Wenn ein selbstüberwachendes Ereignis angibt, dass ein SNMP-Trap erfolgreich an CA NSM gesendet wurde, greifen Sie auf die EM-Konsole in CA NSM zu.
2. Warten Sie, bis eine Protokollmeldung angezeigt wird, durch die der Empfang eines SNMP-Traps angegeben wird. Die Meldung für diesen Trap enthält die benutzerdefinierte Trap-ID 1.3.6.1.4.1.791.9845.3.63.

3. Doppelklicken Sie auf diese Meldung, um sie in einem Format anzuzeigen, in dem Sie sie kopieren können.



4. Kopieren Sie die Meldung, und fügen Sie sie in eine temporäre Textdatei ein.

   Die Ergebnisse sollten etwa wie folgt aussehen:

   ```
   %CATD_I_060, SNMPTRAP: -u auth user 791 155.35.7.63 etr6511l1-sun104.ca.com 6
   63 0:05:00 12
   ```

   Gibt an, dass die folgenden Daten als SNMP-Trap empfangen werden.

   ```
   OID: 1.3.6.1.2.1.1.3.0 system.sysUpTime.0 VALUE: (30000) 0:05:00.00
   ```

   Gibt die Objekt-ID für die Betriebszeit in Hundertstelsekunden an. Dies ist eine über SNMP bekannte OID.

```
OID: 1.3.6.1.6.3.1.1.4.1.0 .iso.org.dod.internet.snmpV2.snmpModules.1.1.4.1.0
VALUE: 1.3.6.1.4.1.791.9845.3.63
```

Gibt die Objekt-ID für "snmpTrapOID" an. Beim Wert handelt es sich um die benutzerdefinierte Trap-ID, die Sie bei der Konfiguration des Alarms angegeben haben.

```
OID: 1.3.6.1.4.1.791.9845.2.80
.iso.org.dod.internet.private.enterprises.791.9845.2.80 VALUE: 2
```

Gibt die OID für "event_severity" und den Schweregradwert 2 an, der für "Information" steht.

```
OID: 1.3.6.1.4.1.791.9845.2.65
.iso.org.dod.internet.private.enterprises.791.9845.2.65 VALUE: Fri Nov 06
2009 22:53:53
```

Gibt die OID für "event_datetime" mit dem Wert für den Tag, das Datum und die Uhrzeit an, als das Ereignis mit den entsprechenden Werten eingetreten ist.

```
OID: 1.3.6.1.4.1.791.9845.2.17
.iso.org.dod.internet.private.enterprises.791.9845.2.17 VALUE:
```

Gibt die Objekt-ID für "dest_username" ohne Wert an.

```
OID: 1.3.6.1.4.1.791.9845.2.1
.iso.org.dod.internet.private.enterprises.791.9845.2.1 VALUE:
```

Gibt die Objekt-ID für "source_username" ohne Wert an.

```
OID: 1.3.6.1.4.1.791.9845.2.22
.iso.org.dod.internet.private.enterprises.791.9845.2.22 VALUE: etr851l2-elm5
```

Gibt die Objekt-ID für "dest_hostname" mit dem Hostnamen des Servers an, auf dem die Abfrageergebnisse beim Aufrufen der URL angezeigt werden.

```
OID: 1.3.6.1.4.1.791.9845.2.53
.iso.org.dod.internet.private.enterprises.791.9845.2.53 VALUE: EiamSdk
```

Gibt die Objekt-ID für "event_logname" an. Hierbei handelt es sich um "EiamSdk", den Namen der Protokolldatei, die diese Details enthält.

```
OID: 1.3.6.1.4.1.791.9845.2.77
.iso.org.dod.internet.private.enterprises.791.9845.2.77 VALUE: Configuration
Management
```

Gibt die Objekt-ID für "event_category" und den Wert für die Kategorie an, die der Abfrage "Konfigurationsänderung - Details" zugewiesen ist.

```
OID: 1.3.6.1.4.1.791.9845.2.75
.iso.org.dod.internet.private.enterprises.791.9845.2.75 VALUE: Configuration
Change
```

Gibt die Objekt-ID für "event_action" und den Wert für die Aktion an, die der Abfrage "Konfigurationsänderung - Details" zugewiesen ist.

```
OID: 1.3.6.1.4.1.791.9845.2.81
.iso.org.dod.internet.private.enterprises.791.9845.2.81 VALUE: S
```

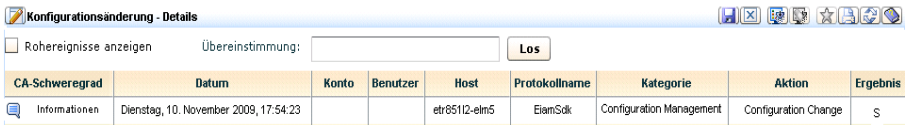
Gibt die Objekt-ID für "event_result" mit dem Wert "S" für "Erfolgreich" (Success) an.

```
OID: 1.3.6.1.4.1.791.9845.4.1
.iso.org.dod.internet.private.enterprises.791.9845.4.1 VALUE:
https://etr6511l1-
sun104:5250/spin/calmapi/getObject.csp?type=getQueryViewer&objectId=Subscript
ion/panels/Configuration_Change_Detail&params=%3cParams%3e%3cParam%20id=%22AR
G_stop%22%20val=%221257528379%2c%27unixepoch%27%22/%3e%3cParam%20id=%22ARG_st
art%22%20val=%221257528079%2c%27unixepoch%27%22/%3e%3cParam%20id=%22ARG_local
timezone%22%20val=%22Asia/Calcutta%22/%3e%3c/Params%3e
```

Gibt die Objekt-ID für "calmAPIURL" unter "elmDynamicVariables" an. Beim Wert handelt es sich um die URL, über die die CA Enterprise Log Manager-API aufgerufen wird. Nach der Anmeldung können Sie die Abfrageergebnisse in der Diagrammansicht oder in einer grafischen Ansicht anzeigen.

5. Kopieren Sie die URL am Ende der Meldung, fügen Sie sie in einen Browser ein, und rufen Sie die URL auf.
6. Melden Sie sich bei der CA Enterprise Log Manager-API an.

   Die Diagrammansicht von "Konfigurationsänderung - Details" wird angezeigt. Dies wird mit folgendem Beispiel verdeutlicht:



Erstellen von Aktionsalarmen

Die Erstellung eines Aktionsalarms mit dem Assistenten für die Planung eines Aktionsalarms umfasst folgende Hauptschritte:

1. Öffnen des Assistenten für die Planung eines Aktionsalarms.
2. Auswählen der Abfrage oder der Kennungen, auf denen der Alarm beruht. Sie können entweder die Ereignisdatenbank, die Incident-Datenbank oder beide in einem einzelnen Job abfragen.
3. (Optional) Festlegen erweiterter Filter, um die Alarmabfrage noch genauer zu definieren.
4. (Optional) Einstellen von Datumsbereich und Ergebnisbedingungen.
5. (Optional) Bestimmen, wie oft der Alarmjob ausgeführt wird und wann er aktiv ist.
6. (Optional) Konfigurieren automatischer Alarm-E-Mails und deren Empfänger.
7. (Optional) Auswählen, ob die Abfrage nur für diesen Server oder für den Server und alle seine untergeordneten Server ausgeführt werden soll.

Weitere Informationen:

Öffnen des Assistenten zum Planen von Aktionsalarmen (siehe Seite 493)
Erstellen erweiterter Ereignisfilter (siehe Seite 621)
Festlegen von Ergebnisbedingungen (siehe Seite 530)
Festlegen von Benachrichtigungszielen (siehe Seite 496)
Definieren eines Ziels für die Abfrage von Alarmjobs (siehe Seite 502)

Öffnen des Assistenten zum Planen von Aktionsalarmen

Zum Erstellen eines Aktionsalarmjobs verwenden Sie den Assistenten zum Planen von Aktionsalarmen.

So öffnen Sie den Assistenten zum Planen von Aktionsalarmen:

1. Klicken Sie auf die Registerkarte "Alarmverwaltung".

   Die Liste "Alarmserver" wird angezeigt.

2. Wählen Sie den Server aus, auf dem Sie einen Alarmjob planen möchten.

   Im Fensterbereich "Serverdetails" wird der ausgewählte Server angezeigt. Standardmäßig ist die Registerkarte "Generierte Alarme" geöffnet.

3. Klicken Sie auf die Registerkarte "Alarmplanung" und dann auf die Schaltfläche "Alarm planen".

   Der Assistent "Aktionsalarme planen" wird eingeblendet.

   Beachten Sie bei Verwendung des Assistenten Folgendes:

   - Klicken Sie auf "Speichern und schließen", um den Aktionsalarm zu speichern und den Assistenten zu schließen.
   - Klicken Sie auf "Zurücksetzen", um die Ansicht im Assistenten auf die zuletzt gespeicherten Einstellungen zurückzusetzen.

Weitere Informationen

Festlegen des Ziels für E-Mail-Benachrichtigungen (siehe Seite 497)
Definieren eines Ziels für die Abfrage von Alarmjobs (siehe Seite 502)

Auswählen einer Alarmabfrage

Wählen Sie Kennungen oder Abfragen als Grundlage für einen neuen Aktionsalarmjob aus. Die Abfrage sowie hinzugefügte Filter definieren den Umstand, unter dem ein Alarm generiert wird. Wenn Sie beispielsweise einen Alarm erstellen möchten, um den Datenverkehr eines Hosts oder Ports zu überwachen, verwenden Sie die Abfrage "Alle Ereignisse" und fügen Sie Filter zur Angabe des zu überwachenden Quell-Hosts sowie einen Ereignisschwellenwert hinzu.

Hinweis: Die Abfragekategorie "Aktionsalarme" enthält Abfragen für verschiedene gängige Alarmanforderungen.

So wählen Sie eine Alarmabfrage aus:

1. Öffnen Sie den Assistenten zum Planen von Aktionsalarmen.
2. Geben Sie einen Jobnamen ein.
3. Wählen Sie im Drop-down-Menü "Zeitzone" die Zeitzone aus, in der Sie den Bericht planen möchten.
4. Um Berichte nach Kennung oder einzeln auszuwählen, aktivieren Sie das Optionsfeld "Abfragen" oder "Kennungen".

   Hinweis: Wenn Sie Alarme nach Kennungen planen, können Sie Alarme hinzufügen, ohne den Job selbst zu ändern. Bei Auswahl der Kennung "Identitätsverwaltung" werden sämtliche Alarme mit dieser Kennung dem Job zur geplanten Ausführungszeit hinzugefügt. Auf diese Weise können Sie dem Job einen neuen Alarm hinzufügen, indem Sie einer Abfrage die Kennung "Identitätsverwaltung" zuweisen. Dies gilt auch für benutzerdefinierte Kennungen.

   (Optional) Deaktivieren Sie das Kontrollkästchen "Aktivieren", wenn Sie den Aktionsalarm nicht gleich nach Fertigstellung, sondern erst später aktivieren möchten. Standardmäßig ist das Kontrollkästchen markiert.

   Hinweis: Die Möglichkeit, einen deaktivierten Alarmjob zu erstellen, ist für wiederkehrende Alarme vorgesehen. Wenn Sie das Kontrollkästchen "Aktiviert" für einen Job deaktivieren und diesen Job als einmal auszuführenden Job ("Jetzt" oder "Einmal") erstellen, wird er aus der Liste "Geplante Alarme" entfernt.
5. (Optional) Die Anzeige von Kennungen und Berichten kann durch Auswahl einer oder mehrerer Kennungen eingegrenzt werden. Mit dieser Funktion wird das Verhalten der Berichtsliste angepasst.

6. Wählen Sie die gewünschten Kennungen oder einzelnen Abfragen aus, und fügen Sie sie mithilfe der Wechselsteuerung zum Bereich "Ausgewählte Abfragen" hinzu. Sie können sowohl Ereignisabfragen als auch Incident-Abfragen in einem einzigen Alarmjob auswählen.
7. Fahren Sie mit dem Planungsschritt fort, den Sie als nächstes ausführen möchten, oder klicken Sie auf "Speichern und schließen".

   Wenn Sie auf "Speichern und Schließen" klicken, wird der Alarmjob geplant. Andernfalls wird der ausgewählte Schritt angezeigt.

Weitere Informationen:

Erstellen erweiterter Ereignisfilter (siehe Seite 621)
Festlegen von Ergebnisbedingungen (siehe Seite 530)

Festlegen von Parametern für die Alarmjobplanung

Sie können bestimmen, wann Ihre Alarme angewendet werden, indem Sie eine Start- und Endzeit festlegen. Sie können auch bestimmen, wie präzise die Alarmanzeige ist, indem Sie festlegen, wie häufig die Abfrage wiederholt wird.

So legen Sie Parameter für die Alarmjobplanung fest:

1. Öffnen Sie den Assistenten zum Planen von Aktionsalarmen, geben Sie die erforderlichen Informationen ein, und fahren Sie mit dem Schritt "Jobs planen" fort.
2. Legen Sie das gewünschte Wiederholungsintervall fest. Je niedriger das Intervall, umso detaillierter wird die Anzeige, aber umso mehr Netzwerkverkehr entsteht.

   Überprüfen Sie, ob CA Enterprise Log Manager mit einem NTP-Server synchronisiert ist, bevor Sie ein niedriges Intervall festlegen.
3. Legen Sie die für den Alarmjob gewünschte Start- und Endzeit fest.
4. Fahren Sie mit dem Planungsschritt fort, den Sie als nächstes ausführen möchten, oder klicken Sie auf "Speichern und schließen".

   Wenn Sie auf "Speichern und Schließen" klicken, wird der Alarmjob geplant. Andernfalls wird der ausgewählte Schritt angezeigt.

Festlegen von Benachrichtigungszielen

Sie können eins oder mehrere der folgenden Ziele für die Alarmbenachrichtigung festlegen:

- E-Mail

  Sie können automatische E-Mail-Benachrichtigungen für einen Alarm festlegen und so sicherstellen, dass die zuständigen Mitarbeiter auf Alarme aufmerksam werden, die sich auf ihr Aufgabengebiet oder ihren Verantwortungsbereich beziehen. Konfigurieren Sie einen E-Mail-Server für Ihre CA Enterprise Log Manager-Umgebung, bevor Sie Alarmbenachrichtigungs-E-Mails versenden.

- IT PAM-Prozess

  Sie können den angegebenen CA IT PAM-Prozess ausführen, wenn für den Alarm die Benachrichtigung des Drittanbieterprodukts erforderlich ist. Die Integration mit CA IT PAM muss unter "Berichtsserver" konfiguriert werden, und in IT PAM muss der Prozess definiert sein, bevor Sie den Prozess von Alarmen aus ausführen können.

- SNMP-Trap

  Sie können Ereignisdaten, die von einem Alarm erfasst wurden, an einen oder mehrere NOCs (Network Operations Centers) versenden. Mit SNMP v2- oder SNMP v3-Traps können Sie Management-Server wie beispielsweise CA Spectrum oder CA NSM als Ziel verwenden. Die Ziele werden beim Planen des Alarms festgelegt. Die Integration mit SNMP muss konfiguriert werden, bevor Sie Alarme über SNMP versenden können.

Hinweis: Wenn Sie kein Ziel festlegen, werden die Alarmergebnisse nur an den RSS-Feed veröffentlicht.

Weitere Informationen:

Festlegen des Ziels für E-Mail-Benachrichtigungen (siehe Seite 497)
Einstellen von CA IT PAM-Informationen (siehe Seite 498)
Beispiel: Benachrichtigung von CA Spectrum über Konfigurationsänderungen (siehe Seite 473)
Beispiel: Senden eines Alarms, durch den ein IT PAM-Prozess pro Zeile ausgeführt wird (siehe Seite 437)
Beispiel: Senden eines Alarms, der einen IT PAM-Prozess pro Abfrage ausführt (siehe Seite 442)

Festlegen des Ziels für E-Mail-Benachrichtigungen

Sie können automatische E-Mail-Benachrichtigungen für einen Alarmjob festlegen und so sicherstellen, dass die zuständigen Mitarbeiter auf Alarme aufmerksam werden, die sich auf ihr Aufgabengebiet oder ihren Verantwortungsbereich beziehen. Dieser Schritt ist optional.

Bevor Sie für Alarme E-Mail-Benachrichtigungen festlegen können, muss für die CA Enterprise Log Manager-Umgebung ein E-Mail-Server konfiguriert werden.

So legen Sie Alarmbenachrichtigungen fest:

1. Öffnen Sie den Assistenten zum Planen von Aktionsalarmen, geben Sie die erforderlichen Informationen ein, und fahren Sie mit dem Schritt "Ziel" fort.
2. Aktivieren Sie das Kontrollkästchen "E-Mail-Benachrichtigung aktivieren".
3. Geben Sie mindestens eine Empfänger-E-Mail-Adresse ein. Sie können mehrere, durch Kommas voneinander getrennte Adressen eingeben.
4. (Optional) Geben Sie unter "Von" und unter "Betreff" einen Text sowie einen Nachrichtentext für die E-Mail-Benachrichtigung ein.

   Hinweis: Der Nachrichtentext wird in HTML erstellt, so dass der gesamte Text, den Sie eingeben, in einer Zeile angezeigt wird. Um einen Zeilenumbruch zu erstellen, geben Sie am Ende der Textzeile <BR/> ein.

Weitere Informationen:

Einstellen von CA IT PAM-Informationen (siehe Seite 498)

Einstellen von CA IT PAM-Informationen

Sie können Ihren Alarmjob so einrichten, dass ein CA IT PAM-Prozess ausgeführt wird, wenn der Alarm generiert wird.

Sie können den Prozess einmal für jede Abfrageergebniszeile oder ein einziges Mal, unabhängig von der Anzahl der Zeilen, ausführen. Wenn Sie den Prozess einmal pro Zeile ausführen, geben Sie in den CEG-Feldern eine Zusammenfassung und eine Beschreibung ein, um die Ereignisdaten an CA IT PAM zu übergeben. Wählen Sie die Felder, die für die Erfassung von Daten durch die Abfrage festgelegt wurden. Wenn Sie den Prozess einmal pro Abfrage ausführen, wird automatisch eine URL an CA IT PAM übergeben, über die alle Zeilen mit Ereignisdaten angezeigt werden. In dem Drittanbieterprodukt, das auf den CA IT PAM-Prozess reagiert, wird die URL an den eingegebenen Zusammenfassungstext angehängt. Beispiel: Sie erscheint im Feld "Zusammenfassung" von CA Service Desk, sofern dieses das Drittanbieterprodukt ist.

So führen Sie einen CA IT PAM-Prozess aus, wenn der Alarm generiert wird:

1. Öffnen Sie den Assistenten zum Planen von Aktionsalarmen, geben Sie die erforderlichen Informationen ein, und fahren Sie mit dem Schritt "Ziel" fort.
2. Klicken Sie auf die Registerkarte "IT PAM-Prozess".

   Im linken Fensterbereich wird für jede Abfrage dieses Alarmjobs ein Kontrollkästchen angezeigt.
3. Wählen Sie eine Abfrage, die Sie an den CA IT PAM-Prozess senden möchten, und führen Sie einen der folgenden Schritte durch:
   - Wählen Sie "IT PAM-Prozess zeilenweise ausführen", um den konfigurierten Prozess für jede zurückgegebene Zeile auszuführen.
   - Wählen Sie "IT PAM-Prozess ausführen", um den konfigurierten Prozess einmal auszuführen, unabhängig von der Anzahl der zurückgegebenen Zeilen.
4. Überprüfen Sie die Standardeinträge für die Prozessparameter, und ändern Sie die, falls nötig. Bei nicht definierten Feldern, in denen eine Zusammenfassung oder eine Beschreibung eingegeben werden kann, geben Sie einen passenden Text ein. Wenn Sie "IT PAM-Prozess zeilenweise ausführen" ausgewählt haben, verwenden Sie die CEG-Felder, um Ereignisdaten zu übermitteln. Wählen Sie das CEG-Feld, und klicken Sie neben dem Zielfeld auf "Hinzufügen".
5. Wenn der CA IT PAM-Prozess mit CEG-Feldern als lokalen Parametern im Datensatz definiert wurde, wählen Sie diese CEG-Felder in den Feldwerten "Senden" als Parameterliste.

6. Wählen Sie im linken Fensterbereich eine weitere Abfrage, und wiederholen Sie die Schritte 3 bis 6.

Hinweis: Wenn die Abfragen eines geplanten Alarmjobs Ergebnisse zurückgeben, werden alle Informationen und Parameter, die für den konfigurierten Prozess benötigt werden, an CA IT PAM gesendet.

Weitere Informationen

Festlegen des Ziels für E-Mail-Benachrichtigungen (siehe Seite 497)

Festlegen von SNMP-Trap-Informationen

Sie können SNMP-Traps verwenden, um über einen Alarmjob zu informieren. So können Sie den Alarm an ein oder mehrere Drittanbieter-Verwaltungssysteme senden. Wenn die ausgewählten Abfragen Ergebnisse zurückgeben, wird ein Trap an alle SNMP-Trap-Ziele gesendet, das zurückgegebene Daten aller ausgewählten Abfragen für die ausgewählten Felder enthält. Dieser Schritt ist optional.

So senden Sie SNMP-Trap-Informationen:

1. Öffnen Sie den Assistenten zum Planen von Aktionsalarmen, geben Sie die erforderlichen Informationen ein, und fahren Sie mit dem Schritt "Ziel" fort.
2. Wählen Sie die Registerkarte "SNMP-Trap".

   Die Registerkarte "SNMP-Trap" zeigt den Zielserver und den Ziel-Port sowie eine Liste der Abfragen an, die im Aktionsalarm enthalten sind. Diese Abfragen verfügen über Kontrollkästchen.
3. Überprüfen Sie den Standardzielserver und die Porteinträge. Korrigieren Sie gegebenenfalls die IP-Adresse oder den vollqualifizierten Hostnamen und die Portnummer.
4. (Optional) Klicken Sie auf "Hinzufügen", um weitere Zielserver und -ports anzugeben.
5. (Optional) Um einen Alarm mit SNMP v3 zu senden, wählen Sie "SNMP Version 3". Standardmäßig wird SNMP Version 2 verwendet.
6. Wenn Sie SNMP Version 3 wählen, klicken sie auf die Schaltfläche "V3-Sicherheit", um im Dialogfeld "Sicherheitsparameter" die Authentifizierung oder Verschlüsselung festzulegen.

   Wichtig: Die Einträge in diesem Dialogfeld müssen den Einstellungen in der Datei "snmpv3.dat" entsprechen, die Sie konfiguriert haben, damit CA NSM SNMP-Traps von CA Enterprise Log Manager-Alarmen empfangen kann. Folgende Einstellung wird empfohlen:

   ```
   *.*.*.* *:*   <Benutzername>:AuthPriv:MD5:<Kennwort>:DES:<Kennwort>
   ```

   a. Wählen Sie die Option "Authentifizierung" aus. Geben Sie unter "Benutzername" den konfigurierten Benutzernamen und unter "Kennwort" das konfigurierte Kennwort ein, und wählen Sie als Protokoll "MD5" aus.

   b. Aktivieren Sie die Option "Verschlüsselung". Geben Sie unter "Kennwort" das konfigurierte Kennwort ein, und wählen Sie als Protokoll "DES" aus.

7. Aktivieren Sie das Kontrollkästchen neben der Abfrage, die in den SNMP-Trap aufgenommen werden soll. Wenn beispielsweise drei Abfragen aufgelistet werden, können Sie wählen, ob SNMP eine, zwei oder alle drei Abfragen liefern soll.

   Wenn Sie eine Abfrage wählen, werden die Felder angezeigt, die in jeder Abfrage enthalten sind, wobei die entsprechenden Kontrollkästchen aktiviert sind. Sie können die Kontrollkästchen deaktivieren, um das entsprechende Feld aus dem Alarm zu entfernen.

8. Geben Sie die benutzerdefinierte Trap-ID ein, die mit jeder Abfrage verbunden werden soll. Dies ermöglicht es Ihnen bei Bedarf, unterschiedliche Abfragen in einem einzigen Alarm an verschiedene Trap-IDs zu senden.

9. Fahren Sie mit dem Planungsschritt fort, den Sie als nächstes ausführen möchten, oder klicken Sie auf "Speichern und schließen".

   Wenn Sie auf "Speichern und Schließen" klicken, wird der Alarmjob geplant. Andernfalls wird der ausgewählte Schritt angezeigt.

Weitere Informationen:

Festlegen des Ziels für E-Mail-Benachrichtigungen (siehe Seite 497)
Einstellen von CA IT PAM-Informationen (siehe Seite 498)

Definieren eines Ziels für die Abfrage von Alarmjobs

Sie können festlegen, welche föderierten Ereignisprotokollspeicher vom Alarmjob abgefragt werden.

So wählen Sie Berichtsziele aus:

1. Öffnen Sie den Assistenten zum Planen von Aktionsalarmen, geben Sie die erforderlichen Informationen ein, und fahren Sie mit dem Schritt "Serverauswahl" fort.
2. Wählen Sie verfügbare Server aus, die Sie abfragen möchten, und verschieben Sie diese mit der Wechselsteuerung in den Bereich "Ausgewählte Server".
3. (Optional) Wenn Sie föderierte Abfragen für diesen Alarmjob deaktivieren möchten, wählen Sie im Dropdown-Menü, das angezeigt wird, wenn Sie auf den Eintrag für föderierte Abfragen klicken, die Option "Nein" aus. Berichtsabfragen sind standardmäßig föderiert.
4. Fahren Sie mit dem Planungsschritt fort, den Sie als nächstes ausführen möchten, oder klicken Sie auf "Speichern und schließen".

   Wenn Sie auf "Speichern und Schließen" klicken, wird der Alarmjob geplant. Andernfalls wird der ausgewählte Schritt angezeigt.

Beispiel: Einen Aktionsalarm für "Wenig Speicherplatz verfügbar" erstellen.

"Wenig Speicherplatz verfügbar" ist eine der vordefinierten Abfragen mit der Kennung "Aktionsalarme". Abfragen mit der Kennung "Aktionsalarme" sind speziell darauf ausgelegt, als Alarme verwendet zu werden, werden jedoch erst dann zu Alarmen, wenn Sie sie planen.

Das folgende Beispiel zeigt, wie Sie einen Aktionsalarm mit der vordefinierten Abfrage "Wenig Speicherplatz verfügbar" erstellen können.

1. Klicken Sie auf die Registerkarte "Abfragen und Berichte" und auf die Unterregisterkarte "Abfragen".

   Die Fensterbereiche "Abfragekennung" und "Abfrageliste" werden eingeblendet.

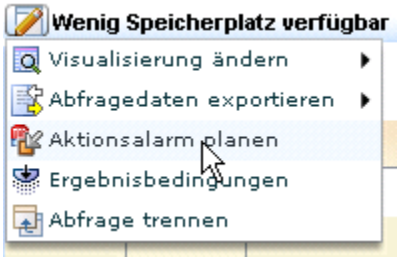
2. Klicken Sie auf die Kennung "Aktionsalarme".

   Die Abfrageliste zeigt die Abfragen mit der Kennung "Aktionsalarme" an.

3. Klicken Sie auf die Abfrage "Wenig Speicherplatz verfügbar" in der Abfrageliste.

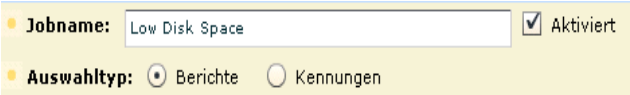
   Die Abfrage "Wenig Speicherplatz verfügbar" wird im Hauptfenster eingeblendet.

4. Klicken Sie auf "Optionen", und wählen Sie "Aktionsalarme planen".



Der Assistent für das Planen von Aktionsalarmen wird geöffnet, und der Schritt "Alarmauswahl" ist vorausgewählt. Unter "Ausgewählte Abfragen" ist "Wenig Speicherplatz verfügbar" vorausgewählt.

5. Geben Sie einen Jobnamen ein, beispielsweise "Wenig Speicherplatz". Löschen Sie vorerst die Markierung im Kontrollkästchen "Aktiviert". So können Sie den Aktionsalarmplan speichern und schließen, bevor er komplett ist, ohne Gefahr zu laufen, dass ein Versuch gemacht wird, ihn auszuführen.



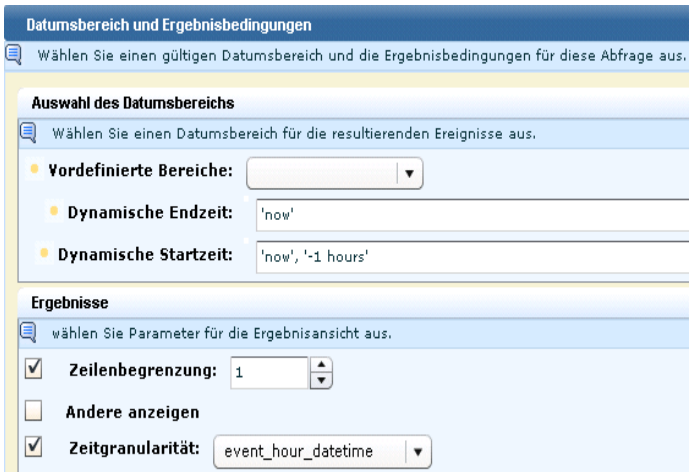
6. Sie können Alarmfilter eingeben oder überspringen. Filter sind additiv, d. h., wenn eine Serie von Filtern evaluiert wird, werden sie durch den Operator UND verbunden.

7. Klicken Sie auf "Ergebnisbedingungen", um die in der Abfragedefinition gesetzten Filter außer Kraft zu setzen.

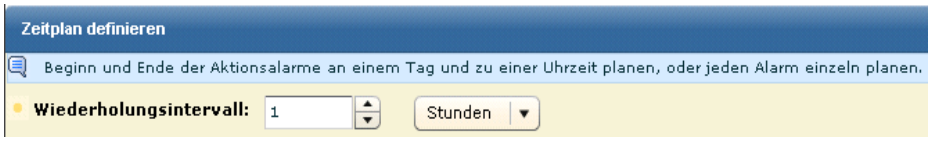
   a. Um festzulegen, dass der Alarm den Speicherplatz für die vergangene Stunde überprüfen soll, geben Sie den Datumsbereich als "jetzt' für die dynamische Endzeit und "jetzt' '-1 Stunde' für die dynamische Startzeit ein.

   b. Um festzulegen, dass Sie nur dann benachrichtigt werden möchten, wenn die Abfrage ein Ergebnis liefert, und dass Sie nur das erste zurückgegebene Ergebnis sehen möchten, wählen Sie "Zeilenbegrenzung", und setzen Sie den Wert auf 1. Da der dynamische Zeitbereich in Stunden angegeben ist, wählen Sie "Ereignis_Stunde_DatumUhrzeit" als Zeitgranularität.

   c. Lassen Sie "Gruppierte Ereignisse" leer, da dies auf diese Abfrage nicht anwendbar ist.



8. Klicken Sie auf "Jobs planen", um den Zeitplan festzulegen. Standard ist, den Job sofort zu starten und kein Enddatum zu definieren. Legen Sie das Wiederholungsintervall fest. Bestimmen Sie beispielsweise, dass die Abfrage jede Stunde einmal durchgeführt wird.



9. Klicken Sie auf den Schritt "Ziel". Wählen Sie "E-Mail-Benachrichtigung aktivieren", und geben Sie Ihre E-Mail-Adresse in das Feld "E-Mail an" ein. Sie können außerdem einen Betreff und einen E-Mail-Text eingeben. Oder adressieren Sie die Meldung an gewünschte Empfänger und geben Sie Ihre E-Mail-Adresse in das Feld "Von" ein. Wenn Sie mehrere E-Mail-Adressen eingeben, trennen Sie diese durch ein Komma (nicht durch einen Strichpunkt).

10. Klicken Sie auf "Serverauswahl". Standardmäßig wird die Abfrage auf dem aktuellen CA Enterprise Log Manager-Server ausgeführt. Wählen Sie "Verbund", um diese Abfrage sowie alle anderen geeigneten Abfragen im Verbund auf diesem Server auszuführen.
11. Klicken Sie auf "Alarmauswahl". Wählen Sie "Aktiviert".
12. Klicken Sie auf "Speichern und schließen".

    Der Aktionsalarmjob wird auf der Unterregisterkarte "Alarmplanung" angezeigt.

13. Klicken Sie auf die Registerkarte "Alarmverwaltung, Aktionsalarme", um das Ergebnis dieses Aktionsalarms zu prüfen.

Sie erhalten, wie angefordert, eine E-Mail-Benachrichtigung. Es folgt ein Beispiel:

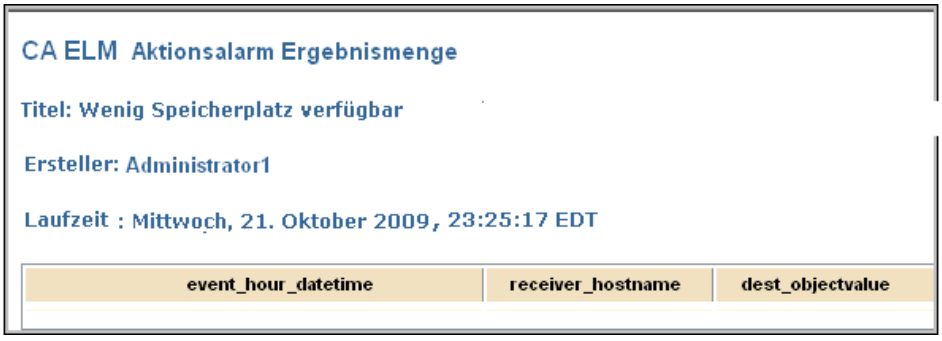
CA Enterprise Log Manager

RSS Link	https://calmrhbuildtest01:5250/spin/calm/getA 8424346294223181834-calmrhbuildtest011220 3207977576 actionquery 1220536215721
Alarmname	Low Disk Space
Abfragename	Wenig Speicherplatz verfügbar
Generiertes Datum	Mittwoch, 21. Oktober 2009 12.19 Uhr EDT
Kennungen	[Action Alerts]
Ersteller	Administrator1
Server	caelm

Kommentare

Disk space has dropped below 20%

Wenn Sie auf den RSS-Link klicken, wird eine Seite ähnlich der folgenden eingeblendet:



Beispiele: Erstellen eines Alarms für ein selbstüberwachendes Ereignis

Die vordefinierte Abfrage für alle selbstüberwachenden Ereignisse ist "Alle Ereignisse des Systems - Details". Sie können diese Abfrage kopieren und als Grundlage für die Definition eines Alarms für ein bestimmtes selbstüberwachendes Ereignis verwenden.

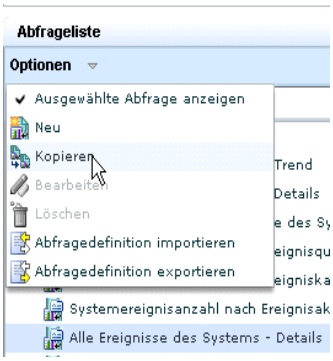
Z. B. wird ein selbstüberwachendes Ereignis erstellt, wenn ein Modul, das einen Neustart erfordert, bei einem automatischen Software-Update heruntergeladen wird. Dieses selbstüberwachende Ereignis wird nur einmal erstellt. Möglicherweise möchten Sie für den Fall, dass dieses selbstüberwachende Ereignis übersehen wird, einen Alarm erstellen, der Sie daran erinnert, das Betriebssystem neu zu starten.

Die folgenden Beispiele können als Anhaltspunkte dienen:

1. Erstellen Sie eine Abfrage auf der Grundlage der Abfrage nach allen selbstüberwachenden Ereignissen folgendermaßen:

   a. Klicken Sie auf die Registerkarte "Abfragen und Berichte" und auf die Unter-Registerkarte "Abfragen".

   b. Wählen Sie in der Abfrageliste "Alle Ereignisse des Systems - Details", erweitern Sie die Dropdown-Liste "Optionen" und wählen Sie "Kopieren".



   Der Assistent für das Erstellen von Abfragen wird angezeigt, zusammen mit dem ausgewählten Details-Schritt.

   c. Ersetzen Sie den Namen der kopierten Abfrage durch einen neuen Namen, z. B. "Alarm Betriebssystem neu starten". Wahlweise können Sie einen Kurznamen und eine neue Beschreibung hinzufügen.

   d. Wählen Sie unter "Verfügbare Kennungen" "Aktionsalarme" aus, und verschieben Sie sie nach "Ausgewählte Kennungen".

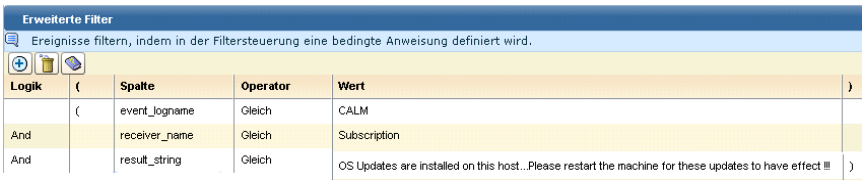
2. Erstellen Sie Abfragefilter wie folgt:

   a. Gehen Sie zum Schritt "Abfragefilter". Klicken Sie auf die Registerkarte "Erweiterte Filter".

   b. Klicken Sie auf "Neuer Ereignisfilter". Wählen Sie "Ereignis_Protokollname" für "Spalte", behalten Sie "Gleich" für "Operator" bei, und wählen Sie "CALM" für "Wert".

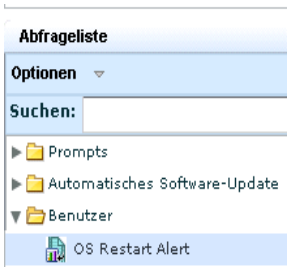
   c. Klicken Sie auf "Neuer Ereignisfilter". Wählen Sie "Empfänger_Name" für "Spalte", behalten Sie "Gleich" für "Operator" bei, und geben Sie "Automatische Software-Updates" ein.

   d. Klicken Sie auf "Neuer Ereignisfilter". Wählen Sie "Ergebnis_Zeichensatz" für "Spalte", behalten Sie "Gleich" für "Operator" bei, und geben Sie die Meldung "Auf diesem Host werden Updates des Betriebssystems installiert ... Bitte starten Sie den Computer neu, damit diese Updates wirksam werden !!!" ein.



3. Klicken Sie auf "Speichern und schließen".

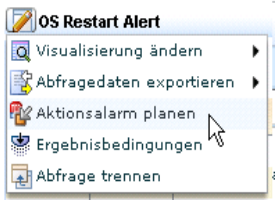
   Der neue Alarm erscheint in der Abfrageliste unter "Benutzerordner".



4. Planen Sie einen Aktionsalarm für die benutzerdefinierte Abfrage folgendermaßen:

   a. Wählen Sie die Abfrage unter "Benutzerordner".

   b. Klicken Sie auf die Schaltfläche "Bearbeiten" im rechten Fensterbereich, um die Dropdown-Liste "Alarm Betriebssystem neu starten" anzuzeigen, und wählen Sie "Aktionsalarm planen".



   Der Assistent "Aktionsalarm planen" wird mit dem Schritt "Alarmauswahl" angezeigt. Unter "Ausgewählte Abfragen" ist "Alarm Betriebssystem neu starten" vorausgewählt.

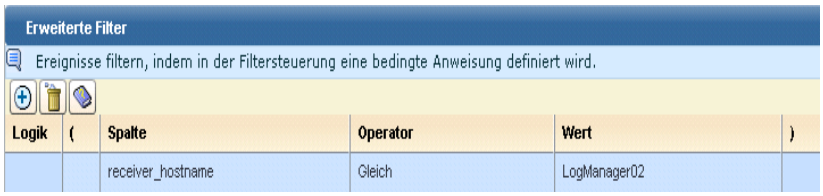
   c. Geben Sie einen Jobnamen ein. Geben Sie z. B. "Alarm Neustart des Betriebssystems" ein.

5. Fügen Sie folgendermaßen einen Ereignisfilter hinzu:

   a. Klicken Sie auf "Alarmfilter".

   b. Klicken Sie auf "Neuer Ereignisfilter".

   c. Wählen Sie "Empfänger_Hostname" für "Spalte", behalten Sie "Gleich" für "Operator" bei, und geben Sie den Namen des lokalen CA Enterprise Log Manager für "Wert" ein.



6. Legen Sie folgendermaßen die Häufigkeit fest, mit der Alarm gegeben wird, wenn ein Neustart erforderlich ist:

   a. Klicken Sie auf "Jobs planen"

   b. Legen Sie das Wiederholungsintervall für die Häufigkeit des Alarms fest. Geben Sie z. B. "1" und "Tag" für "einmal pro Tag" ein.

7. Wenn Sie per E-Mail benachrichtigt werden möchten, geben Sie folgendermaßen Ihre E-Mail-Informationen ein.
   a. Klicken Sie auf den Schritt "Ziel".
   b. Klicken Sie auf "E-Mail-Benachrichtigung aktivieren", und geben Sie Ihre E-Mail-Adresse sowie evtl. gewünschte weitere, optionale Informationen ein.
8. Schränken Sie folgendermaßen die Benachrichtigung auf den Fall ein, dass der aktuelle Server neu gestartet werden muss:
   a. Klicken Sie auf "Serverauswahl"
   b. Wählen Sie "Nein" für "Verbundabfrage".
9. Klicken Sie auf "Speichern und schließen", um den Alarmjob zu speichern.

   Der Aktionsalarmjob wird auf der Registerkarte "Alarmverwaltung", Unter-Registerkarte "Alarmplanung" angezeigt.

Aktionsalarmjobs

Jobname	Aktiviert	Server	Wiederholung	Startzeit	Endzeit
Restart Operating System Alert	wahr	caelm5	1 Tag	Freitag, 30. Oktober 2009, 16:12:19	

Beispiel: E-Mail an den Administrator, wenn Ereignisfluss stoppt

Administratoren müssen benachrichtigt werden, wenn ein Connector oder Agent keine Ereignisse mehr protokolliert. Sie können diese Benachrichtigung automatisieren, wenn ein Indikator darauf hinweist, dass diese Situation eingetreten ist. Sie können den Indikator konfigurieren. Dabei handelt es sich um die Zeit, die vergangen sein muss, seit ein Protokollquellserver Ereignisse von einem Connector erhalten hat. Sie können diese Zeitspanne auf eine beliebige Anzahl von Minuten, Stunden oder Tagen einstellen. Sie können die Abfrage auf alle Protokollquellserver in der Föderation erweitern.

Um die Anzahl von E-Mails zu beschränken, die versendet werden, wenn ein Connector fehlschlägt, sollten nur die Connectors berücksichtigt werden, die bis zu diesem Zeitpunkt Ereignisse erfasst haben. Stellen Sie einen Alarm beispielsweise so ein, dass nur Zeilen für Connectors zurückgegeben werden, die Ereignisse bis zu einer Stunde vor diesem Zeitpunkt erfasst haben, jedoch in der letzten Stunde keine Ereignisse mehr erfasst haben.

Um diese Daten zu erfassen, wählen Sie die vordefinierte Abfrage "Erfassungsüberwachung nach Protokollmanager - Agent-Connector nicht verfügbar". Diese Abfrage gibt den Namen des Connectors und des Agenten zurück, wenn keine Ereignisse mehr ankommen, wie in den Ergebnisbedingungen dieses Alarms definiert. Orientieren Sie sich an dem folgenden Beispiel, um einen Alarm zu generieren, wenn während der letzten Stunde keine Ereignisse von einem Connector empfangen wurden, der noch ein bis zwei Stunden zuvor Ereignisse gesendet hat. Geben Sie als Ziel für den Alarm die E-Mail-Adresse der Person an, die benachrichtigt werden soll. Um einen Plan zum Ausführen der Abfrage zu erstellen, legen Sie eine Frequenz fest, die größer oder gleich der abgelaufenen Zeitspanne ist.

Hinweis: E-Mail-Einstellungen müssen vor Erstellen des Alarms unter "Verwaltung", "Berichtsserver" vorgenommen werden.

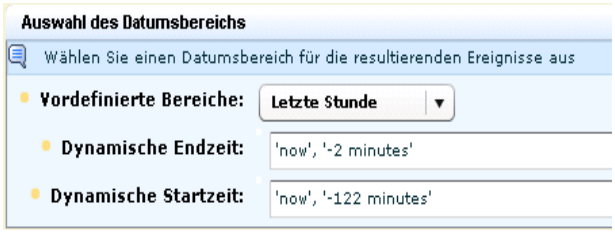
So senden Sie eine E-Mail an den Administrator, wenn ein Connector keine Ereignisse mehr erfasst

1. Wählen Sie den Server, von dem aus dieser Alarm ausgeführt werden soll. Wählen Sie in einer Hub-and-Spoke-Architektur einen Erfassungsserver aus, um die Bedingung so schnell wie möglich zu erfassen.
2. Wählen Sie die Registerkarte "Alarmverwaltung" und die Unterregisterkarte "Alarmplanung".
3. Klicken Sie auf "Aktionsalarm planen".
4. Geben Sie einen Namen für den Job ein, z. B: "Connector nicht verfügbar".
5. Wählen Sie unter "Verfügbare Abfragen" die Abfrage "Erfassungsüberwachung nach Protokollmanager - Agent-Connector nicht verfügbar", und verschieben Sie sie in die Liste "Ausgewählte Abfragen".

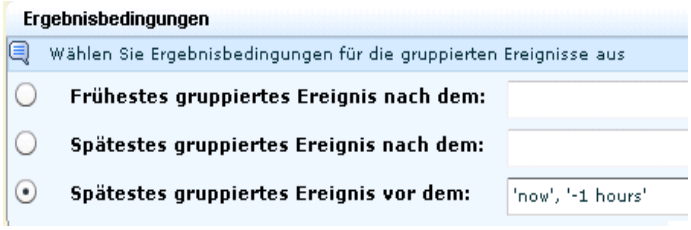
6. Klicken Sie auf "Ergebnisbedingungen".
7. Legen Sie die Zeit auf die letzten beiden Stunden fest.
   a. Wählen Sie "Vordefinierte Bereiche: Letzte Stunde".

      Dadurch setzen Sie die dynamische Endzeit genau auf "jetzt", "-2 Minuten".

   b. Klicken Sie unter "Dynamische Startzeit" auf "Dynamische Zeitzeichenfolge bearbeiten".
   c. Ersetzen Sie unter "Dynamische Zeitzeichenfolge" den Wert "62" durch "122".
   d. Klicken Sie auf OK.



8. Legen Sie die Ergebnisbedingungen fest.
   a. Wählen Sie "Spätestes gruppiertes Ereignis vor dem", und klicken Sie auf "Bearbeiten".
   b. Wählen Sie als Referenzzeit "Jetzt", und klicken Sie auf "Referenzzeit zur dynamischen Zeitzeichenfolge hinzufügen".
   c. Klicken Sie einmal auf den Pfeil nach unten, um die Zeit auf "-1" zu verschieben, wählen Sie aus der Dropdown-Liste "Stunde", und klicken Sie auf "Zeitverschiebung zur dynamischen Zeitzeichenfolge hinzufügen".
   d. Klicken Sie auf OK.



9. Klicken Sie auf den Schritt "Jobs planen", und definieren Sie das Wiederholungsintervall. Setzen Sie das Intervall zum Beispiel auf 1 Stunde.

10. Klicken Sie auf "Ziel", und füllen Sie die Registerkarte "E-Mail" aus.
    a. Wählen Sie "E-Mail-Benachrichtigung aktivieren".
    b. Geben Sie unter "E-Mail an" die E-Mail-Adresse des Administrators ein.
    c. Geben Sie unter "E-Mail von" Ihre E-Mail-Adresse ein.
    d. Geben Sie im Feld "Betreff" einen Betreff ein. Geben Sie beispielsweise "Connector möglicherweise ausgefallen" ein.
    e. Geben Sie den E-Mail-Text ein. Geben Sie beispielsweise ein: "Connector hat in der letzten Stunde keine Ereignisse mehr gesendet".
11. Klicken Sie auf "Serverauswahl", und löschen Sie den Wert unter "Föderiert", falls gewünscht.
12. Klicken Sie auf "Speichern und schließen".

Sie können diesen Alarm so definieren, dass der Datumsbereich in Tagen anstelle von Stunden abgefragt wird, und ihn dann so planen, dass er nur einmal am Tag ausgeführt wird. In diesem Fall wird die dynamische Endzeit auf 'Jetzt', die dynamische Startzeit auf 'Jetzt', '-2 Tage' und "Spätestes gruppiertes Ereignis vor dem" auf 'Jetzt', '-1 Tage' gesetzt.

Konfigurieren des Aufbewahrungszeitraums für Aktionsalarme

Sie können bestimmen, wie viele Aktionsalarme wie lange auf dem Berichtsserver gespeichert werden sollen.

So konfigurieren Sie den Aufbewahrungszeitraum für Aktionsalarme:

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

   Die Service-Liste wird angezeigt.

2. Bei einer globalen Einstellung klicken Sie auf "Berichtsserver", bei einer lokalen Einstellung auf den Host des Berichtsservers.

   Das Fenster für die Konfiguration des Berichtsservers wird angezeigt.

3. Geben Sie im Feld "Maximale Aktionsalarme" einen Wert ein. Überschreitet die Alarmanzahl diesen Wert, wird der älteste Alarm gelöscht.

4. Geben Sie im Feld "Aufbewahrungszeitraum für Aktionsalarme" den Zeitraum in Tagen ein, nach dessen Ablauf die Alarme gelöscht werden.

   Hinweis: Aktionsalarme werden gelöscht, wenn die zulässige Höchstzahl an Alarmen erreicht wurde.

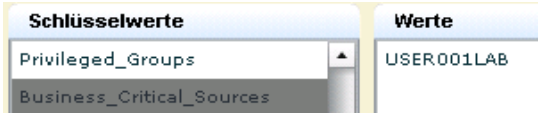
5. Klicken Sie auf "Speichern".

Beispiel: Erstellen eines Alarms für "Unternehmenskritische_Quellen"

Sie können eine benutzerdefinierte Abfrage mit der Schlüsselliste "Unternehmenskritische_Quellen" erstellen und auf der Grundlage dieser Abfrage einen Alarm planen. Die entsprechende Schlüsselliste enthält keine Standardwerte und keine/n zugehörige/n vordefinierte/n Abfrage oder Alarm. Verwenden Sie das folgende durchgehende Verfahren als Anleitung.

1. Installieren Sie einen Agenten.
2. Konfigurieren Sie einen Connector für diesen Agenten, um Ereignisse von allen unternehmenskritischen Quellen zu erfassen.

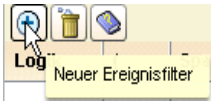
3. Geben Sie die Hostnamen-Werte an für die benutzerdefinierten Listen für "Unternehmenskritische_Quellen" (Schlüssel).
   a. Klicken Sie auf die Registerkarte "Verwaltung" und auf die Unter-Registerkarte "Services".
   b. Wählen Sie in der Service-Liste "Berichtsserver" aus.
   c. Wählen Sie "Unternehmenskritische_Quellen" im Bereich "Benutzerdefinierte Listen (Schlüssel)" aus.
   d. Klicken Sie auf "Wert hinzufügen" im Bereich "Werte", und geben Sie den Hostnamen einer unternehmenskritischen Quelle ein.



   e. Wiederholen Sie den letzten Schritt für jede unternehmenskritische Quelle, von der Ereignisse erfasst werden sollen.
   f. Klicken Sie auf "Speichern".
4. Erstellen Sie eine Abfrage nach fehlgeschlagenen Versuchen der Anmeldung durch unternehmenskritische Quellen.
   a. Klicken Sie auf "Abfragen und Berichte".
   b. Geben Sie unter "Abfrageliste" in das Suchfeld "Anmeldung" ein.
   c. Wählen Sie "Nicht erfolgreiche Anmeldeversuche nach Host" aus sowie "Kopieren" aus der Dropdown-Liste "Optionen".

      Der Assistent "Abfragedesign" wird geöffnet mit dem Namen "Kopie von Nicht erfolgreiche Anmeldeversuche nach Host".

      Benennen Sie die Abfrage um in "Nicht erfolgreiche Anmeldeversuche nach "Unternehmenskritischen_Quellen".
   d. Wählen Sie den Schritt "Abfragefilter".
   e. Klicken Sie auf die Registerkarte "Erweiterte Filter".
   f. Klicken Sie auf "Neuer Ereignisfilter".

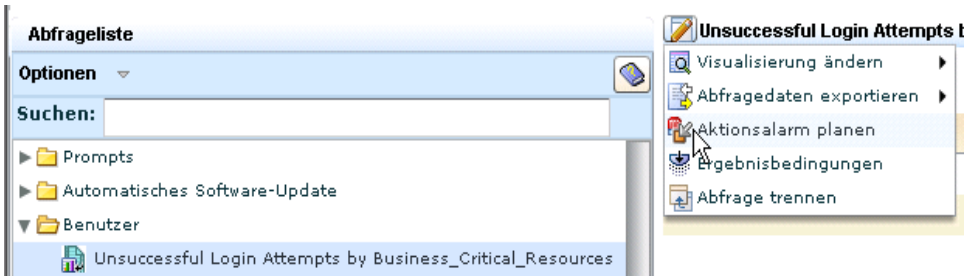


   g. Wählen Sie "Quelle_Hostname" für die "Spalte", "Mit Schlüssel" für den "Operator" und "Unternehmenskritische_Quellen" als "Wert".

Logik	(	Spalte	Operator	Wert	)
		source_hostname	Mit Schlüssel	Business_Critical_Sources	

h. Klicken Sie auf "Speichern und schließen".

5. Planen Sie auf der Basis dieser benutzerdefinierten Abfrage einen Alarm.
   a. Klicken Sie auf die Registerkarte "Abfragen und Berichte".
   b. Wählen Sie unter "Benutzerordner" in der Abfrageliste "Nicht erfolgreiche Anmeldeversuche nach "Unternehmenskritischen_Quellen".
   c. Wählen Sie "Aktionsalarm planen" aus der Dropdown-Liste "Bearbeiten".



   Der Assistent "Aktionsalarme planen" wird eingeblendet.
   d. Geben Sie einen Jobnamen ein, wie z. B. "Nicht erfolgreiche Anmeldeversuche nach unternehmenskritischen Quellen".
   e. Klicken Sie auf "Jobs planen" und legen Sie den Plan fest.
   f. Sie können ggf. auch E-Mail-Optionen für "Ziel" angeben.
   g. Klicken Sie auf "Speichern und schließen".
6. Überprüfen Sie, ob der Job geplant worden ist.
   a. Klicken Sie auf die Registerkarte "Alarmverwaltung" und auf die Unter-Registerkarte "Alarmplanung".
   b. Überprüfen Sie, ob der Jobname in die Liste eingefügt worden ist.

7. Überprüfen Sie, ob der Alarm erstellt worden ist.
   a. Klicken Sie auf die Registerkarte "Alarmverwaltung". Die Unter-Registerkarte "Aktionsalarme" wird eingeblendet.
   b. Zeigen Sie die aufgelisteten Alarme an, um festzustellen, ob der von Ihnen in die Liste eingeführte Jobname erscheint.

Bearbeiten von Aktionsalarmen

Sie können einen vorhandenen Aktionsalarm bearbeiten.

So bearbeiten Sie einen Aktionsalarm:

1. Klicken Sie auf die Registerkarte "Alarmverwaltung".

   Die Liste "Alarmserver" wird angezeigt.

2. Wählen Sie den Server aus, auf dem der Aktionsalarm, den Sie bearbeiten möchten, geplant ist.

   Das Fenster mit den Serverdetails wird angezeigt. Standardmäßig ist die Registerkarte "Generierte Berichte" geöffnet.

3. Klicken Sie auf die Registerkarte "Geplante Alarme", wählen Sie den gewünschten Alarm aus, und klicken Sie oben in der Liste auf "Bearbeiten".

   Der Assistent für die Planung von Aktionsalarmen wird geöffnet.

4. Nehmen Sie die gewünschten Änderungen vor, und klicken Sie auf "Speichern und schließen".

   Der bearbeitete Aktionsalarm wird in die Liste der Aktionsalarme übernommen.

Deaktivieren oder Aktivieren von Aktionsalarmen

Sie können einen oder mehrere Aktionsalarme inaktivieren, wenn Sie nicht länger möchten, dass die mit dem Aktionsalarm verbundenen planmäßigen Abfragen ausgeführt werden. Sie können zuvor deaktivierte Aktionsalarme aktivieren, so dass sie entsprechend dem gespeicherten Plan ausgeführt werden.

So deaktivieren oder aktivieren Sie einen Aktionsalarmjob:

1. Klicken Sie auf die Registerkarte "Alarmverwaltung" und auf die Unterregisterkarte "Alarmplanung".

   Die Liste "Aktionsalarmjobs" wird angezeigt. In der Spalte "Aktiviert" wird der Status der einzelnen Jobs aufgeführt. Wenn der Job aktiviert ist, wird unter "Aktiviert" der Wert "wahr" aufgeführt. Wenn der deaktiviert ist, wird unter "Aktiviert" der Wert "falsch" aufgeführt.

2. Wählen Sie den/die gewünschten Job(s), und klicken Sie auf "Auswahl aktivieren" oder "Auswahl deaktivieren".

   Die Liste "Aktionsalarmjobs" zeigt den neuen Status aller aktivierten oder deaktivierten Jobs an.

   Hinweis: Die Möglichkeit, Alarmjobs zu deaktivieren, ist bei wiederkehrenden Alarmen hilfreich. Wenn Sie einen einmaligen Alarmjob ("Einmalig") deaktiveren, wird er aus der Liste "Aktionsalarmjobs" entfernt.

Löschen von Aktionsalarmen

Nicht mehr benötigte Aktionsalarme können gelöscht werden.

So löschen Sie einen Aktionsalarm:

1. Klicken Sie auf die Registerkarte "Alarmverwaltung".

   Die Liste "Alarmserver" wird angezeigt.

2. Wählen Sie den Server aus, auf dem sich der Aktionsalarm, den Sie löschen möchten, befindet.

   Das Fenster "Serverdetails" wird geöffnet.

3. Klicken Sie auf die Registerkarte "Geplante Alarme", wählen Sie den gewünschten Alarm durch Klicken auf die entsprechende Zeile aus, und klicken Sie oben in der Liste auf "Löschen". Sie können mehrere Alarmjobs zum Löschen auswählen.

   Hinweis: Über die Kontrollkästchen neben den einzelnen Alarmjobs können Sie die Alarmjobs aktivieren oder deaktivieren.

   Ein Bestätigungsdialogfeld wird angezeigt.

4. Klicken Sie auf "Ja".

   Eine Meldung informiert Sie darüber, dass der Alarm gelöscht wurde.

5. Klicken Sie auf OK.

   Der Alarmjob wird aus der entsprechenden Liste gelöscht.

Kapitel 13: Geplante Berichte

Dieses Kapitel enthält folgende Themen:

Anzeigen generierter Berichte

Generierte Berichte können angezeigt und als Kopie an einem beliebigen Speicherort abgelegt werden. In der Soft-Appliance erstellte Berichte werden mit der Kennzeichnung "CA Enterprise Log Manager" an folgendem Ort gespeichert:

```
/opt/CA/LogManager/data/reports
```

So zeigen Sie einen generierten Bericht an:

1. Klicken Sie auf die Registerkarte "Geplante Berichte".

   Die Registerkarte öffnet sich und zeigt standardmäßig den lokalen CA Enterprise Log Manager-Host an.

2. Wählen Sie den Server aus, auf dem die generierten Berichte, die Sie anzeigen möchten, geplant sind.

   Der von Ihnen ausgewählte Server wird im Fenster "Details" angezeigt.

3. Andernfalls klicken Sie auf die Registerkarte "Generierte Berichte".

   Die Liste mit den generierten Berichten wird angezeigt.

4. Wählen Sie den Namen des Berichts aus, den Sie anzeigen möchten.

   Das Dialogfeld "Speichern" wird geöffnet.

5. Um einen Speicherort für den Bericht anzugeben, klicken Sie auf "Speichern".

Weitere Informationen:

Filtern von Berichten (siehe Seite 523)
Ergänzen generierter Berichte mit Anmerkungen (siehe Seite 524)
Planen von Berichtsjobs (siehe Seite 525)
Selbstüberwachende Ereignisse (siehe Seite 544)

Filtern von Berichten

Mit Hilfe von Filtern können Sie die Anzeige der verfügbaren generierten Berichte und Jobs für geplante Berichte verfeinern.

So filtern Sie generierte oder geplante Berichte:

1. Wählen Sie den Berichtsserver aus, auf dem sich die geplanten oder generierten Berichte befinden, und klicken Sie auf die Registerkarte "Generierte Berichte" oder "Geplante Berichte".

   Die Liste der geplanten oder generierten Berichte wird aufgerufen.

2. Wählen Sie im entsprechenden Dropdown-Menü den Widerholungstyp oder das Format aus, nach dem die angezeigten Berichte gefiltert werden sollen.

   Die Liste enthält die Berichte, die Ihre Filterkriterien erfüllen.

Weitere Informationen

Anzeigen generierter Berichte (siehe Seite 522)
Ergänzen generierter Berichte mit Anmerkungen (siehe Seite 524)

Ergänzen generierter Berichte mit Anmerkungen

Generierte Berichte können zu Nachverfolgungs- oder Prüfzwecken mit Anmerkungen versehen werden.

So ergänzen Sie einen generierten Bericht mit Anmerkungen:

1. Wählen Sie den Berichtsserver aus, auf dem sich die generierten Berichte befinden, die Sie mit Anmerkungen versehen möchten, und klicken Sie auf die Registerkarte "Generierte Berichte".

   Die Liste mit den generierten Berichten wird geöffnet.

2. Klicken Sie neben dem Bericht, den Sie kommentieren möchten, auf das Symbol für Anmerkungen.

   Das Dialogfeld "Berichtsanmerkungen" wird geöffnet. Darin werden frühere Anmerkungen mitsamt dem Namen des Autors, der Uhrzeit und dem Datum der Anfertigung angezeigt.

3. Kommentieren Sie den Bericht, und klicken Sie auf "Speichern".

   Die Anmerkung wird in das Dialogfeld übernommen. Zur Eingabe weiterer Anmerkungen bleibt das Dialogfeld geöffnet.

4. (Optional) Wiederholen Sie Schritt 3, um weitere Anmerkungen einzugeben.

5. Wenn Sie fertig sind, klicken Sie auf "Schließen".

   Das Dialogfeld "Berichtsanmerkungen" wird geschlossen.

Weitere Informationen

Anzeigen generierter Berichte (siehe Seite 522)
Filtern von Berichten (siehe Seite 523)

Planen von Berichtsjobs

Die Erstellung eines Berichtsjobs mit dem Assistenten für die Berichtsplanung umfasst folgende Hauptschritte:

1. Öffnen des Assistenten für die Berichtsplanung.
2. Auswählen der Berichtsvorlagen: Bei der Planung eines Berichtsjobs bestimmen Sie, welcher Bericht oder welche Kennung als Vorlage für den Job verwendet werden soll. Zur Auswahl stehen einzelne oder mehrere Vorlagen und Kennungen.
3. Erstellen der Berichtsfilter: Mit Hilfe erweiterter Berichtsfilter können noch individuellere Berichtsergebnisse erzielt werden.
4. Festlegen von Datumsbereich und Ergebnisbedingungen: Bestimmen Sie neben anderen Bedingungen für welchen Datumsbereich die Abfrage gilt.
5. Planen der Jobs: Legen Sie den Tag und die Uhrzeit fest, an dem bzw. zu der die Berichte (Einmalberichte und wiederkehrende Berichte) ausgeführt werden. Sie können auch eines der vorhandenen Muster zur Wiederholung von Berichten auswählen.
6. Auswählen des Berichtsformats und des Ziels: Wählen Sie das gewünschte Berichtsformat und die Optionen für den Versand per E-Mail aus.
7. Auswählen eines Servers: Wählen Sie den Server aus, der mit Hilfe des Berichts abgefragt werden soll. Legen Sie außerdem fest, ob die föderierten Hosts des Servers auch abgefragt werden sollen.

Öffnen des Assistenten zur Planung von Berichten

Wenn Sie einen neuen Berichtsjob für einen oder mehrere wiederkehrende Berichte erstellen möchten, öffnen Sie den Assistenten zur Planung von Berichten.

So öffnen Sie den Assistenten zur Planung von Berichten:

1. Klicken Sie auf die Registerkarte "Geplante Berichte".

   Die Liste der Berichtsserver wird angezeigt.

2. Wählen Sie den Server aus, auf dem Sie einen Bericht planen möchten.

   Im Fensterbereich "Berichtsserverdetails" wird der ausgewählte Server angezeigt. Standardmäßig ist die Registerkarte "Generierte Berichte" geöffnet.

3. Klicken Sie auf die Registerkarte "Berichtsplanung" und anschließend auf "Bericht planen".

   Der Assistent für die Planung von Berichten wird angezeigt.

   Beachten Sie bei Verwendung des Assistenten Folgendes:

   - Klicken Sie auf "Speichern und schließen", um den geplanten Bericht zu speichern und den Assistenten zu schließen.
   - Klicken Sie auf "Zurücksetzen", um die Ansicht im Assistenten auf die zuletzt gespeicherten Einstellungen zurückzusetzen.

Weitere Informationen

Festlegen von Planungsparametern (siehe Seite 534)
Erstellen erweiterter Ereignisfilter (siehe Seite 621)
Festlegen von Ergebnisbedingungen (siehe Seite 530)
Auswählen des Ziels einer Berichtsabfrage (siehe Seite 536)

Auswählen von Berichtsvorlagen

Wenn Sie einen neuen Berichtsjob erstellen möchten, wählen Sie zuerst eine Berichtsvorlage aus. Zur Planung mehrerer Berichtsjobs mit gemeinsamen Filtern, Ziel- und Planungseinstellungen wählen Sie mehrere Berichte oder Kennungen als Vorlagen aus.

Bei Auswahl mehrerer Berichte werden die Jobs einzeln nach Bericht angezeigt. Wenn Sie beispielsweise zwei einzelne Berichte auswählen, gelten für diese zwar die gleichen Optionen für Planung und Filter, sie werden in der Liste der generierten Berichte aber einzeln nach Berichtsname angezeigt.

Benutzer mit Administratorrolle können Berichtsjobs in einem inaktiven Status zur späteren Verwendung erstellen. Benutzer mit Administrator- und Analyst-Rolle können Jobs zu einem späteren Zeitpunkt aktivieren und deaktivieren. Bei inaktiven Berichten wird in der Spalte "Aktiviert" der Tabelle "Geplante Berichte" der Wert *falsch* angezeigt.

So wählen Sie eine Berichtsvorlage aus:

1. Geben Sie einen Jobnamen ein.
2. Wählen Sie im Dropdown-Menü "Zeitzone" die Zeitzone aus, in der Sie den Bericht planen möchten.
3. Um Berichte nach Kennung oder einzeln auszuwählen, aktivieren Sie das Optionsfeld "Berichte" oder "Kennungen".

   Hinweis: Werden Berichte nach Kennung geplant, können weitere Berichte hinzugefügt werden, ohne dass der Job an sich geändert werden muss. Bei Auswahl der Kennung "Identitätsverwaltung" werden sämtliche Berichte mit dieser Kennung dem Job zur geplanten Ausführungszeit hinzugefügt. Dies gilt auch für benutzerdefinierte Kennungen.
4. (Optional) Die Anzeige von Kennungen und Berichten kann durch Auswahl einer oder mehrerer Kennungen eingegrenzt werden. Mit dieser Funktion wird das Verhalten der Berichtsliste angepasst.
5. (Optional) Entfernen Sie die Markierung im Kontrollkästchen "Aktiviert", um diesen Berichtsjob in einem deaktiven Status zu erstellen. Das Kontrollkästchen "Aktiviert" ist standardmäßig markiert.

   Hinweis: Die Möglichkeit, einen deaktiven Berichtsjob zu erstellen, ist für wiederkehrende Berichte vorgesehen. Wenn Sie das Kontrollkästchen "Aktiviert" für einen Job deaktivieren und diesen Job als einmal auszuführenden Job ("Jetzt" oder "Einmal") erstellen, wird er aus der Liste "Geplante Berichte" entfernt.

6. (Optional) Aktivieren Sie das Feld "Nach Ablauf beibehalten", um die Berichtskonfiguration nach Generierung des Berichts beizubehalten.

   Hinweis: Nachdem der Bericht generiert wurde, können Sie die Berichtsvorlage bearbeiten und den Bericht neu planen.

7. Wählen Sie die Kennungen oder einzelnen Berichte aus, die als Vorlage verwendet werden sollen, und verschieben Sie sie mit der Wechselsteuerung in den Bereich für ausgewählte Berichte.

8. Fahren Sie mit dem Planungsschritt fort, den Sie als nächstes ausführen möchten, oder klicken Sie auf "Speichern und schließen".

   Bei Auswahl von "Speichern und schließen" wird der Bericht geplant. Andernfalls wird der von Ihnen ausgewählte Schritt eingeblendet.

Verwenden erweiterter Filter

Mit Hilfe erweiterter SQL-basierter Filter lassen sich die Funktionen zur Abfrage des Ereignisprotokollspeichers genauer definieren. Dazu gehören beispielsweise das Eingrenzen von Abfragen und das Anpassen von Schnellfiltern. Die Schnittstelle "Erweiterte Filter" beinhaltet ein Formular, in das Sie Logik, Spalten, Operatoren und Werte eintragen können, um die Filter in der richtigen Syntax zu erstellen.

Hinweis: Dieser Abschnitt enthält einen kurzen Überblick über die in den erweiterten Filtern verwendeten SQL-Begriffe. Um alle Möglichkeiten erweiterter Filter zu nutzen, sollten Sie mit SQL und der ELM-Schemadefinition vertraut sein.

Die folgenden SQL-Begriffe dienen zur Verknüpfung mehrerer Filteranweisungen:

And

Ereignisinformationen werden angezeigt, falls *alle* verbundenen Bedingungen zutreffen.

Or

Ereignisinformationen werden angezeigt, falls *eine* der verbundenen Bedingungen zutrifft.

Having

Zur Verfeinerung der Begriffe der SQL-Hauptanweisung, indem eine qualifzierende Anweisung hinzugefügt wird. Beispielsweise könnten Sie einen erweiterten Filter für Ereignisse bestimmter Hosts einrichten und durch Hinzufügen einer Having-Anweisung dafür sorgen, dass nur Ereignisse mit einem bestimmten Schweregrad von diesen Hosts zurückgegeben werden.

Folgende SQL-Operatoren werden von erweiterten Filtern für die grundlegenden Bedingungen verwendet:

Vergleichsoperatoren

Es werden die Ereignisinformationen aufgenommen, deren Spaltenwert dem entsprechenden Vergleich mit dem von Ihnen eingegebenen Wert standhält. Die folgenden Vergleichsoperatoren stehen zur Verfügung:

- Gleich
- Ungleich
- Kleiner als
- Größer als
- Kleiner oder gleich
- Größer oder gleich

Wenn Sie beispielsweise *Größer als* verwenden, werden die Ereignisinformationen aus Ihrer gewählten Spalte übernommen, falls deren Wert größer als der von Ihnen angegebene Wert ist.

Wie

Berücksichtigt die Ereignisinformationen, wenn die Spalte das von Ihnen angegebene Muster enthält. Verwenden Sie "%" für die Definition des Musters. Beispielsweise würde "L%" jeden Wert zurückgeben, der mit einem L beginnt und "%L%" alle Werte, die ein L enthalten, das jedoch weder an erster noch an letzter Stelle stehen darf.

Nicht wie

Berücksichtigt die Ereignisinformationen, falls der Spaltenwert nicht dem angegebenen Muster entspricht.

Enthalten

Berücksichtigt die Ereignisinformationen, wenn die Spalte einen oder mehrere der Werte enthält, die Sie durch Anführungszeichen getrennt eingegeben haben. Mehrere Werte in der Gruppe müssen mit einem Komma getrennt werden.

Nicht enthalten

Berücksichtigt die Ereignisinformationen, wenn die Spalte keinen der Werte enthält, die Sie durch Anführungszeichen getrennt eingegeben haben. Mehrere Werte in der Gruppe müssen mit einem Komma getrennt werden.

Übereinstimmend

Berücksichtigt beliebige Ereignisinformationen, die einem oder mehreren der von Ihnen eingegebenen Zeichen entsprechen. So können Sie nach Schlüsselwörtern suchen.

Mit Schlüssel

Schließt alle Ereignisinformationen ein, die beim Konfigurieren des Berichtsservers als Schlüsselwerte festgelegt wurden. Sie können Schlüsselwerte verwenden, um die Unternehmensrelevanz oder andere organisatorische Gruppen festzulegen.

Ohne Schlüssel

Schließt alle Ereignisinformationen ein, die beim Konfigurieren des Berichtsservers nicht als Schlüsselwerte festgelegt wurden. Sie können Schlüsselwerte verwenden, um die Unternehmensrelevanz oder andere organisatorische Gruppen festzulegen.

Festlegen von Ergebnisbedingungen

Sie können für die Abfrage einen Datumsbereich und andere Ergebnisbedingungen festlegen, wie die Begrenzung der Zeilen oder einen Basisanzeigezeitraum. Ergebnisbedingungen können bis zur Ausführung der Abfrage jederzeit geändert werden. Mit ihnen lassen sich Abfragen ändern, ohne dass die Abfrage an sich oder die zugehörigen Filter geändert werden müssen.

Folgende Typen von Ergebnisbedingungen stehen zur Auswahl:

- Bedingungen für den Datumsbereich zur Bestimmung des Abfragezeitraums
- Anzeigebedingungen (beispielsweise maximale Zeilenanzahl)
- Ergebnisbedingungen für gruppierte Ereignisse, wie z. B. die jüngsten gruppierten Ereignisse nach einem bestimmten Datum oder gruppierte Ereignisse mit einer bestimmten Anzahl an Ereignissen.

  Hinweis: Damit Benutzer die Ergebnisbedingungen in der Abfrageanzeige bearbeiten können, muss beim Erstellen einer Abfrage mindestens eine Spalte gruppiert werden.

Festlegen von Zeit- oder Datumsbereichen

Sie können Ihrer Abfrage eine Bedingung für den Zeit- oder Datumsbereich hinzufügen. Dies verbessert die Abfrageeffizienz, da die zu durchsuchende Datenmenge im Ereignisprotokollspeicher eingegrenzt wird.

Sie können einen vordefinierten Zeitraum verwenden oder einen benutzerdefinierten Zeitraum erstellen. Damit ein benutzerdefinierter Zeitraum ordnungsgemäß funktioniert, müssen Sie sowohl eine Anfangs- als auch eine Endzeit angeben. Wenn Sie nur einen Zeitparameter eingeben, wird dieser in der SQL-Abfrage als Where-Klausel wiedergegeben.

So legen Sie Ergebnisbedingungen fest:

1. Öffnen Sie das Dialogfeld "Ergebnisbedingungen".
2. Wählen Sie einen vordefinierten Zeitraum aus der Dropdown-Liste aus. Wenn Sie zum Beispiel die am Vortag eingegangenen Ereignisse anzeigen möchten, wählen Sie "Vorheriger Tag" aus.

   Hinweis: Wenn Sie einen Aktionsalarm oder geplanten Bericht erstellen, gibt die Schnittstelle die folgenden Standardzeitbereiche vor:

   - Aktionsalarm: vorherige 5 Minuten
   - Geplanter Bericht: vorherige 6 Stunden
3. (Optional) Mit den folgenden Zwischenschritten können Sie einen benutzerdefinierten Zeitraum erstellen:

   a. Klicken Sie im Bereich "Auswahl des Datumsbereichs" neben dem Wert für "Dynamische Endzeit" auf "Bearbeiten". Damit können Sie das Ende des Zeitraums festlegen, für den die Abfrage erfolgen soll.

   Das Dialogfeld "Dynamische Zeitangabe" wird angezeigt.

   b. Wählen Sie die Referenzzeit aus, auf der der Parameter basieren soll, und klicken Sie auf "Hinzufügen".

   c. Wählen Sie den gewünschten Zeitparameter aus, und klicken Sie auf "Hinzufügen". Sie können mehrere Zeitparameter hinzufügen.

   d. Sobald Sie alle Parameter hinzugefügt haben, klicken Sie auf "OK".

   Das Dialogfeld "Dynamische Zeitangabe" wird geschlossen, und die von Ihnen ausgewählten Werte werden im Bereich "Dynamische Endzeit" angezeigt. Bei Verwendung mehrerer Parameter ergeben diese eine vollständige Zeitangabe, bei der jeder Parameter auf den ersten verweist. Wenn Sie zum Beispiel im Bereich "Dynamische Endzeit" die Werte "Anfang des Monats" und "Wochentag – Dienstag" hinzufügen, endet Ihre Abfrage am ersten Dienstag des Monats.

Hinweis: Bei den "Anzahl"-Werten, z. B. "Anzahl der Tage" oder "Anzahl der Stunden" müssen Sie zur Einstellung eines vergangenen Zeitraums eine *negative* Zahl eingeben. Mit der Eingabe einer positiven Zahl stellen Sie eine zukünftige Endzeit ein, und die Abfrage liefert weiterhin Ergebnisse, solange sich mindestens ein qualifiziertes Ereignis im Protokollspeicher befindet.

Wenn Sie beispielsweise im Bereich "Dynamische Startzeit" die Werte "Jetzt" und "Anzahl der Minuten – 10" hinzufügen, beginnt Ihre Abfrage 10 Minuten vor der ausgewählten Endzeit.

e. Wiederholen Sie Schritt 2 im Bereich "Dynamische Startzeit", um den Beginn des Zeitraums festzulegen, für den die Abfrage erfolgen soll.

Wenn Sie keinen Datumsbereich eingeben, wird die Abfrage auf alle Ereignisse im Protokollspeicher angewandt.

4. Klicken Sie auf den entsprechenden Pfeil, um zu dem Schritt im Abfragedesign zu gelangen, den Sie als Nächsten durchführen möchten, oder klicken Sie auf "Speichern und schließen".

   Wenn Sie auf "Speichern und schließen" klicken, wird die neue Abfrage in der Abfrageliste angezeigt. Anderenfalls wird der von Ihnen ausgewählte Abfragedesignschritt angezeigt.

Weitere Informationen

Festlegen von Ergebnisbedingungen (siehe Seite 530)
Festlegen von Anzeige- und Gruppenbedingungen (siehe Seite 533)

Festlegen von Anzeige- und Gruppenbedingungen

Sie können Bedingungen festlegen, mit denen Sie einerseits die Ansicht der Abfrageanzeige einrichten und andererseits nach Ereignissen auf Basis ihres Gruppierungstyps suchen können.

So legen Sie Anzeige- und Gruppenbedingungen fest:

1. Öffnen Sie das Dialogfeld "Ergebnisbedingungen".
2. Mit den Kontrollkästchen unter "Ergebnisse" können Sie beliebige der folgenden Anzeigebedingungen aktivieren.

   Zeilenbegrenzung

   Legt die maximale Anzahl von Ereigniszeilen fest, die in der Abfrage angezeigt werden. Dabei stehen die neuesten Ereignisse am Anfang der Liste.

   Minimum: 1

   Maximum: 5000

   Andere anzeigen

   Weist auf das Vorhandensein weiterer Ergebnisse hin, die aufgrund der Zeilenbegrenzung nicht angezeigt werden. Dies ermöglicht Ihnen, die ausgewählten Ereignisse vor dem Hintergrund aller Ereignisse dieses Typs zu vergleichen. Wenn Sie zum Beispiel für Ihre Ereignisanzeige als Zeilenbegrenzung den Wert 10 angeben und "Andere anzeigen" aktivieren, werden alle über den Wert 10 hinausgehenden Ereignisse zu einem Eintrag mit der Bezeichnung "Andere" zusammengefasst, der alle übrigen Ereignisse anzeigt. Diese Einstellung ist nur wirksam, wenn eine Zeilenbegrenzung ausgewählt wurde.

   Zeitgranularität

   Legt den Detailgrad des in der Abfrageanzeige verwendeten Zeitraumfeldes fest.

3. Mit "Ergebnisbedingungen" können Sie für die Abfrage Bedingungen angeben, mit denen Ereignisse nach ihrem Gruppierungstyp gesucht werden. Beispielsweise könnten Sie Ihre Abfrage so einrichten, dass das neueste gruppierte Ereignis nach einem ausgewählten Datum oder eine bestimmte Anzahl von gruppierten Ereignissen gesucht wird. Ein gruppiertes Ereignis ist ein verfeinertes Ereignis, für das Sie im Abfrageerstellungsschritt eine Funktion und eine Gruppenreihenfolge festgelegt haben.

   Die Gruppenbedingungen basieren auf demselben Zeitangabesystem wie bei den Feldern für den Zeitbereich.

4. Klicken Sie auf den entsprechenden Pfeil, um zu dem Schritt im Abfragedesign zu gelangen, den Sie als Nächsten durchführen möchten, oder klicken Sie auf "Speichern und schließen".

   Wenn Sie auf "Speichern und schließen" klicken, wird die neue Abfrage in der Abfrageliste angezeigt. Anderenfalls wird der von Ihnen ausgewählte Abfragedesignschritt angezeigt.

Weitere Informationen:

Festlegen von Ergebnisbedingungen (siehe Seite 530)

Festlegen von Planungsparametern

Sie können bestimmen, wann geplante Berichte ausgeführt werden und ob und in welchem Abstand sie wiederholt werden.

So legen Sie Planungsparameter fest:

1. Öffnen Sie den Assistenten für die Planung von Berichten, und fahren Sie mit dem Schritt zur Planung von Jobs fort.
2. Wählen Sie mit Hilfe der Optionsfelder "Nicht wiederkehrend" oder "Wiederkehrend" ggf. das Wiederholungsintervall aus und wann der Bericht erstellt werden soll.

   Hinweis: Wenn für Ihre Umgebung die Sommerzeit gilt, planen Sie während der Zeitumstellung keinen Bericht, da dieser nicht erstellt wird. Beginnt die Sommerzeit beispielsweise am 8. März um 2 Uhr morgens, können Sie zwischen 2:00:00 Uhr und 2:59:59 Uhr keine Berichtsausführung planen.
3. Fahren Sie mit dem Planungsschritt fort, den Sie als nächstes ausführen möchten, oder klicken Sie auf "Speichern und schließen".

   Bei Auswahl von "Speichern und schließen" wird der Bericht geplant. Andernfalls fahren Sie mit dem gewünschten Schritt fort.

Weitere Informationen

Verwenden erweiterter Filter (siehe Seite 528)
Festlegen von Ergebnisbedingungen (siehe Seite 530)
Auswählen des Ziels einer Berichtsabfrage (siehe Seite 536)

Auswählen von Format und Benachrichtigungseinstellungen

Berichte werden wahlweise im PDF-, Excel- oder XML-Format erstellt. Ferner können Sie eine automatische E-Mail-Benachrichtigung einrichten.

So legen Sie Format und Benachrichtigung fest:

1. Öffnen Sie den Assistenten für die Planung von Berichten, und fahren Sie mit dem Schritt zur Festlegung des Ziels fort.
2. Wählen Sie das gewünschte Format im Dropdown-Menü "Berichtsformat" aus.

   Hinweis: Im PDF-Format sind Diagramme auf 100 Datenpunkte begrenzt, wodurch die Achsenbeschriftungen deutlich lesbar bleiben. Wenn das Diagramm, das Sie anzeigen möchten, mehr als 100 Punkte umfasst, nimmt CA Enterprise Log Manager nur die ersten 100 in die erstellte PDF-Datei auf.
3. Soll nach Erzeugung des Berichts eine Benachrichtigung gesendet werden, aktivieren Sie das Kontrollkästchen "E-Mail".

   Das Feld zur Eingabe der E-Mail-Adresse wird angezeigt.
4. Geben Sie die E-Mail-Adresse aller Benutzer ein, die benachrichtigt werden sollen. Trennen Sie mehrere Adressen durch ein Komma.
5. (Optional) Nehmen Sie weitere Eingaben vor, darunter den Betreff, die E-Mail-Adresse zum Antworten und den Text.
6. (Optional) Um eine Kopie des Berichts im gewünschten Format an die E-Mail anzuhängen, wählen Sie die Option "Bericht anhängen" aus.
7. Fahren Sie mit dem Planungsschritt fort, den Sie als nächstes ausführen möchten, oder klicken Sie auf "Speichern und schließen".

   Bei Auswahl von "Speichern und schließen" wird der Bericht geplant. Andernfalls wird der von Ihnen ausgewählte Schritt eingeblendet.

Weitere Informationen

Verwenden erweiterter Filter (siehe Seite 528)
Festlegen von Ergebnisbedingungen (siehe Seite 530)
Festlegen von Planungsparametern (siehe Seite 534)
Auswählen des Ziels einer Berichtsabfrage (siehe Seite 536)

Auswählen des Ziels einer Berichtsabfrage

Sie können bestimmen, in welchem Ereignisprotokoll die Berichtsabfragen gespeichert werden.

So wählen Sie Berichtsziele aus:

1. Öffnen Sie den Assistenten für die Planung von Berichten, und fahren Sie mit dem Schritt zur Serverauswahl fort.
2. Wählen Sie verfügbare Server aus, die Sie abfragen möchten, und verschieben Sie diese mit der Wechselsteuerung in den Bereich "Ausgewählte Server".
3. (Optional) Wenn Sie föderierte Abfragen für den Bericht deaktivieren möchten, wählen Sie im Dropdown-Menü, das nach Klicken auf "Föderierte Abfragen " angezeigt wird, die Option "Nein" aus. Berichtsabfragen sind standardmäßig föderiert.
4. Fahren Sie mit dem Planungsschritt fort, den Sie als nächstes ausführen möchten, oder klicken Sie auf "Speichern und schließen".

   Bei Auswahl von "Speichern und schließen" wird der Bericht geplant. Andernfalls fahren Sie mit dem gewünschten Schritt fort.

Weitere Informationen

Verwenden erweiterter Filter (siehe Seite 528)
Festlegen von Ergebnisbedingungen (siehe Seite 530)
Festlegen von Planungsparametern (siehe Seite 534)

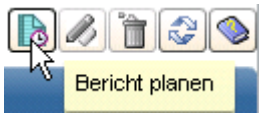
Beispiel: Planen von Berichten mit einer gemeinsamen Kennung

Sie können planen, dass ein Bericht oder mehrere Berichte bis zum angegebenen Enddatum so oft wie angegeben generiert werden.

Auditoren, Analysten und Administratoren können Berichte planen.

So planen Sie Berichte:

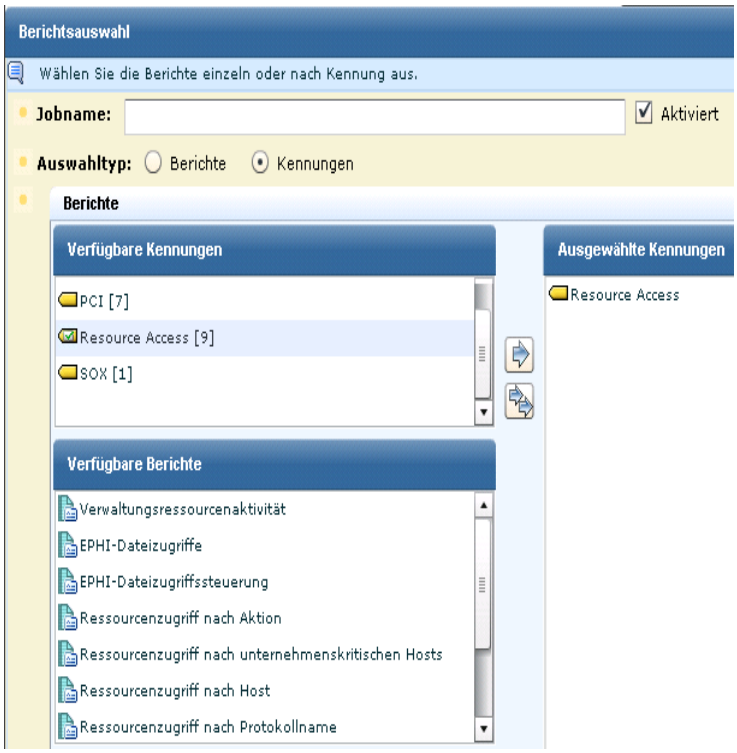
1. Klicken Sie auf die Registerkarte "Geplante Berichte", auf die Unterregisterkarte "Berichtsplanung" und anschließend auf "Bericht planen".



   Der Assistent zur Planung von Berichten wird angezeigt, wobei Schritt 1, "Berichtsauswahl", ausgewählt ist.

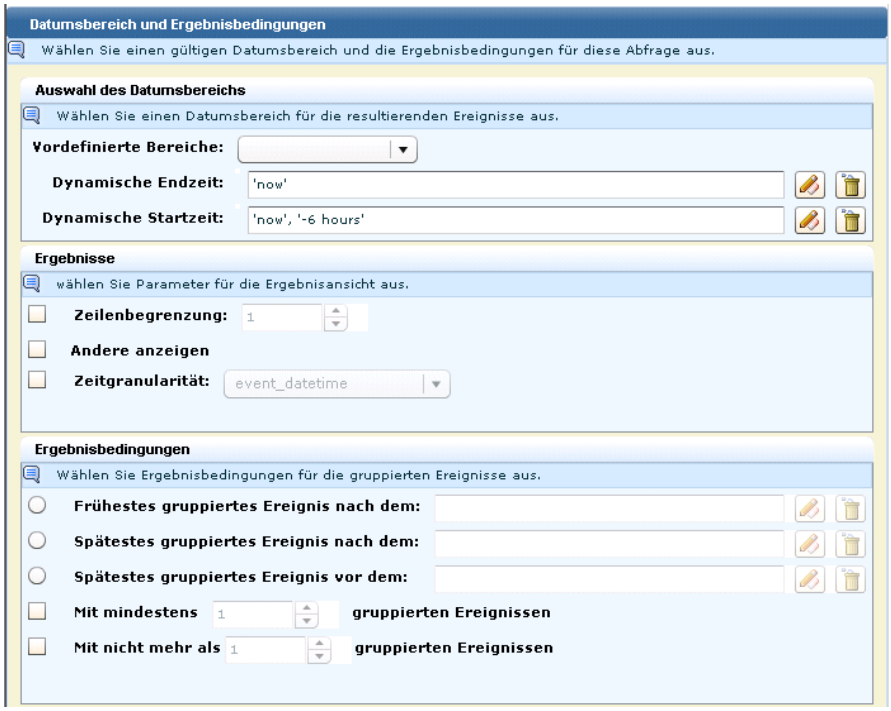
2. Geben Sie einen Jobnamen ein, und wählen Sie "Berichte" aus, um die Auswahl einzelner Berichte zu ermöglichen, oder aber "Kennungen", damit alle Berichte ausgewählt werden können, denen einer ausgewählten Kennung zugeordnet ist.

   Im folgenden Beispiel können Sie durch Auswahl der Kennungen vom Typ "Ressourcenzugriff" problemlos die sechs zugehörigen Berichte auswählen.



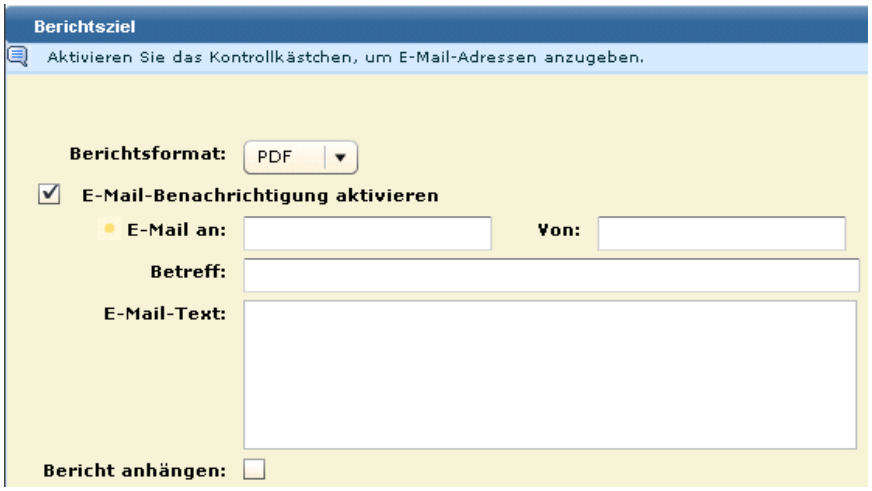
3. (Optional) Klicken Sie auf "Berichtsfilter", und erstellen Sie einen neuen Filter, um den Bericht auf die benötigten Daten zu beschränken.

4. (Optional) Klicken Sie auf "Ergebnisbedingungen", und wählen Sie einen Datumsbereich und/oder Ergebnisbedingungen für diese Abfrage aus. Wenn Sie beispielsweise nach Ereignissen suchen möchten, die innerhalb der letzten sechs Stunden aufgetreten sind, wählen Sie unter "Dynamische Endzeit" die Option "Jetzt" und unter "Dynamische Startzeit" die Option "-6 Stunden" aus. Aktivieren Sie das Kontrollkästchen "Zeilenbegrenzung", und wählen Sie eine Zahl aus, beispielsweise 250.



5. Klicken Sie auf "Geplante Jobs", um die Generierung für "Jetzt" zu planen, oder wählen Sie eine andere Option aus, und geben Sie die entsprechenden Details an.

6. Klicken Sie auf "Ziel", und legen Sie fest, ob der Bericht als Excel-Arbeitsblatt, PDF- oder XML-Dokument formatiert werden soll. Ein Arbeitsblatt eignet sich für Tabellendaten. Ein PDF-Dokument eignet sich für Grafiken. Optional können Sie auch eine E-Mail-Benachrichtigung senden. (Verwenden Sie als Trennzeichen zwischen mehreren E-Mail-Adressen das Komma.) Die E-Mail kann ohne Bericht nur zur Bestätigung gesendet werden, dass der geplante Bericht generiert wurde. Sie können den Bericht jedoch auch als Anlage der E-Mail senden.



Hinweis: Der Administrator kann Berichte so konfigurieren, dass sie nach dem angegebenen Aufbewahrungszeitraum gelöscht werden. Als Alternative zur manuellen Archivierung können Sie eine Kopie der E-Mail aufbewahren.

7. Klicken Sie auf "Serverauswahl", und wählen Sie mindestens einen Server für die Berichte aus. Geben Sie dabei an, ob die Föderation des Servers abgefragt werden soll.

8. Klicken Sie auf "Speichern und schließen".

   Die Generierung der ausgewählten Berichte wird geplant.

Beispiel: Versenden täglicher PCI-Berichte via E-Mail als PDF-Dateien

Sie können die Übermittlung bestimmter Berichte in dem von Ihnen gewählten Format an eine von Ihnen angegebene Person und in der erforderlichen Häufigkeit automatisieren.

Bevor Sie festlegen können, dass geplante Berichte als PDF-Dateien formatiert und an E-Mails angehängt werden, müssen Sie unter der Registerkarte "Verwaltung" und der Unter-Registerkarte "Services" in der globalen Service-Konfiguration für den Berichtsserver Folgendes konfigurieren.

- Mailserveroptionen:
  - Mailserver
  - SMTP-Port (25)
  - Admin-E-Mail
  - SMTP-Benutzername und -Kennwort
- PDF-Spezifikationen:
  - Unternehmens-/Produktname
  - Unternehmens-/Produktlogo URL
  - Schriftart und Schriftgröße für Kopfzeile
  - Schriftart und Schriftgröße für Daten
  - Seitenausrichtung, -breite und -höhe

Beispiel: Übermittlung aller täglichen PCI-Berichte an allen Werktagen als PDF-Dateien an den Posteingang des Auditors

1. Klicken Sie auf die Registerkarte "Geplante Berichte" und auf die Unter-Registerkarte "Berichtsplanung".

   Die Symbolleiste mit der Schaltfläche "Berichte" wird angezeigt.

2. Klicken Sie auf "Einen Bericht planen"

   Das Fenster „Berichtsauswahl“ wird angezeigt.

3. Wählen Sie folgendermaßen einen Bericht aus:

   a. Geben Sie "PCI-Berichte" als Jobnamen ein.

   b. Wählen Sie "Kennungen" als Auswahltyp.

   c. Wählen Sie "PCI" unter "Verfügbare Kennungen" aus und verschieben Sie sie nach "Ausgewählte Kennungen".

4. Planen Sie den Job folgendermaßen:
   a. Klicken Sie auf den Schritt "Jobs planen".
   b. Wählen Sie "Täglich" unter "Wiederkehrend".
   c. Wählen Sie alle Wochentage aus.
5. Wählen Sie das Berichtsziel und das Format wie folgt aus:
   a. Klicken Sie auf die Registerkarte "Ziel".
   b. Akzeptieren Sie das Standardberichtsformat PDF.
   c. Wählen Sie "E-Mail-Benachrichtigung aktivieren".
   d. Geben Sie die E-Mail-Adresse des Auditors ein. Verwenden Sie die folgende Syntax: <E-Mail_Name>@<Unternehmen>.com
   e. Wählen Sie "Bericht anhängen".
6. Klicken Sie auf "Speichern und schließen".

Bearbeiten von Jobs für geplante Berichte

Die Jobs für geplante Berichte können bearbeitet werden.

So bearbeiten Sie einen Job für einen geplanten Bericht:

1. Klicken Sie auf die Registerkarte "Geplante Berichte".

   Die Liste der Berichtsserver wird angezeigt.
2. Wählen Sie den Server aus, auf dem der Bericht, den Sie bearbeiten möchten, geplant ist.

   Der ausgewählte Server wird im Fenster "Berichtsserverdetails" angezeigt.
3. Wählen Sie den gewünschten Berichtsjob aus, und klicken Sie oben in der Liste auf die Schaltfläche "Bearbeiten".

   Der Assistent für die Planung von Berichten wird angezeigt.
4. Führen Sie die gewünschten Änderungen durch, und klicken Sie auf "Speichern und schließen".

   Der bearbeitete Bericht wird innerhalb von fünf Minuten, d. h. nach Aktualisierung der Liste der geplanten Jobs, in dieser angezeigt. Um die Liste sofort zu aktualisieren, klicken Sie auf "Aktualisieren".

Weitere Informationen

Planen von Berichtsjobs (siehe Seite 525)
Löschen von Jobs für geplante Berichte (siehe Seite 544)

Aktivieren und Deaktivieren von geplanten Berichtsjobs

Sie können einen oder mehrere geplante Berichtsjobs deaktivieren, wenn die mit diesem Bericht verknüpften Abfragen nicht mehr ausgeführt werden sollen. Sie können zuvor deaktivierte geplante Berichtsjobs auch aktivieren, so dass sie entsprechend dem gespeicherten Plan ausgeführt werden.

So deaktivieren oder aktivieren Sie geplante Berichtsjobs:

1. Klicken Sie auf die Registerkarte "Geplante Berichte" und auf die Unterregisterkarte "Berichtsplanung".

   Die Liste "Geplante Jobs" wird angezeigt. In der Spalte "Aktiviert" wird der Status der einzelnen Jobs aufgeführt. Wenn der Job aktiviert ist, wird unter "Aktiviert" der Wert "wahr" aufgeführt. Wenn der deaktiviert ist, wird unter "Aktiviert" der Wert "falsch" aufgeführt.

2. Wählen Sie den/die gewünschten Job(s), und klicken Sie auf "Auswahl aktivieren" oder "Auswahl deaktivieren".

   Die Liste "Geplante Jobs" zeigt den neuen Status aller aktivierten oder deaktivierten Jobs an.

   Hinweis: Die Möglichkeit, Berichtsjobs zu deaktivieren, ist bei wiederkehrenden Berichten hilfreich. Wenn Sie einen einmaligen Berichtsjob ("Einmalig") deaktiveren, wird er aus der Liste "Geplante Jobs" entfernt.

Löschen von Jobs für geplante Berichte

Die Jobs für geplante Berichte können gelöscht werden.

So löschen Sie einen Job für einen geplanten Bericht:

1. Klicken Sie auf die Registerkarte "Geplante Berichte".

   Die Liste der Berichtsserver wird angezeigt.

2. Wählen Sie den Server aus, auf dem der Bericht, den Sie löschen möchten, geplant ist.

   Der ausgewählte Server wird im Fenster "Berichtsserverdetails" angezeigt.

3. Klicken Sie auf die Registerkarte "Berichtsplanung", wählen Sie den gewünschten Job durch Klicken auf die entsprechende Zeile aus, und klicken Sie oben in der Liste auf "Löschen". Sie können mehrere Jobs zum Löschen auswählen.

   Hinweis: Über die Kontrollkästchen neben den einzelnen Berichtsjobs können Sie die Berichtsjobs aktivieren oder deaktivieren.

   Ein Bestätigungsdialogfeld wird angezeigt.

4. Klicken Sie auf "Ja".

   Der Job für den geplanten Bericht wird aus der entsprechenden Liste gelöscht.

Weitere Informationen:

Planen von Berichtsjobs (siehe Seite 525)
Bearbeiten von Jobs für geplante Berichte (siehe Seite 542)

Selbstüberwachende Ereignisse

Die meisten vom Benutzer getätigten Aktionen führen zu selbstüberwachenden Ereignissen. Mit Hilfe dieser Ereignisse können Sie verfolgen, welche Aktionen im Zusammenhang mit dem Server durchgeführt wurden und welche Aktionen fehlschlugen. Selbstüberwachende Ereignisse werden in der Ereignisanzeige auf den Registerkarten "Geplante Berichte" und "Alarmverwaltung" nach Server angeordnet angezeigt. Mit Hilfe des Berichts "Selbstüberwachende Ereignisse" können sie auch als normale oder geplante Berichte abgerufen werden.

Weitere Informationen

Anzeigen selbstüberwachender Ereignisse (siehe Seite 545)
Planen von Berichtsjobs (siehe Seite 525)

Anzeigen selbstüberwachender Ereignisse

Wichtige selbstüberwachende Ereignisse lassen sich auf den Registerkarten "Geplante Berichte" und "Alarmverwaltung" nach Server angeordnet anzeigen. Zur Anzeige von Alarmen oder Überwachungsereignissen kann die Ansicht der einzelnen Registerkarten entsprechend gefiltert werden. Wenn Sie den Filter entfernen, werden alle selbstüberwachenden Ereignisse angezeigt.

So zeigen Sie selbstüberwachende Ereignisse an:

1. Öffnen Sie die Registerkarte "Geplante Berichte" oder "Alarmverwaltung".

   Die Liste der Berichts- oder Alarmserver wird aufgerufen.

2. Wählen Sie den Server aus, dessen lokale selbstüberwachende Ereignisse Sie einsehen möchten.

   Der von Ihnen ausgewählte Server wird im Fenster "Details" angezeigt.

3. Klicken Sie auf die Registerkarte "Selbstüberwachende Ereignisse".

   Die Ereignisanzeige für selbstüberwachende Ereignisse wird mit den selbstüberwachenden Ereignissen im Zusammenhang mit Berichten oder Alarmen angezeigt. Sie können von hier aus alle Aufgaben durchführen, die normalerweise an Berichten vorgenommen werden. Dazu gehören:

   - Aufgaben zur Ereignisanzeige
   - Globales oder lokales Filtern
   - Festlegen von Favoriten
   - Exportieren

Kapitel 14: Unterdrückung und Zusammenfassung

Dieses Kapitel enthält folgende Themen:

Versionen von Ereignisverfeinerungskomponenten

CA Enterprise Log Manager behält frühere Versionen bestimmter benutzerdefinierter Ereignisverfeinerungskomponenten zurück, wenn Sie sie erstellen und bearbeiten. So können Sie auf frühere Versionen zurückgreifen. Sie können Versionen der folgenden Komponenten anzeigen oder kopieren:

- Meldungsanalysedateien
- Datenzuordnungsdateien
- Unterdrückungsregeln
- Zusammenfassungsregeln

Jedes Mal, wenn Sie eine neue benutzerdefinierte Komponente erstellten, wird diese als Version 1.0 bezeichnet. Wenn Sie eine neue Version desselben Objekts bearbeiten und speichern, wird sie als Version 2.0 bezeichnet. Beide Versionen werden in einem geeigneten Bereich der Benutzeroberfläche zur Auswahl und Anwendung angezeigt.

Wenn Sie z. B. eine benutzerdefinierte Unterdrückungsregel mit der Bezeichnung "NeueRegel" erstellen, wird sie als Version 1.0 in der Benutzeroberflächenliste "Ereignisprotokollspeicher" zur Anwendung angezeigt. Wenn Sie diese Datei bearbeiten, wird sie als "NeueRegel, Version 2.0" in der Liste "Ereignisprotokollspeicher" angezeigt.

Sie können frühere Versionen von Ereignisverfeinerungskomponenten in der entsprechenden Liste einsehen. Sie sind schreibgeschützt und können nicht bearbeitet werden. Sie können jedoch alte Versionen kopieren, bearbeiten und so zu einer neuen Version machen. Um bei dem vorigen Beispiel zu bleiben: Sie können "NeueRegel, Version 1.0" nicht mehr bearbeiten, sobald die Version 2.0 existiert. Sie müssen vielmehr Version 1.0 kopieren und bearbeiten. Speichern der Änderungen führt zu Version 3.0.

Weitere Informationen

Bearbeiten von Unterdrückungs- oder Zusammenfassungsregeln (siehe Seite 570)

Aufgaben mit Unterdrückungs- und Zusammenfassungsregeln

Mit Hilfe von Unterdrückungs- und Zusammenfassungsregeln können Sie den Ereignisablauf und die Größe des Ereignisprotokollspeichers durch Löschen oder Kombinieren bestimmter Ereignisse regulieren. Unterdrückungsregeln dienen dazu, die Erfassung nativer Ereignisse, die den Regelkriterien entsprechen, zu unterbinden. Mit Zusammenfassungsregeln lassen sich mehrere native Ereignisse zu einem einzigen verfeinerten Ereignis zusammenfassen. Dieses wird dann anstelle der ursprünglichen Ereignisse angezeigt.

Wichtig! Verwenden Sie Unterdrückungs- und Zusammenfassungsregeln nur nach reiflicher Überlegung, da die Aufzeichnung und Anzeige bestimmter nativer Ereignisse damit evtl. verhindert wird. Testen Sie die Regeln vor ihrer Anwendung zuerst in einer Testumgebung.

Unterdrückungs- und Zusammenfassungsaufgaben können allesamt in der Protokollerfassung in der Benutzeroberfläche ausgeführt werden. Benutzerdefinierte Unterdrückungs- und Zusammenfassungsregeln können erstellt, bearbeitet und gelöscht werden.

Weitere Informationen

Erstellen von Unterdrückungsregeln (siehe Seite 551)
Erstellen von Zusammenfassungsregeln (siehe Seite 557)
Anwenden von Unterdrückungs- oder Zusammenfassungsregeln (siehe Seite 565)
Kopieren von Unterdrückungs- oder Zusammenfassungsregeln (siehe Seite 569)
Bearbeiten von Unterdrückungs- oder Zusammenfassungsregeln (siehe Seite 570)
Löschen von Unterdrückungs- oder Zusammenfassungsregeln (siehe Seite 571)
Importieren von Unterdrückungs- oder Zusammenfassungsregeln (siehe Seite 572)
Exportieren von Unterdrückungs- oder Zusammenfassungsregeln (siehe Seite 573)

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.

Erstellen von Unterdrückungsregeln

Mit Unterdrückungsregeln können Sie dafür sorgen, dass zahlenmäßig umfangreiche Routinevorgänge oder bekannte und vorhergesehene Transaktionen den Ereignisprotokollspeicher nicht unnötig aufblähen und sich so negativ auf die Umgebung auswirken. Beispielsweise könnten Sie mit Hilfe einer Unterdrückungsregel überflüssige Syslog-Informationsereignisse unterbinden, insbesondere dann, wenn die Ereignisquelle nicht so konfiguriert werden kann, dass nur erforderliche Sets übertragen werden.

Die Erstellung einer Unterdrückungsregel mit dem Assistenten für Unterdrückungsregeln umfasst folgende Schritte:

1. Öffnen des Assistenten für Unterdrückungsregeln.
2. Benennen der Regel: Eingeben von Name und Beschreibung.
3. Ereignisauswahl: Angeben des zu unterdrückenden Ereignisses. Dazu verwenden Sie die CEG-Standardisierungsattribute und wahlweise erweiterte Filter.

Hinweis: Nachdem Sie die Unterdrückungsregel erstellt haben, übernehmen Sie sie, damit sie in der Umgebung zur Verfügung steht.

Weitere Informationen

Öffnen des Assistenten für Unterdrückungen (siehe Seite 552)
Benennen von Unterdrückungsregeln (siehe Seite 552)
Anwenden von Unterdrückungs- oder Zusammenfassungsregeln (siehe Seite 565)

Öffnen des Assistenten für Unterdrückungen

Zum Erstellen einer neuen oder zum Bearbeiten einer vorhandenen Unterdrückungsregel öffnen Sie den Assistenten für Unterdrückungen.

So öffnen Sie den Assistenten für Unterdrückungen:

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

   Die Ordnerliste "Protokollerfassung" wird angezeigt.

2. Erweitern Sie den Ordner "Ereignisverfeinerungs-Bibliothek" durch Klicken auf den Pfeil daneben, und wählen Sie anschließend den Ordner "Unterdrückung und Zusammenfassung" aus.

   Die Schaltflächen zur Unterdrückung und Zusammenfassung werden im Detailbereich angezeigt.

3. Klicken Sie auf "Neue Unterdrückungsregel": 

   Der Assistenten für Unterdrückungen wird geöffnet.

   Beachten Sie bei Verwendung des Assistenten Folgendes:

   - Klicken Sie auf "Speichern", um die Regeldatei zu speichern, ohne den Assistenten zu schließen.
   - Klicken Sie auf "Speichern und schließen", um die Regeldatei zu speichern und den Assistenten zu schließen.
   - Klicken Sie auf "Zurücksetzen", um die Ansicht im Assistenten auf die zuletzt gespeicherten Einstellungen zurückzusetzen.

Weitere Informationen

Benennen von Unterdrückungsregeln (siehe Seite 552)

Benennen von Unterdrückungsregeln

Sie müssen eine Unterdrückungsregel mit einem Namen versehen. Sie können auch optional zu Referenzzwecken eine Beschreibung eingeben.

So benennen Sie eine Unterdrückungsregel:

1. Öffnen Sie den Assistenten für Unterdrückungen.
2. Geben Sie einen Namen für die neue Regel ein.
3. (Optional) Geben Sie eine Beschreibung ein.
4. Fahren Sie mit dem Schritt "Filterung" fort.

Weitere Informationen

Erstellen von Unterdrückungsregeln (siehe Seite 551)

Auswählen zu unterdrückender Ereignisse

Geben Sie das native Ereignis an, das mit der Regel unterdrückt werden soll, indem Sie einen einfachen Filter für die Felder "CEG-Ereignisnormalisierung" festlegen. Die Felder gehören der ereignisspezifischen Klasse an, werden für alle in der CEG ausgedrückten Ereignisse verwendet und erlauben die genaue Angabe eines nativen Ereignisses.

Sie können die gewünschte Kombination von Ereignisnormalisierungsfeldern auf der Registerkarte "Einfache Filter" festlegen. Zusätzliche Filter sorgen für zusätzliche Detailangaben bei der Bestimmung von Ereignissen. Eine Unterdrückungsregel erfordert mindestens einen einfachen Filter.

So wählen Sie ein Ereignis für eine Unterdrückungsregel aus:

1. Geben Sie die erforderlichen Informationen im Assistenten für Unterdrückungsregeln ein, und fahren Sie mit dem Schritt für die Filterung fort.
2. Erstellen Sie einfache Filter, um das gewünschte Ereignis auszuwählen, indem Sie das entsprechende Kontrollkästchen aktivieren und anschließend den gewünschten Wert auswählen oder eingeben. Die folgenden Felder sind verfügbar:

   Idealmodell

   Beschreibt die umfangreiche Klasse der Technologien, die mit dem Ereignis in Zusammenhang stehen. Beispiel: Firewall oder Netzwerkgerät.

   Ereigniskategorie

   Beschreibt die Ereigniskategorien innerhalb des Idealmodells. Beispielsweise werden alle Ereignisse im Zusammenhang mit Konten, Benutzergruppen und Rollen in der Kategorie "Identitätsverwaltung" erfasst. Jede Ereigniskategorie hat mindestens eine Klasse (Teilklasse). Somit wirkt sich jede Auswahl, die Sie tätigen, auf die verfügbaren Auswahlmöglichkeiten im Menü "Ereignisklasse" aus.

Ereignisklasse

Erlaubt eine genauere Klassifizierung von Ereignissen innerhalb einer bestimmten Ereigniskategorie. Beispielsweise werden Ereignisse im Zusammenhang mit der Identitätsverwaltung in folgende drei Gruppen unterteilt: Konto, Gruppe und Identität. Jede Ereigniskategorie hat mindestens eine zugehörige Aktion. Somit wirkt sich jede Auswahl, die Sie tätigen, auf die verfügbaren Auswahlmöglichkeiten im Menü "Ereignisaktion" aus.

Ereignisaktion

Erläutert die für jede Ereigniskategorie und -klasse gängigen Aktionen. Beispielsweise umfasst die Klasse "Kontoverwaltung" der Kategorie "Identitätsverwaltung" Aktionen zur Erstellung, Löschung und Änderung von Konten.

3. Klicken Sie auf den entsprechenden Pfeil, der Sie zu dem Schritt im Assistenten führt, mit dem Sie fortfahren möchten, oder klicken Sie auf "Speichern und schließen".

   Wenn Sie auf "Speichern und schließen" klicken, wird die neue Regel in der Liste angezeigt. Andernfalls wird der von Ihnen ausgewählte Schritt angezeigt.

Eine neu erstelle Regel wird als Version 1.0 gespeichert. Wird die Regel später bearbeitet, wird eine Kopie der Regel als neue Version gespeichert. Ältere Versionen können auf Wunsch angezeigt, angewendet und kopiert werden.

Weitere Informationen:

Erstellen eines einfachen Ereignisfilters (siehe Seite 618)
Erstellen erweiterter Ereignisfilter (siehe Seite 621)
Verwenden erweiterter Filter (siehe Seite 555)

Verwenden erweiterter Filter

Mit Hilfe von erweiterten Filtern können Sie Abfragen des Ereignisprotokollspeichers im Zusammenhang mit Unterdrückung oder Zusammenfassung qualifizieren. Mit einem Formular, in das Sie, entsprechend den Anforderungen Ihrer Unterdrückungs- und Zusammenfassungsregeln, Logikspalten, Operatoren und Werte eintragen können, ermöglicht Ihnen die Schnittstelle "Erweiterte Filter", Ihre Filter in der richtigen Syntax zu erstellen.

Hinweis: Dieser Abschnitt enthält einen kurzen Überblick über die in den erweiterten Filtern für Unterdrückungs- und Zusammenfassungsregeln verwendeten Fachbegriffe. Um alle Möglichkeiten erweiterter Filter zu nutzen, sollten Sie mit den Filterbegriffen und der ELM-Schemadefinition vertraut sein.

Die folgenden Begriffe dienen zur Verknüpfung mehrerer Filteranweisungen:

And

Ereignisinformationen werden angezeigt, falls *alle* verbundenen Bedingungen zutreffen.

Or

Ereignisinformationen werden angezeigt, falls *eine* der verbundenen Bedingungen zutrifft.

Folgende SQL-Operatoren werden von erweiterten Filtern zur Erstellung der grundlegenden Bedingungen für Zusammenfassung und Unterdrückung verwendet:

Übereinstimmung

Berücksichtigt alle Ereignisinformationen, die mit einem oder mehreren der von Ihnen als alphanumerische Zeichenfolge eingegebenen Zeichen übereinstimmen, wodurch Sie nach Schlüsselwörtern suchen können. Bei dieser Suche wird die Groß-/Kleinschreibung berücksichtigt.

Übereinstimmung (Groß-/Kleinschreibung ignorieren)

Berücksichtigt alle Ereignisinformationen, die mit einem oder mehreren der von Ihnen als alphanumerische Zeichenfolge eingegebenen Zeichen übereinstimmen, wodurch Sie nach Schlüsselwörtern suchen können. Bei dieser Suche wird die Groß-/Kleinschreibung nicht berücksichtigt.

Keine Übereinstimmung

Berücksichtigt alle Ereignisinformationen, die nicht mit einem oder mehreren der Zeichen übereinstimmen, die Sie als alphanumerische Zeichenfolge eingeben. Bei dieser Suche wird die Groß-/Kleinschreibung berücksichtigt.

Keine Übereinstimmung (Groß-/Kleinschreibung ignorieren)

Berücksichtigt alle Ereignisinformationen, die nicht mit einem oder mehreren der Zeichen übereinstimmen, die Sie als alphanumerische Zeichenfolge eingeben. Bei dieser Suche wird die Groß-/Kleinschreibung nicht berücksichtigt.

Regulärer Ausdruck - Übereinstimmung

Berücksichtigt alle Ereignisinformationen, die mit einem oder mehreren der regulären Ausdruckszeichen übereinstimmen, die Sie eingeben. Hiermit kann in einer Multibyte-Umgebung sowie mit Platzhaltern gesucht werden.

Regulärer Ausdruck - keine Übereinstimmung

Berücksichtigt alle Ereignisinformationen, die nicht mit einem oder mehreren der regulären Ausdruckszeichen übereinstimmen, die Sie eingeben. Hiermit kann in einer Multibyte-Umgebung sowie mit Platzhaltern gesucht werden.

Vergleichsoperatoren

Es werden die Ereignisinformationen aufgenommen, deren Spaltenwert dem entsprechenden Vergleich mit dem von Ihnen eingegebenen Wert standhält. Die folgenden Vergleichsoperatoren stehen zur Verfügung:

- Gleich (numerisch)

- Ungleich (numerisch)
- Größer als (numerisch)
- Größer oder gleich (=>) (numerisch)
- Kleiner als (numerisch)
- Kleiner oder gleich (=>) (numerisch)

Wenn Sie beispielsweise *Größer als* verwenden, werden die Ereignisinformationen aus Ihrer gewählten Spalte übernommen, falls deren Wert größer als der von Ihnen angegebene Wert ist.

Alle diese Operatoren finden nur Zahlen; um nach anderen Zeichen zu suchen, wählen Sie einen geeigneten "Übereinstimmungs"-Operator.

Erstellen von Zusammenfassungsregeln

Mit Zusammenfassungsregeln lassen sich bestimmte native Ereignisse desselben Typs zu einem gemeinsamen Ereignis zusammenfassen. Dies spart Speicherplatz im Ereignisprotokollspeicher und vereinfacht die Analyse von Ereignissen.

Beispielsweise könnten Sie eine Zusammenfassungsregel erstellen, mit der, wenn die Anmeldung eines Benutzers drei Mal hintereinander fehlschlägt, ein einzelnes Ereignis erfasst wird. Im Ereignisprotokollspeicher würde in diesem Fall anstelle von drei Ereignissen nur eines aufgezeichnet.

Die Erstellung oder Bearbeitung einer Zusammenfassungsregel mit dem Assistenten für Zusammenfassungsregeln umfasst folgende Hauptschritte:

1. Öffnen des Assistenten für Zusammenfassungsregeln.
2. Schwellenwerte für die Zusammenfassung: Festlegen, wie viele native Ereignisse zu einem Ereignis zusammengefasst werden sollen.
3. Ereignisauswahl: Angeben der zusammenzufassenden Ereignisse. Dazu verwenden Sie die CEG-Standardisierungsattribute und wahlweise erweiterte Filter.
4. Zusammenfassung: Festlegen, wie das zusammengefasste Ereignis in den Berichten abgebildet werden soll.

Hinweis: Nachdem Sie die Zusammenfassungsregel erstellt haben, übernehmen Sie sie, damit sie in der Umgebung zur Verfügung steht.

Weitere Informationen

Öffnen des Assistenten für Zusammenfassungen (siehe Seite 558)
Festlegen von Schwellenwerten für Zusammenfassungen (siehe Seite 559)
Konfigurieren der Zusammenfassungsanzeige (siehe Seite 563)
Anwenden von Unterdrückungs- oder Zusammenfassungsregeln (siehe Seite 565)

Öffnen des Assistenten für Zusammenfassungen

Zum Erstellen einer neuen oder zum Bearbeiten einer vorhandenen Zusammenfassungsregel öffnen Sie den Assistenten für Zusammenfassungen.

So öffnen Sie den Assistenten für Zusammenfassungen:

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

   Die Ordnerliste "Protokollerfassung" wird angezeigt.

2. Erweitern Sie den Ordner "Ereignisverfeinerungs-Bibliothek" durch Klicken auf den Pfeil daneben, und wählen Sie anschließend den Ordner "Unterdrückung und Zusammenfassung" aus.

   Die Schaltflächen zur Unterdrückung und Zusammenfassung werden im Detailbereich angezeigt.

3. Klicken Sie auf "Neue Zusammenfassungsregel": 

   Der Assistent für Zusammenfassungen wird geöffnet.

   Beachten Sie bei Verwendung des Assistenten Folgendes:

   - Klicken Sie auf "Speichern", um die Regeldatei zu speichern, ohne den Assistenten zu schließen.
   - Klicken Sie auf "Speichern und schließen", um die Regeldatei zu speichern und den Assistenten zu schließen.
   - Klicken Sie auf "Zurücksetzen", um die Ansicht im Assistenten auf die zuletzt gespeicherten Einstellungen zurückzusetzen.

Weitere Informationen

Festlegen von Schwellenwerten für Zusammenfassungen (siehe Seite 559)
Konfigurieren der Zusammenfassungsanzeige (siehe Seite 563)

Festlegen von Schwellenwerten für Zusammenfassungen

Zum Erstellen oder Bearbeiten einer Zusammenfassungsregel geben Sie allgemeine Informationen ein und legen Schwellenwerte für die Zusammenfassung fest. Bei Schwellenwerten handelt es sich entweder um eine Anzahl von Ereignissen, die Häufigkeit eines Vorkommnisses oder eine Kombination beider Werte, die die Erstellung eines zusammengefassten Ereignisses auslösen.

So legen Sie Schwellenwerte für Zusammenfassungen fest:

1. Öffnen Sie den Assistenten für Zusammenfassungen.
2. Geben Sie einen Namen für die neue Regel ein. Sie können auch optional zu Referenzzwecken eine Beschreibung eingeben.

3. Definieren Sie die Kombination, indem Sie die Anzahl von nativen Ereignissen und die verstrichene Zeit festlegen, anhand derer die Regel ein einziges verfeinertes Ereignis erstellt. Verwenden Sie dazu die Optionen unter "Ereigniszusammenfassung":

   Schwellenwert für Ereignisanzahl aktivieren

   Steuert, ob von der Regel ein Ereignisschwellenwert verwendet wird. Der Ereignisschwellenwert muss größer als 1 sein. Wenn Sie dieses Feld auswählen, wird ein Wert für die maximale Anzahl von Ereignissen festgelegt. Ist dieses Feld nicht ausgewählt, jedoch ein Timeout-Zeitraum für das Ereignis aktiviert, wird beim Zusammenfassen von Ereignissen nur dieser Zeitraum berücksichtigt. Sind beide Felder aktiviert, wird nach den angegebenen Zeiträumen jeweils ein zusammengefasstes Ereignis erstellt, solange mindestens ein qualifiziertes Rohereignis auftritt.

   Maximale Anzahl an Ereignissen

   Definiert die Anzahl von nativen Ereignissen, die ein zusammengefasstes Ereignis auslösen. Wenn die von Ihnen angegebene Anzahl von nativen Ereignissen aufgetreten ist, wird ein zusammengefasstes Ereignis erstellt.

   Minimum: 2

   Maximum: 5000

   Timeout-Zeitraum für Ereignis aktivieren

   Steuert, ob von der Regel ein Schwellenwert für den Zeitraum verwendet wird. Wenn Sie dieses Feld auswählen, wird ein Wert für den Zeitraum festgelegt. Ist dieses Feld nicht ausgewählt, tritt nur dann ein zusammengefasstes Ereignis auf, wenn der Schwellenwert für die Ereignisanzahl erreicht wird.

   Zeitraum

   Definiert die Zeit in Sekunden, die verstreicht, bis ein zusammengefasstes Ereignis ausgelöst wird, falls Ereignisse des angegebenen Typs aufgetreten sind. Beim Erreichen dieses Schwellenwertes wird ein zusammengefasstes Ereignis erstellt, sofern mindestens ein qualifiziertes natives Ereignis aufgetreten ist. Sie können den Wert für den Zeitraum auf 0 einstellen. Dies führt dazu, dass nur beim Erreichen des Schwellenwertes für die maximale Anzahl von Ereignissen ein zusammengefasstes Ereignis erstellt wird.

   Minimum: 0

   Maximum: 86400

Angenommen, eine Regel fasst die Anzahl fehlgeschlagener Anmeldeversuche zusammen. Wenn Sie im Menü "Maximale Anzahl an Ereignissen" beispielsweise den Wert 3 und im Menü "Zeitraum" den Wert 10 auswählen, wird nach drei fehlgeschlagenen Anmeldeversuchen oder alle 10 Sekunden, solange mindestens eine Anmeldung fehlschlägt, ein zusammengefasstes Ereignis erstellt.

4. Klicken Sie auf den Pfeil, der Sie zu dem Schritt im Assistenten führt, mit dem Sie fortfahren möchten, oder klicken Sie auf "Speichern und schließen".

   Wenn Sie auf "Speichern und schließen" klicken, wird die neue Regel in der Liste angezeigt. Andernfalls wird der von Ihnen ausgewählte Schritt angezeigt.

Weitere Informationen

Konfigurieren der Zusammenfassungsanzeige (siehe Seite 563)

Auswählen von Ereignissen zur Zusammenfassung

Geben Sie das native Ereignis an, zu dem die Regel eine Zusammenfassung erstellen soll, indem Sie einen einfachen Filter für die Felder "CEG-Ereignisnormalisierung" einrichten. Diese vier Felder gehören der ereignisspezifischen Klasse an, werden für alle in der CEG ausgedrückten Ereignisse bereitgestellt und erlauben die genaue Angabe eines Ereignisses.

Sie können die Kombination von Ereignisnormalisierungsfeldern mithilfe der Tabelle "Einfache Filter" festlegen. Zusätzliche Filter sorgen für zusätzliche Detailangaben bei der Bestimmung von Ereignissen. Geben Sie mindestens einen einfachen Filter für eine Unterdrückungsregel an.

So wählen Sie ein Ereignis für eine Zusammenfassungsregel aus:

1. Öffnen Sie den Assistenten für Zusammenfassungsregeln, und fahren Sie mit dem Schritt zum Filtern fort.
2. Erstellen Sie einfache Filter zum Auszuwählen des gewünschten Ereignisses, indem Sie das entsprechende Kontrollkästchen markieren, und wählen Sie dann den gewünschten Wert aus oder geben Sie ihn ein. Die folgenden Felder sind verfügbar:

   Idealmodell

   Beschreibt die umfangreiche Klasse der Technologien, die mit dem Ereignis in Zusammenhang stehen. Beispiel: Firewall und Netzwerkgeräte sind Idealmodelle.

   Ereigniskategorie

   Beschreibt die Ereigniskategorien. Beispielsweise werden alle Ereignisse im Zusammenhang mit Konten, Benutzergruppen und Rollen in der Kategorie "Identitätsverwaltung" erfasst. Jede Ereigniskategorie hat mindestens eine Klasse (Teilklasse). Somit wirkt sich jede Auswahl, die Sie vornehmen, auf die verfügbaren Auswahlmöglichkeiten im Menü "Ereignisklasse" aus.

   Ereignisklasse

   Erlaubt eine genauere Klassifizierung von Ereignissen innerhalb einer bestimmten Ereigniskategorie. Beispielsweise werden Ereignisse im Zusammenhang mit der Identitätsverwaltung in folgende drei Gruppen unterteilt: Konto, Gruppe und Identität. Jede Ereigniskategorie hat mindestens eine zugehörige Aktion. Somit wirkt sich jede Auswahl, die Sie vornehmen, auf die verfügbaren Auswahlmöglichkeiten im Menü "Ereignisaktion" aus.

   Ereignisaktion

Erläutert die für jede Ereigniskategorie und -klasse gängigen Aktionen. Beispielsweise umfasst die Klasse "Kontoverwaltung" der Kategorie "Identitätsverwaltung" Aktionen zur Erstellung, Löschung und Änderung von Konten.

3. Klicken Sie auf den entsprechenden Pfeil, der Sie zu dem Schritt im Assistenten führt, mit dem Sie fortfahren möchten, oder klicken Sie auf "Speichern und schließen".

   Wenn Sie auf "Speichern und schließen" klicken, wird die neue Regel in der Liste angezeigt. Andernfalls wird der von Ihnen ausgewählte Schritt eingeblendet.

Weitere Informationen

Erstellen eines einfachen Ereignisfilters (siehe Seite 618)
Erstellen erweiterter Ereignisfilter (siehe Seite 621)
Konfigurieren der Zusammenfassungsanzeige (siehe Seite 563)
Festlegen von Schwellenwerten für Zusammenfassungen (siehe Seite 559)

Konfigurieren der Zusammenfassungsanzeige

Zusammenfassungsregeln bestimmen, wie native Ereignisse innerhalb eines verfeinerten Ereignisses angezeigt werden. Konfigurieren Sie eine Zusammenfassungsanzeige mit den Feldern "Zusammengefasst nach" und "Aggregierte Felder".

So konfigurieren Sie die Anzeige einer Zusammenfassungsregel:

1. Öffnen Sie den Assistenten für Zusammenfassungsregeln, und fahren Sie mit dem Schritt zur Zusammenfassung fort.
2. Wählen Sie mit der Wechselsteuerung das oder die Felder aus, nach denen das verfeinerte Ereignis zusammengefasst werden soll.

   Zusammengefasst nach

   Zur Steuerung des oder der Felder, nach denen die zusammengefassten Informationen angeordnet werden sollen. Bei einer Regel zur Zusammenfassung fehlgeschlagener Anmeldeversuche wählen Sie "source_username" aus, um die Anzahl der Ereignisse im Zusammenhang mit einer fehlgeschlagenen Anmeldung für die einzelnen Benutzer anzugeben. Damit die Regel vollständig ist, muss mindestens eines der Felder "Zusammengefasst nach" ausgewählt werden.

3. (Optional) Wählen Sie das Feld bzw. die Felder aus, mit denen das verfeinerte Ereignis aggregiert werden soll.

   Aggregiert

   Zur Steuerung des oder der Felder, nach denen die zusammengefassten Informationen je nach dem Feld "Zusammengefasst nach" unterteilt werden sollen. Bei einer Regel zur Zusammenfassung fehlgeschlagener Anmeldeversuche wählen Sie "source_username" als ein Feld für "Zusammengefasst nach" und "dest_hostname" als ein Feld für "Aggregiert" aus. Anschließend wird die Anzahl der Ereignisse im Zusammenhang mit einer fehlgeschlagenen Anmeldung für die einzelnen Benutzer angezeigt, und zwar sortiert nach dem Host, auf dem sich der Benutzer anmelden wollte.

   Die Daten aus den aggregierten Feldern werden in das Feld für Rohereignisse der zusammengefassten Ereignisse übernommen. Im vorherigen Beispiel wird jeder Host, auf dem sich der Benutzer anmelden wollte, zusammen mit der Anzahl der Vorkommnisse in folgendem Format gespeichert: *Hostname1:2, Hostname2:5*. Das Beispiel zeigt zwei Anmeldeversuche an Host 1 und fünf Versuche an Host 2.

   Aggregierte Felder sind keine Pflichtfelder. d. h. für die Regel muss kein aggregiertes Feld ausgewählt werden.

4. Klicken Sie auf den Pfeil, der Sie zu dem Schritt im Assistenten führt, mit dem Sie fortfahren möchten, oder klicken Sie auf "Speichern und schließen".

   Wenn Sie auf "Speichern und schließen" klicken, wird die neue Regel in der Liste angezeigt. Andernfalls wird der von Ihnen ausgewählte Schritt angezeigt.

Eine neu erstelle Regel wird als Version 1.0 gespeichert. Wird die Regel später bearbeitet, wird eine Kopie der Regel als neue Version gespeichert. Ältere Versionen können auf Wunsch angezeigt, angewendet und kopiert werden.

Weitere Informationen

Festlegen von Schwellenwerten für Zusammenfassungen (siehe Seite 559)

Anwenden von Unterdrückungs- oder Zusammenfassungsregeln

Nachdem Sie eine Unterdrückungs- oder Zusammenfassungsregel erstellt haben, müssen Sie diese anwenden, damit sie zur Verwendung in Ihrer Umgebung verfügbar wird. Mit dieser Funktion können Sie leichter verhindern, dass Unterdrückungs- oder Zusammenfassungsregeln ohne ordnungsgemäße Tests oder Genehmigung angewendet werden.

So wenden Sie eine Unterdrückungs- oder Zusammenfassungsregel an:

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

   Die Service-Liste wird angezeigt.

2. Klicken Sie auf das Symbol für den Ereignisprotokollspeicher.

   Das Konfigurationsfenster für den Ereignisprotokollspeicher wird angezeigt.

3. Suchen Sie die Unterdrückungs- oder Zusammenfassungsregel, die Sie anwenden möchten, und wählen Sie diese mit Hilfe der entsprechenden Wechselsteuerung aus.

4. Klicken Sie auf "Speichern".

   Nach erfolgreicher Anwendung der Regel wird eine Bestätigungsmeldung angezeigt.

Anwenden der Unterdrückung und Zusammenfassung auf Agentenkomponenten

Sie können Unterdrückungs- und/oder Zusammenfassungsregeln auf Agentengruppen, Agenten oder Connectors in Ihrer Umgebung anwenden. Durch diese Regeln können sämtliche Unterdrückungsregeln, die auf dem CA Enterprise Log Manager-Server angewendet wurden, ersetzt oder ergänzt werden. Hierdurch können Sie den Ereignisübertragungs- und -empfangsprozess optimieren, da Sie steuern können, an welcher Stelle die Ereignisverfeinerung stattfindet.

Wenn Sie beispielsweise mit einer Windows-Agentengruppe arbeiten, können Sie eine Unterdrückungsregel verknüpfen, die Windows-Ereignisse entfernt, welche von den Agenten der Gruppe nicht benötigt werden. Sie ignorieren beispielsweise die Windows-spezifische Überprüfung aller ankommenden Ereignisse auf dem CA Enterprise Log Manager-Server.

Sie können Unterdrückungs- und Zusammenfassungsregeln auf verschiedenen Ebenen der Ordnerhierarchie von Agenten anwenden:

- Im Agenten-Explorer-Ordner können Sie Regeln auf beliebige Agentengruppen, einzelne Agenten oder Connectors anwenden.
- In einem bestimmten Ordner einer Agentengruppe können Sie Regeln auf alle Agenten innerhalb dieser Gruppe und auf alle Connectors anwenden, die diesen zugewiesen sind.
- Bei einem einzelnen Agenten können Sie Regeln nur auf diesen Agenten und alle ihm zugewiesenen Connectors anwenden.

Der Prozess der Anwendung von Unterdrückungs- oder Zusammenfassungsregeln auf Agentenkomponenten umfasst folgende Schritte:

1. Den Assistenten für die Regelverwaltung öffnen
2. Ziele, Agentengruppen, Agenten oder Connectors auswählen
3. Anzuwendende Unterdrückungsregeln auswählen
4. Anzuwendende Zusammenfassungsregeln auswählen

Sie können Unterdrückungs- oder Zusammenfassungsregeln mit dem Assistenten für die Regelverwaltung auch aus mehreren Agentengruppen, Agenten oder Connectors entfernen.

Weitere Informationen

Öffnen des Assistenten für die Regelverwaltung (siehe Seite 566)
Auswählen von Unterdrückungs- und Zusammenfassungszielen (siehe Seite 567)
Auswählen von anzuwendenden Unterdrückungsregeln (siehe Seite 567)
Auswählen von anzuwendenden Zusammenfassungsregeln (siehe Seite 568)

Öffnen des Assistenten für die Regelverwaltung

Verwenden Sie den Assistenten für die Regelverwaltung, um Unterdrückungs- oder Zusammenfassungsregeln auf Agentengruppen oder individuelle Agenten oder Collectors anzuwenden.

So öffnen Sie den Assistenten für die Regelverwaltung:

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

   Die Ordnerliste "Protokollerfassung" wird angezeigt.

2. Klicken Sie auf den Ordner "Agenten-Explorer" und anschließend auf "Unterdrückungs- und Zusammenfassungsregeln verwalten": 

   Der Assistent für die Regelverwaltung wird geöffnet.

   Beachten Sie bei Verwendung des Assistenten Folgendes:

   - Klicken Sie auf "Speichern", um die Datei zu speichern, ohne den Assistenten zu schließen.
   - Klicken Sie auf "Speichern und schließen", um die Datei zu speichern und den Assistenten zu schließen.
   - Klicken Sie auf "Zurücksetzen", um die Ansicht im Assistenten auf die zuletzt gespeicherten Einstellungen zurückzusetzen.

Auswählen von Unterdrückungs- und Zusammenfassungszielen

Um Unterdrückungs- oder Zusammenfassungsregeln auf Agentenkomponenten anzuwenden, wählen Sie Ziele für die Regeln aus.

So wählen Sie Ziele aus:

1. Öffnen Sie den Assistenten für die Regelverwaltung.
2. Wählen Sie aus, ob Sie Regeln auf Agentengruppen, Agenten oder Connectors anwenden möchten.
3. (Optional) Wählen Sie "Löschen", wenn Sie Regeln nicht hinzufügen, sondern entfernen möchten.
4. Wählen Sie mit Hilfe der Wechselsteuerung die gewünschten Ziele aus.

   Hinweis: Sie können nach Agenten- oder Connector-Namen suchen. Falls in der Liste "Verfügbar" keine Agenten oder Connectors angezeigt werden, klicken Sie auf "Suchen", um alle verfügbaren Agenten oder Connectors anzuzeigen.
5. Fahren Sie mit dem gewünschten Schritt zur Anwendung von Regeln fort.

Auswählen von anzuwendenden Unterdrückungsregeln

Wenn Sie die Zuweisung von Unterdrückungsregeln zu einer Agentengruppe, einem Agenten oder einem Connector abschließen möchten, legen Sie fest, welche Regeln angewendet werden sollen.

So wählen Sie Unterdrückungsregeln aus:

1. Öffnen Sie den Assistenten für die Anwendung von Unterdrückungsregeln, und fahren Sie mit dem Schritt "Unterdrückungsregeln anwenden" fort.

2. Wählen Sie mit Hilfe der Wechselsteuerung aus, welche der verfügbaren Regeln angewendet werden sollen.

   Hinweis: Sie können im Feld "Muster für Unterdrückungsregeln" nach Unterdrückungsregeln suchen.

3. Klicken Sie auf "Speichern und schließen".

   Die ausgewählten Regeln werden auf die gewählten Ziele angewendet.

Auswählen von anzuwendenden Zusammenfassungsregeln

Wenn Sie die Zuweisung von Zusammenfassungsregeln zu einer Agentengruppe, einem Agenten oder einem Connector abschließen möchten, legen Sie fest, welche Regeln angewendet werden sollen.

So wählen Sie Zusammenfassungsregeln aus:

1. Öffnen Sie den Assistenten für die Verwaltung von Zusammenfassungsregeln, und fahren Sie mit dem Schritt "Zusammenfassungsregeln anwenden" fort.
2. Wählen Sie mit Hilfe der Wechselsteuerung aus, welche der verfügbaren Regeln angewendet werden sollen.

   Hinweis: Sie können im Feld "Muster für Zusammenfassungsregeln" nach Zusammenfassungsregeln suchen.

3. Wenn Sie die Anwendung von Regeln abgeschlossen haben, klicken Sie auf "Speichern" und "Schließen".
4. Die ausgewählten Regeln werden auf die gewählten Ziele angewendet. Wenn Sie im Schritt "Ziele auswählen" die Option "Löschen" gewählt haben, werden die ausgewählten Regeln gelöscht.

Kopieren von Unterdrückungs- oder Zusammenfassungsregeln

Sie können eine Unterdrückungs- oder Zusammenfassungsregel kopieren, so dass Sie basierend auf der vorhandenen Regel eine neue Regel erstellen können.

So kopieren Sie eine Unterdrückungs- oder Zusammenfassungsregel:

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

   Die Ordnerliste "Protokollerfassung" wird angezeigt.

2. Erweitern Sie den Ordner "Ereignisverfeinerungs-Bibliothek" durch Klicken auf den Pfeil daneben, und wählen Sie anschließend den Ordner "Unterdrückung und Zusammenfassung" aus.

   Die Schaltflächen zur Unterdrückung und Zusammenfassung werden im Detailbereich angezeigt.

3. Klicken Sie auf den Ordner "Unterdrückung und Zusammenfassung", der die zu kopierende Regel enthält.

   Der Ordner wird geöffnet, so dass die Regeln angezeigt werden.

4. Wählen Sie die zu kopierende Regel aus, und klicken Sie auf "Ausgewähltes Element kopieren": 

   Der Assistent für Unterdrückungen und Zusammenfassungen wird geöffnet und zeigt die Regel an.

5. Nehmen Sie die gewünschten Änderungen vor, und klicken Sie auf "Speichern und schließen".

   Die neue Regel wird in der entsprechenden Liste angezeigt.

Bearbeiten von Unterdrückungs- oder Zusammenfassungsregeln

Unterdrückungs- oder Zusammenfassungsregeln können bearbeitet werden.

So bearbeiten Sie eine Unterdrückungs- oder Zusammenfassungsregel:

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

   Die Ordnerliste "Protokollerfassung" wird angezeigt.

2. Erweitern Sie den Ordner "Ereignisverfeinerungs-Bibliothek" durch Klicken auf den Pfeil daneben, und wählen Sie anschließend den Ordner "Unterdrückung und Zusammenfassung" aus.

   Die Schaltflächen zur Unterdrückung und Zusammenfassung werden im Detailbereich angezeigt.

3. Klicken Sie auf den Ordner "Unterdrückung und Zusammenfassung", in dem sich die Regel befindet, die Sie bearbeiten möchten.

4. Wählen Sie die gewünschte Regel aus, und klicken Sie auf das Symbol zum Bearbeiten einer Zusammenfassungs- oder Unterdrückungsregel.

   Der Assistent für Unterdrückungs- oder Zusammenfassungsregeln wird aufgerufen und zeigt die ausgewählte Regel an.

5. Nehmen Sie die gewünschten Änderungen vor, und klicken Sie auf "Speichern und schließen".

   Die Regel wird in der entsprechenden Liste als eine neue Version der bearbeiteten Regel angezeigt.

Weitere Informationen

Versionen von Ereignisverfeinerungskomponenten (siehe Seite 548)

Löschen von Unterdrückungs- oder Zusammenfassungsregeln

Unterdrückungs- oder Zusammenfassungsregeln können gelöscht werden.

So löschen Sie eine Unterdrückungs- oder Zusammenfassungsregel:

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

   Die Ordnerliste "Protokollerfassung" wird angezeigt.

2. Erweitern Sie den Ordner "Ereignisverfeinerungs-Bibliothek" durch Klicken auf den Pfeil daneben, und wählen Sie anschließend den Ordner "Unterdrückung und Zusammenfassung" aus.

   Die Schaltflächen zur Unterdrückung und Zusammenfassung werden im Detailbereich angezeigt.

3. Klicken Sie auf den Ordner "Unterdrückung und Zusammenfassung", in dem sich die Regel befindet, die Sie löschen möchten.

4. Wählen Sie die gewünschte Regel aus, und klicken Sie auf das Symbol zum Löschen. Standardmäßig wird die aktuelle Version ausgewählt. Aus der Pulldown-Liste "Version" im Detailfenster können Sie eine ältere Version zum Löschen auswählen.

   Ein Bestätigungsdialogfeld wird angezeigt. Wenn Sie die Regel auf eine Integration anwenden, wird eine Warnung angezeigt. Beim Löschen der Regel wird diese auch aus der Integration gelöscht.

5. Klicken Sie auf "Ja".

   Die gelöschte Regel wird aus der entsprechenden Liste entfernt.

Importieren von Unterdrückungs- oder Zusammenfassungsregeln

Unterdrückungs- oder Zusammenfassungsregeln können von einer Umgebung in eine andere verschoben werden. Dazu müssen sie importiert werden. Beispielsweise lassen sich Regeln, die Sie in einer Testumgebung erstellt haben, in eine Live-Umgebung importieren.

So importieren Sie eine Unterdrückungs- oder Zusammenfassungsregel:

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

   Die Ordnerliste "Protokollerfassung" wird angezeigt.

2. Erweitern Sie den Ordner "Ereignisverfeinerungs-Bibliothek" durch Klicken auf den Pfeil daneben, und wählen Sie den Ordner "Unterdrückung und Zusammenfassung" aus.

   Die Schaltflächen zum Importieren und Exportieren einer Unterdrückungs- und Zusammenfassungsregel werden im Detailfenster angezeigt.

3. Klicken Sie auf "Unterdrückungs- oder Zusammenfassungsregel importieren".

   Das Dialogfeld "Datei importieren" wird angezeigt.

4. Suchen Sie die Datei, die importiert werden soll, und klicken Sie auf "OK".

   Der Assistent für Unterdrückungs- oder Zusammenfassungsregeln wird zusammen mit den Detailangaben der ausgewählten Regel angezeigt.

5. Nehmen Sie die gewünschten Änderungen vor, und klicken Sie auf "Speichern und schließen". Hat die importierte Regel einen Namen, der bereits für eine Regel in der Verwaltungsdatenbank in Verwendung ist, werden Sie aufgefordert, den Namen zu ändern.

   Die importierte Regel wird im entsprechenden Ordner angezeigt.

Exportieren von Unterdrückungs- oder Zusammenfassungsregeln

Unterdrückungs- oder Zusammenfassungsregeln können exportiert werden. So können Sie Regeln in mehreren Umgebungen verwenden. Beispielsweise lassen sich Regeln, die Sie in einer Testumgebung erstellt haben, in eine Live-Umgebung exportieren.

So exportieren Sie eine Unterdrückungs- oder Zusammenfassungsregel:

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

   Die Ordnerliste "Protokollerfassung" wird angezeigt.

2. Erweitern Sie den Ordner "Ereignisverfeinerungs-Bibliothek" durch Klicken auf den Pfeil daneben, und wählen Sie den Ordner "Unterdrückung und Zusammenfassung" aus.

   Die Schaltfläche zum Exportieren einer Unterdrückungs- oder Zusammenfassungsregel wird im Detailfenster angezeigt.

3. Klicken Sie auf den Ordner "Unterdrückung und Zusammenfassung", in dem sich die Regel befindet, die Sie exportieren möchten.

   Der Ordner wird eingeblendet, und die einzelnen Dateien werden angezeigt.

4. Wählen Sie die gewünschte Regel aus, und klicken Sie auf das Symbol zum Exportieren. Standardmäßig wird die aktuelle Version ausgewählt. Aus der Pulldown-Liste "Version" im Detailfenster können Sie eine ältere Version zum Exportieren auswählen.

   Ein Dialogfeld für den Exportspeicherort wird angezeigt.

5. Suchen oder geben Sie den Speicherort ein, an dem die exportierte Regel gespeichert werden soll, und klicken Sie auf "Speichern".

   Ein Dialogfeld über den erfolgreichen Export wird angezeigt.

6. Klicken Sie auf "OK".

   Die Regel wird exportiert.

Erstellen einer Regel zur Unterdrückung des Windows-Ereignisses 560

Wenn auf einem Windows-Server die Objektzugriffsüberwachung aktiviert wird, entsteht eine erhebliche Menge an Ereignisverkehr, von dem Sie möglicherweise einen Teil eliminieren möchten. Windows erstellt beispielsweise jedes Mal, wenn ein Administrator die Microsoft Management Console (mmc.exe) öffnet, zwei Ereignisse. Diese Ereignisse haben die ID-Werte 560 und 562.

In diesem Fall erstellen Sie eine neue Regel, mit der Windows-Ereignisse mit der Ereignis-ID 560 unterdrückt werden. Wenn Sie die Schritte im folgenden Verfahren durchführen, haben Sie eine Unterdrückungsregel, die Sie sowohl in Ihrer Netzwerkumgebung als auch zum Zeigen der Funktionsweise des Assistenten verwenden können.

Um mit diesem Beispiel zu beginnen, müssen Sie sich bei einem CA Enterprise Log Manager-Server als Benutzer mit der Administratorrolle und den Administratorberechtigungen anmelden. Wenn Sie als EiamAdmin-Benutzer angemeldet sind, können Sie keine Unterdrückungsregeln erstellen oder bearbeiten.

So erstellen Sie eine Unterdrückungsregel für das Windows-Ereignis 560:

1. Öffnen Sie den Assistenten für Unterdrückungsregeln.
2. Geben Sie in das Eingabefeld für den Namen "Unterdrückung des Windows-Ereignisses 560" ein, und fügen Sie folgende Beschreibung hinzu: "Diese Regel unterdrückt Windows-Ereignisse mit der ID 560, da das Betriebssystem für dieselbe Art des Ressourcenzugriffs auch Ereignis 562 erstellt. Zum Beleg der Richtlinientreue muss dieses Ereignis nicht aufbewahrt werden."
3. Fahren Sie mit dem Schritt "Filterung" fort, und wählen Sie die folgenden einfachen Filter aus:
   a. Idealmodellwert, Betriebssystem.
   b. Ereigniskategoriewert, Ressourcenzugriff.
   c. Ereignisklassenwert, Ressource geöffnet.
   d. Ereignisaktionswert, Ressourcenaktivität.

4. Klicken Sie auf der Registerkarte "Erweiterte Filter" auf die Schaltfläche "Neuer Ereignisfilter".

   In der Tabelle wird eine neue Filterzeile angezeigt. Sie können auf einen Wert oder auf den leeren Bereich in den einzelnen Tabellenzellen klicken, um einen Wert auszuwählen oder einen neuen Wert einzugeben.

   Das Feld für den logischen Operator enthält den Wert AND (UND). Wenn Sie mehrere unterschiedliche Arten von Ereignissen unterdrücken möchten, können Sie die jeweiligen Ereignis-IDs in neue Zeilen eingeben, für die der logische Operator OR (ODER) verwendet wird.

5. Legen Sie die Werte für den erweiterten Feldfilter fest:

   a. Klicken Sie auf den Wert im Feld "Spalte", und wählen Sie das Feld "event_id" aus.

   b. Klicken Sie auf das Feld "Operator", und wählen Sie "Gleich" aus.

   c. Klicken Sie auf das Feld "Wert", und geben Sie den Wert 560 ein.

6. Klicken Sie auf "Speichern und schließen".

   Der Assistent erstellt automatisch einen Benutzerordner, in dem Ihre Unterdrückungsregeln gespeichert werden. Sie können diesen Ordner anzeigen, indem Sie den Ordner "Unterdrückungsregeln" erweitern.

Kapitel 15: Zuordnen und analysieren

Dieses Kapitel enthält folgende Themen:

Ereignisstatus

Die Informationen über Ereignisse in Ihrer Umgebung durchlaufen eine Vielzahl an Stationen, vom erstmaligen Vorkommnis bis hin zur finalen Anzeige durch CA Enterprise Log Manager. Da sich der Begriff "Ereignis" auf jede dieser Stationen beziehen kann, verwenden Sie die folgende Terminologie für mögliche Ereignisstatus in Ihrer Umgebung:

Natives Ereignis

Bezieht sich auf das ursprüngliche Vorkommnis des Status oder der Aktion, die das Ereignis ausgelöst hat, z. B. eine fehlgeschlagene Authentifizierung oder eine Verletzung der Firewall. Native Ereignisse werden von dem entsprechenden Connector- oder Listener-Service gesendet, dann analysiert und zugeordnet (falls erforderlich), und schließlich in den Ereignisprotokollspeicher eingefügt, wo sie zur Anzeige als Rohereignisse oder verfeinerte Ereignisse verfügbar sind.

Rohereignis

Bezieht sich auf die Kommunikation, die von dem entsprechenden Überwachungsagenten gesendet wird. Rohereignisse enthalten Informationen über das native Ereignis, häufig in Form einer Syslog-Zeichenfolge oder eines Namenswertepaars. Diese Informationen werden gespeichert und sind durchsuchbar, sofern sie nicht von Unterdrückungs- oder Zusammenfassungsregeln verändert worden sind. Unterdrückte Ereignisse werden nicht im Ereignisprotokollspeicher aufgezeichnet. Ein Satz von zusammengefassten Ereignissen wird als ein einzelnes Ereignis aufgezeichnet und gibt das Resultat der Zusammenfassung aus.

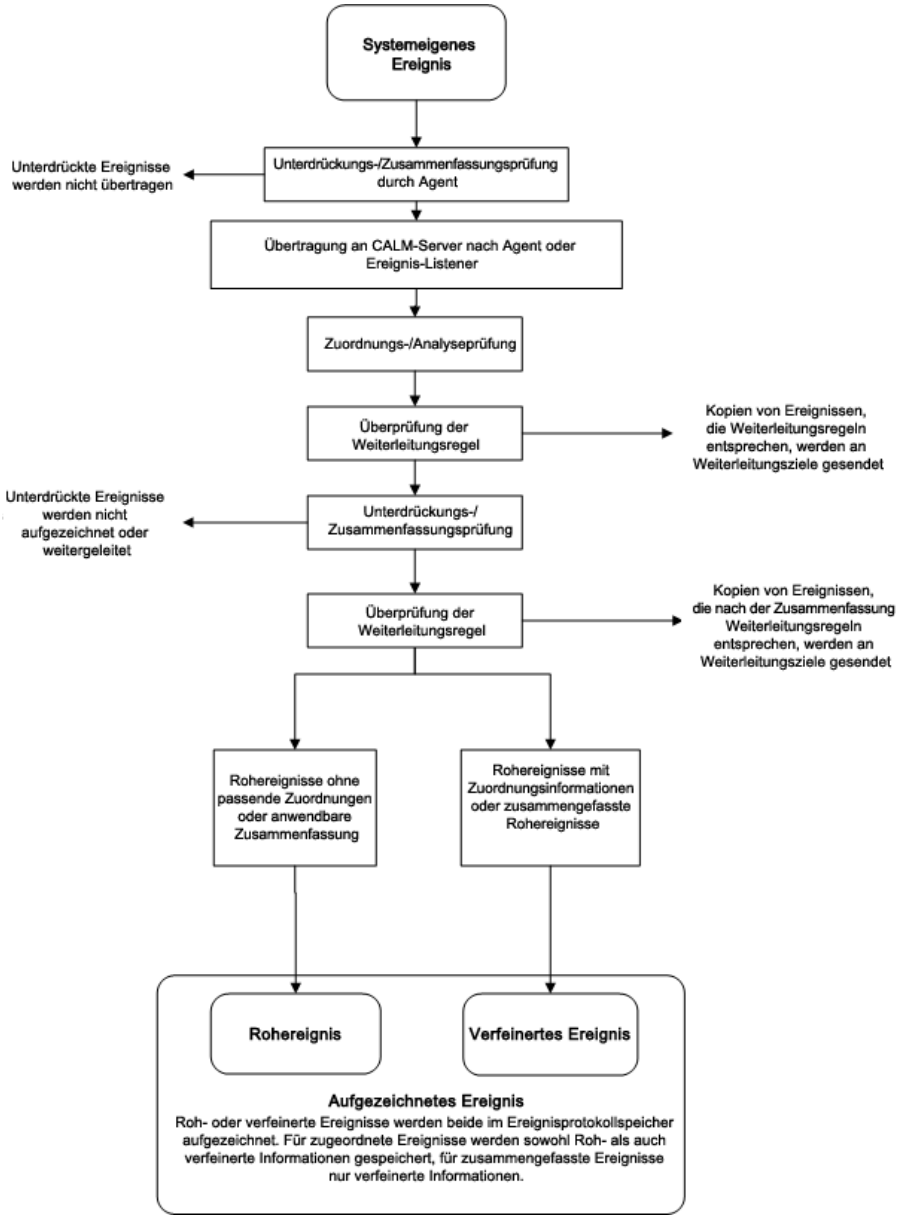
Verfeinertes Ereignis

Bezieht sich auf Ereignisinformationen wie sie von CA Enterprise Log Manager zugeordnet und zusammengefasst werden. Diese Informationen werden gespeichert und sind durchsuchbar.

Aufgezeichnetes Ereignis

Bezieht sich auf Informationen von Rohereignissen oder verfeinerten Ereignissen im Ereignisprotokollspeicher. Rohereignisse und verfeinerte Ereignisse werden immer aufgezeichnet, sofern sie nicht unterdrückt oder zusammengefasst werden. Für zugeordnete Ereignisse sind in der Regel sowohl Rohinformationen als auch verfeinerte Informationen verfügbar. Diese Informationen werden gespeichert und sind durchsuchbar.

Informationen zu den Ereignisstatus finden Sie im folgenden Diagramm:



Weitere Informationen

Aufgaben mit Unterdrückungs- und Zusammenfassungsregeln (siehe Seite 549)
Aufgaben mit Zuordnungs- und Analyseregeln (siehe Seite 580)

Aufgaben mit Zuordnungs- und Analyseregeln

Mit Hilfe von Paaren aus Dateien zum Analysieren von Nachrichten (XMP) und Zuordnen von Daten (DM) werden Daten bestimmter Typen von Ereignisquellen erfasst und standardisiert. Zur Generierung eines Ereignisses, das in einen Bericht aufgenommen und im Ereignisprotokoll erfasst werden kann, durchlaufen die meisten eingehenden nativen Ereignisse einen Analyse- und Zuordnungsprozess. Über SAPI oder iTechnology übermittelte Ereignisse müssen nicht analysiert werden, sondern werden direkt zugeordnet.

Hinweis: Damit Sie von diesen Funktionen bestmöglich profitieren, sollten Sie unbedingt mit Folgendem vertraut sein: Rohereignissen und erfassten Ereignissen in Ihrer Umgebung, Zielfeldern, die analysiert werden sollen, der Syntax für reguläre Ausdrücke, CEG, DM- und XMP-Dateien und wie diese Ereignisse analysieren.

Die XML-basierten XMP-Dateien lesen eingehende Rohereignisdaten und erstellen entsprechend Ihren Angaben Namen-Wert-Paare. Anschließend werden die durch die Nachrichtenanalyse zugewiesenen Namen-Wert-Paare mit Hilfe von DM-Dateien der ELM-Schemadefinition zugeordnet. Bei der Erstellung neuer Analyse- und Zuordnungsdateien sind diese als Teil eines Prozesses zu betrachten. Beispiel: Eine effiziente und vollständige Analyse erleichtert und beschleunigt die Zuordnung.

Weitere Informationen

Versionen von Ereignisverfeinerungskomponenten (siehe Seite 548)
Erstellen von Dateien zum Analysieren von Nachrichten (siehe Seite 580)
Erstellen von Datenzuordnungsdateien (siehe Seite 600)

Erstellen von Dateien zum Analysieren von Nachrichten

XMP-Dateien zum Analysieren von Nachrichten können mit dem Assistenten für Analysedateien erstellt werden. Analysedateien lesen die Daten eingehender Rohereignisse und erstellen Namen-Wert-Paare, mit denen Sie Zuordnungen schon vor dem Datenzuordnungsprozess erstellen können. Dies beschleunigt die Zuordnung.

Hinweis: Die Felder für die ELM-Schemadefinition (CEG) gelten nicht für die Ereignisanalyse, so dass Sie bei der Erstellung von Namen-Wert-Paaren noch flexibler sind. Die CEG-Felder können ausgewählt werden, aber die Feldnamen und Werte sind nicht auf CEG-Werte beschränkt.

Die Erstellung oder Bearbeitung einer XMP-Datei umfasst folgende Schritte:

1. Öffnen des Assistenten für Analysedateien.
2. Angeben der Dateiinformationen (Anmeldename, Protokollname und Supportinformationen).
3. Suchen von Beispielereignissen zum Testen und Erstellen von Dateien.
4. Auswählen globaler Werte, die für alle Ereignisse gelten, die von der Datei analysiert werden.
5. Erstellen oder Bearbeiten von Vorübereinstimmungs-Zeichenfolgen, um mit der Ereignisanalyse zu beginnen.
6. Auswählen von Vorübereinstimmungsfiltern für die Analyse von Filteranhängen.
7. Erstellen oder Bearbeiten von Analysefiltern, um die Ereignisanalyse abzuschließen.
8. Analysieren und Speichern der neuen oder bearbeiteten XMP-Datei.

Weitere Informationen

Angeben von Dateidetails (siehe Seite 582)
Laden von Beispielereignissen (siehe Seite 584)
Hinzufügen von globalen Feldern (siehe Seite 585)
Erstellen von Vorübereinstimmungsfiltern (siehe Seite 586)
Analysieren der XMP-Datei (siehe Seite 600)

Öffnen des Assistenten für Analysedateien

Zum Erstellen einer neuen oder zum Bearbeiten einer vorhandenen Analyseregel öffnen Sie den Assistenten für Analysedateien.

So öffnen Sie den Assistenten für Analysedateien:

1. Klicken Sie auf die Registerkarte "Verwaltung" und anschließend auf die Unterregisterkarte "Bibliothek".
2. Klicken Sie auf den Pfeil neben dem Ordner "Ereignisverfeinerungs-Bibliothek", um ihn zu öffnen. Wählen Sie anschließend den Ordner "Zuordnen und analysieren" aus.

   Die Schaltflächen zur Produktintegration werden im Fenster "Details" angezeigt.
3. Klicken Sie auf "Regel zum Analysieren neuer Nachrichten": 

   Der Assistent für Analysedateien wird geöffnet.

   Beachten Sie bei Verwendung des Assistenten Folgendes:

   - Klicken Sie auf "Speichern", um ihre Daten zu speichern, ohne den Assistenten zu schließen.
   - Klicken Sie auf "Speichern und schließen", um die Datei zu speichern und den Assistenten zu schließen.
   - Klicken Sie auf "Zurücksetzen", um die Ansicht im Assistenten auf die zuletzt gespeicherten Einstellungen zurückzusetzen.

Angeben von Dateidetails

Sie können Informationen zur Analysedatei eingeben, darunter Namen, Quelle und Verweisinformationen. Neu erstellte oder bearbeitete Dateien werden im Benutzerordner im Bereich "Zuordnen und analysieren" angezeigt.

So ergänzen Sie eine Analysedatei mit neuen Informationen:

1. Öffnen Sie den Assistenten für Analysedateien.
2. Geben Sie die Informationen wie folgt ein:
   a. Benennen Sie die Datei. Der Dateiname ist erforderlich und darf folgende Zeichen nicht enthalten: / \ : * ? “ < > ^;'`,&{}[]. oder |.
   b. Geben Sie den Quellprotokollnamen ein, um den Protokollnamen des Typs des Ereignisses zu bestimmen, das mit Hilfe der Datei analysiert werden soll. Die Funktion zum automatischen Ausfüllen schlägt während der Eingabe mögliche Protokollnamen vor. Der ausgewählte Protokollname wird im Feld "event_logname" des verfeinerten Ereignisses angegeben.
   c. Geben Sie bei Bedarf eine Beschreibung ein.
3. (Optional) Geben Sie, wie folgt, Supportinformationen ein.
   a. Klicken Sie im Supportinformationsbereich auf "Produkt hinzufügen".

      Eine neue Zeile für Supportinformationen wird eingefügt.
   b. Klicken Sie auf "Neues Produkt" oder "Neue Version", um die Eingabefelder zu aktivieren, und geben Sie die Informationen zum Produkt oder der Version ein.
4. Klicken Sie auf den Pfeil, der Sie zu dem Schritt im Assistenten führt, mit dem Sie fortfahren möchten, oder klicken Sie auf "Speichern und schließen".

   Wenn Sie auf "Speichern und Schließen" klicken, wird die neue Datei im Benutzerordner "Analysedatei" angezeigt. Andernfalls wird der ausgewählte Schritt angezeigt.

Laden von Beispielereignissen

Zur Angabe von Beispielereignissen, um die neue XMP-Datei zu testen, durchsuchen Sie den Ereignisprotokollspeicher, oder öffnen Sie eine Protokolldatei. Mit Beispielereignissen können Sie die Analysedatei während der Zusammenstellung im Assistenten testen. Zudem lässt sich mit Beispielereignissen die Analyseausgabe im letzten Schritt im Assistenten testen.

So geben Sie Beispielereignisse an:

1. Öffnen Sie den Assistenten für Analysedateien, und fahren Sie mit dem Schritt zum Laden von Ereignissen fort.

   Das Fenster zum Laden von Ereignissen wird geöffnet.

2. Aktivieren Sie im Bereich zum Suchen von Beispielereignissen das Optionsfeld "Protokollspeicher" oder "Protokolldatei".

   - Wenn Sie "Protokollspeicher" auswählen, gehen Sie wie folgt vor:

     a. Wählen Sie im Menü "Analysespalte" den Quelltyp des gewünschten Beispielereignisses aus. Für WMI-Ereignisse wählen Sie "result_string", für Syslog-Ereignisse "raw_event" aus.

     b. Wählen Sie in der Liste für Abfragekennungsfilter und Abfragen die Abfrage aus, mit der die Beispielereignisse abgerufen werden sollen.

     Die Abfrage wird angezeigt und enthält sämtliche Ereignisse, die für Analysetests im Assistenten zur Verfügung stehen.

     Hinweis: Beispielereignisse können mit einer beliebigen verfügbaren oder benutzerdefinierten Abfrage abgerufen werden. Soll eine benutzerdefinierte Abfrage verwendet werden, empfiehlt es sich, diese vor Erstellung der Analysedatei zu erstellen und zu testen. Um die Analyse zu vereinfachen, verwenden Sie eine Datei mit weniger als 1500 Ereignissen.

   - Bei Auswahl von "Protokolldatei" suchen Sie die gewünschte Datei, und klicken Sie auf "Hochladen".

     Die Ereignisse aus der Protokolldatei werden im Bereich mit den Beispielereignissen angezeigt. Testen Sie die Analysefunktion mit Hilfe der Beispiele während Sie den Assistenten ausführen.

     Hinweis: Im Assistenten wird davon ausgegangen, dass jede Zeile in der Datei einem Ereignis entspricht. Mehrzeilige Ereignisse werden nicht unterstützt.

3. Klicken Sie auf den Pfeil, der Sie zu dem Schritt im Assistenten führt, mit dem Sie fortfahren möchten.

   Wenn Sie auf "Speichern und Schließen" klicken, wird die neue Datei im Benutzerordner "Analysedatei" angezeigt. Andernfalls wird der ausgewählte Schritt angezeigt.

Hinzufügen von globalen Feldern

Sie können globale Felder, d. h. statische Paare, die mit einem Feldnamen mit einer speziellen Wert übereinstimmen, hinzufügen. Der Analyseprozess fügt die globalen Felder zu allen analysierten Ereignissen hinzu, so dass sie gut für Standardwerte, wie z. B. das Idealmodell, verwendet werden können.

So fügen Sie globale Felder hinzu:

1. Öffnen Sie den Analysedatei-Assistenten und fahren Sie mit dem Schritt "Globale Felder" fort.

   Der Bildschirm "Globale Felder" erscheint.

2. Klicken Sie im Bereich "Globale Felder" auf "Globales Feld hinzufügen".

   In der Feldertabelle erscheint ein neues globales Feld, in dem die Einträge "Neues globales Feld" und "Neuer Wert" angezeigt werden.

3. Klicken Sie auf den Text "Neues globales Feld", um die gewünschten Namensinformationen einzugeben. Beim Eingeben liefert die Funktion der Auto-Vervollständigung die verfügbaren CEG-Feldnamen. Klicken Sie zur Auswahl auf eine Option, oder geben Sie einen Nicht-CEG-Feldnamen ein.

4. Klicken Sie auf den Text "Neuer Wert", um die gewünschten Namensinformationen einzugeben.

5. (Optional) Wiederholen Sie die Schritte 2-4, um bei Bedarf zusätzliche globale Felder hinzuzufügen.

6. Klicken Sie auf den entsprechenden Pfeil, der Sie zu dem Schritt im Assistenten führt, mit dem Sie fortfahren möchten, oder klicken Sie auf "Speichern und schließen".

   Wenn Sie auf "Speichern und schließen" klicken, erscheint die neue Datei im Ordner "Analysedateibenutzer", andernfalls wird der ausgewählte Schritt angezeigt.

Erstellen von Vorübereinstimmungsfiltern

Sie können einen Vorübereinstimmungsfilter erstellen, damit die XMP-Datei die Suche auf Ereignisinformationen einschränkt, die Sie analysieren möchten. Der Vorübereinstimmungsfilter erkennt eine ausgewählte Textzeichenfolge, um die Ereignisauswahl einzuschränken, die dann von Analysefiltern durchgeführt wird. Wenn Sie sich die Analysedatei als Trichter vorstellen, stellt der Vorübereinstimmungsfilter das Einfüllstück und der Analysefilter den Hals dar.

Je umfassender der Vorübereinstimmungsfilter, umso effizienter verläuft die Analyse. Dies ist so, weil eingeschränkte Vorübereinstimmungskategorien den Verarbeitungsaufwand beim Analysieren von Ereignissen reduzieren.

Wenn Sie beispielsweise Zugriffsversuchsereignisse analysieren möchten, erstellen Sie einen Vorübereinstimmungsfilter, der nach dem Text "login" (Anmeldung) sucht, und fügen diesem Vorübereinstimmungsfilter entsprechende Analysefilter hinzu.

Hinweis: Wenn Sie einen Vorübereinstimmungsfilter löschen, werden auch die zugehörigen Analysefilter entfernt.

So erstellen Sie einen Vorübereinstimmungsfilter:

1. Öffnen Sie den Analysedatei-Assistenten und fahren Sie mit dem Schritt "Übereinstimmung und Analyse" fort.

   Der Assistent zeigt vorhandene Vorübereinstimmungsfilter in der Liste "Vorübereinstimmungsfilter" an. Jede zeigt die Anzahl der Vorübereinstimmungen für alle Beispielereignisse in Klammern daneben an.

2. Klicken Sie oben in der Liste "Vorübereinstimmungsfilter" auf "Vorübereinstimmungs-Zeichenfolge hinzufügen", oder wählen Sie einen Vorübereinstimmungsfilter zum Bearbeiten aus.

   Hinweis: Um einen Vorübereinstimmungsfilter auszuwählen, geben Sie die ersten Zeichen der Vorübereinstimmungs-Zeichenfolge in das Suchfeld ein. Es werden alle Vorübereinstimmungs-Zeichenfolgen angezeigt, die mit den eingegebenen Zeichen übereinstimmen. Innerhalb der angezeigten, übereinstimmenden Vorübereinstimmungs-Zeichenfolgen können Sie nicht die Pfeile nach oben bzw. unten verwenden, um eine Vorübereinstimmungs-Zeichenfolge zu verschieben.

3. Geben Sie den Text, den der Filter suchen soll, in das Eingabefeld "Vorübereinstimmungs-Zeichenfolge" ein.

   Beispielereignisse, die mit dem eingegebenen Text übereinstimmen, werden sofort zusammen mit der Anzahl an übereinstimmenden Ereignissen angezeigt, die gefunden und analysiert wurden.

4. (Optional) Klicken Sie auf "Vorübereinstimmung basierend auf nicht übereinstimmenden Ereignissen hinzufügen", um alle nicht übereinstimmende Beispielereignisse anzuzeigen.

   Beispielereignisse, die derzeit nicht übereinstimmen, werden im Bereich "Ereignisse" zum leichteren Verweis beim Erstellen eines neuen Vorübereinstimmungsfilters angezeigt.

5. (Optional) Fügen Sie ggf. weitere Vorübereinstimmungsfilter hinzu, oder bearbeiten Sie ggf. weitere Vorübereinstimmungsfilter.

6. Legen Sie die Reihenfolge fest, in der bei der Analyse nach Vorübereinstimmungen gesucht werden soll. Verwenden Sie hierzu die Pfeile nach oben bzw. unten neben der Liste "Vorübereinstimmungsfilter". Wenn Sie Vorübereinstimmungsfilter festlegen, die mit mehreren Ereignissen weiter oben in der Prioritätenliste übereinstimmen, wird die Analyse effizienter.

7. Klicken Sie auf den entsprechenden Pfeil, der Sie zu dem Schritt im Assistenten führt, mit dem Sie fortfahren möchten, oder klicken Sie auf "Speichern und schließen".

   Wenn Sie auf "Speichern und schließen" klicken, erscheint die neue Datei im Ordner "Analysedateibenutzer", andernfalls wird der ausgewählte Schritt angezeigt.

Erstellen von Analysefiltern

Sie können einen Analysefilter erstellen, um festzulegen, wie die XMP-Datei Ereignisdaten analysiert. Jeder Analysefilter wird an einen Vorübereinstimmungsfilter angehängt. Nachdem bei der Analyse eine Vorübereinstimmungs-Zeichenfolge gefunden wurde, wird mit allen an diese Vorübereinstimmung angehängten Analysefiltern nach den angegebenen Informationen gesucht. Die Analyse gibt die erste positive Übereinstimmung zurück.

Wenn Sie beim Schritt für die Übereinstimmung und Analyse des Assistenten für die Analyse von Nachrichten auf die Schaltfläche "Analysefilter hinzufügen" klicken, wird der Assistent für Analysedateien gestartet. Um effektive Analysefilter erstellen zu können, müssen Sie sich mit der Syntax für reguläre Ausdrücke gut auskennen.

So erstellen Sie einen Analysefilter:

1. Öffnen Sie den Assistenten für Analysedateifilter, und geben Sie auf der Seite "Filterdetails" einen Filternamen und optional eine Beschreibung ein.
2. Klicken Sie auf "Neue hinzufügen", um einen statischen Feldwert hinzuzufügen, der in allen, vom Filter analysierten Ereignissen angezeigt werden soll.

   Eine Zeile mit statischen Feldern wird angezeigt. Sie enthält die Zellen "Neues Feld" und "Neuer Wert".
3. Geben Sie in die Zelle "Neues Feld" und in die Zelle "Neuer Wert" jeweils einen Eintrag ein. Die Funktion zum automatischen Vervollständigen grenzt verfügbare CEG-Feldnamen bei der Eingabe in die Zelle "Neues Feld" ein, und zeigt ein Menü mit Auswahlmöglichkeiten an.
4. (Optional) Wiederholen Sie die Schritte 2 bis 3, um Werte für statische Felder nach Bedarf hinzuzufügen.
5. Fahren Sie mit dem Schritt "Regulärer Ausdruck" fort.

   Im Fenster "Test des Analyseausdrucks" wird der aktuelle reguläre Ausdruck angezeigt. Direkt unterhalb des regulären Ausdrucks befindet sich der Bereich "Ereignis". In diesem Bereich werden ein oder mehrere Beispielereignisse angezeigt, wenn zuvor Beispielereignisse geladen wurden. Der Assistent kann diese Ereignisse für den von Ihnen erstellten regulären Ausdruck testen.

6. Klicken Sie auf "Tokens zur Bibliothek hinzufügen oder daraus entfernen", um eine Liste mit vordefinierten regulären Ausdrücken anzuzeigen, die Sie zur Verwendung im aktuellen Filter hinzufügen können. Wählen Sie die Tokens aus, die Sie hinzufügen möchten, und klicken Sie auf "OK", um sie der Liste "Analyse-Tokens" hinzuzufügen.
7. (Optional) Klicken Sie auf "Neues Token für reguläre Ausdrücke", um ein Analyse-Token zu erstellen, und geben Sie die zugehörige Syntax für reguläre Ausdrücke in das Fenster "Token-Details" ein. Jetzt können Sie benutzerdefinierte Ausdrücke für Ihre Umgebung erstellen. Sie können Ihrer lokalen Bibliothek ein benutzerdefiniertes Token hinzufügen, indem Sie oben im Fenster "Analyse-Tokens" auf "Ausgewähltes Token zur Bibliothek hinzufügen" klicken.

   Hinweis: Wenn Sie ein neues Token für Datum/Uhrzeit erstellen, aktivieren Sie das Kontrollkästchen "Als Wert für Datum/Uhrzeit behandeln", um ein Format für die Analyse des Zeitwerts einzugeben. Dieser Wert wirkt sich nicht auf das Anzeigeformat aus.
8. Fügen Sie Anweisungen für reguläre Ausdrücke für den Filter im Eingabefeld "Regulärer Ausdruck" hinzu. Sie können Ausdrücke aus der Liste "Analyse-Tokens" ziehen und ablegen. Sie können den Ausdruck auch direkt in das Eingabefeld "Regulärer Ausdruck" eingeben oder dort bearbeiten.

   Hinweis: Wenn Sie in der Liste "Analyse-Tokens" ein Token auswählen, wird die zugehörige Syntax für reguläre Ausdrücke im Bereich "Token-Details" angezeigt. Sie können die Analyse-Token-Zuordnung in einer gegebenen Regel anzeigen, um sie in anderen Analyseregeln zu wiederholen.
9. (Optional) Aktivieren Sie das Kontrollkästchen "Dynamischer Name/Wertepaare", wenn Ihre Zielereignisse Schlüsselpaare enthalten, die Sie anzeigen möchten. Weitere Informationen finden Sie unter "Dynamische Analyse".
10. (Optional) Wenn Sie die dynamische Analyse verwenden möchten, geben Sie einen dynamischen Analyseausdruck im Eingabefeld für dynamische Paare ein. Geben Sie z. B. ein:

    ```
    (_PAIR_KEY_)=(_PAIR_VALUE_);
    ```

    Es werden alle Paare angezeigt, die durch ein Gleichheitszeichen miteinander verbunden und durch ein Semikolon voneinander getrennt sind. Sie können mehrere Ausdrücke eingeben, um Paare zu finden, die in anderen Formaten angezeigt werden. Weitere Informationen finden Sie unter "Dynamische Analyse".

11. Zeigen Sie an, wie die Datei die Beispielereignisse analysiert. Verwenden Sie hierzu die Fenster "Ereignis" und "Analysiertes Ereignis". Beim Ändern des regulären Ausdrucks eines Analysefilters werden analysierte Teile des Beispielereignisses blau und dynamisch analysierte Paare grün hervorgehoben. Sie können die Effizienz der Analyse überprüfen.
12. (Optional) Ändern Sie das Beispielereignis für weitere Tests. Verwenden Sie hierzu die Vorwärts- und Rückwärtspfeile unter dem Fenster "Ereignis", um durch die verfügbaren Beispielereignisse zu blättern.
13. Klicken Sie auf "Speichern und schließen", wenn Sie mit dem regulären Ausdruck zufrieden sind. Mit "Zurücksetzen" können Sie den regulären Ausdruck in den anfänglichen Status zurücksetzen.

    Der Assistent für Analysedateifilter wird geschlossen, und Sie kehren zum Schritt für die Übereinstimmung und Analyse des Assistenten für Analysedateien zurück.

Weitere Informationen

Dynamisches Analysieren (siehe Seite 591)
Analyse-Tokens (siehe Seite 592)
Hinzufügen eines benutzerdefinierten Tokens zur Bibliothek (siehe Seite 596)

Dynamisches Analysieren

Verwenden Sie die dynamische Analyse, um mehrere, nicht geänderte Namenswertepaare anzuzeigen. Diese Analyse unterscheidet sich von der statischen Analyse, bei der die Werte extrahiert und auf CEG oder andere vordefinierte Felder eingestellt werden. Die dynamische Analyse ist bei Anwendungen oder Formaten hilfreich, bei denen Ereignisdaten in Schlüsselpaaren aufgezeichnet werden, die unverändert angezeigt werden sollen, d. h. nicht in CEG-Namen oder anderen Werten analysiert werden. Zusätzlich wird in anwendbaren Fällen die Analyseleistung verbessert.

Der reguläre Ausdruck, der das dynamische Analysieren ermöglicht, enthält vier Elemente:

1. Einen Paarschlüssel-Indikator "(_PAIR_KEY_)"
2. Einen Paarwerte-Indikator "(_PAIR_VALUE_)"
3. Ein Schlüsselwerte-Trennzeichen zwischen dem Paar und dem Schlüsselwert
4. Ein Paartrennzeichen zwischen dem gesamten Ausdruck und dem nächsten Ausdruck.

Die von Ihnen verwendeten Trennzeichen müssen mit der Struktur der Ereignisquelle, die Sie analysieren, übereinstimmen. Wenn Ihre Ereignisquelle ein Komma als Trennzeichen verwendet, muss Ihr regulärer Ausdruck dies ebenfalls verwenden.

Beispiel

```
(_PAIR_KEY_)=(_PAIR_VALUE_);
```

In diesem Beispiel ist das Trennzeichen für den Schlüsselwert "=" und das Trennzeichen für das Paar ist ";".

Wenn Sie diesen Ausdruck nach anderen regulären Ausdrücken verwenden, kann die XMP-Datei alle Schlüsselpaare, die in den analysierten Dateien auftreten, suchen und anzeigen.

Analyse-Tokens

Ein Analyse-Token ist eine Vorlage für einen regulären Ausdruck und kann für die Erstellung von Analysefiltern verwendet werden. CA Enterprise Log Manager verfügt über eine Analyse-Token-Bibliothek, die vordefinierte Analyse-Tokens enthält. Beispielsweise wird mit dem Token _IP_ der reguläre Ausdruck festgelegt, der das standardmäßige IP-Adressformat analysiert. Wenn Sie möchten, dass ein Analysefilter eine IP-Adresse extrahiert, können Sie das Token _IP_ in den Filter einfügen, so dass Sie nicht jedes Mal den vollständigen regulären Ausdruck erstellen müssen.

Außerdem können Sie Ihre eigenen benutzerdefinierten Analyse-Tokens erstellen und sie der lokalen Bibliothek hinzufügen, oder für die Verwendung in einer anderen CA Enterprise Log Manager-Umgebung exportieren. Wenn Sie ein benutzerdefiniertes Token exportieren möchten, fügen Sie es zunächst der Bibliothek hinzu. Sie haben auch die Möglichkeit, benutzerdefinierte Tokens aus einer anderen CA Enterprise Log Manager-Umgebung zu importieren, um Analyse-Tokens in einer Testumgebung zu erstellen und anschließend in eine Live-Umgebung zu verschieben.

Weitere Informationen

Token für Datum/Uhrzeit (siehe Seite 593)
Hinzufügen eines benutzerdefinierten Tokens zur Bibliothek (siehe Seite 596)
Entfernen eines benutzerdefinierten Tokens aus der Bibliothek (siehe Seite 597)
Importieren von Analyse-Tokens (siehe Seite 598)
Exportieren von Analyse-Tokens (siehe Seite 599)

Token für Datum/Uhrzeit

CA Enterprise Log Manager unterstützt verschiedene Syntaxoptionen für Analyse-Tokens für Datum/Uhrzeit. Mit diesen Optionen können Sie im Datums-/Uhrzeitformat der Analysedatei das Erscheinungsbild des Uhrzeit- und Datumsstempels anpassen.

Alle Datums-/Uhrzeit-Tokens bestehen aus einer der folgenden Komponenten:

- Ein normales Zeichen (kein "'%" oder Leerzeichen), das wie eingegeben angezeigt wird: z. B. ein Doppelpunkt zum Trennen von Zeitwerten.

  oder

- Eine Umwandlungspezifikation. Eine Umwandlungsspezifikation besteht aus einem '%', gefolgt von einem Umwandlungszeichen, das die Anzeigeausgabe definiert: z. B. "%m" für die Anzeige des Monats.

CA Enterprise Log Manager unterstützt die folgenden Umwandlungspezifikationen:

%a oder %A

Zeigt den Namen des lokalen Wochentags in voller Länge oder abgekürzt an. Für Windows ist dies Spezifikation nur für US-Englisch verfügbar.

%b oder %B oder %h

Zeigt den Namen des lokalen Monats in voller Länge oder abgekürzt an. Für Windows ist dies Spezifikation nur für US-Englisch verfügbar.

%c

Zeigt das lokale Datum und die Uhrzeit an.

%c

Zeigt die Zahl für das Jahrhundert an (0-99).

%d oder %e

Zeigt den Tag des Monats an (1 bis 31).

%d

Zeigt das Datum im amerikanischen Format an: Monat/Tag/Jahr, entspricht der Eingabe von %m/%t/%j.

Hinweis: In Europa wird die Syntax %t/%m/%j verwendet. Das ISO 8601-Standardformat lautet %J-%m-%t.

%H

Zeigt die Uhrzeit im 24-Stunden-Format (0-23) an.

%I

Zeigt die Uhrzeit im 12-Stunden-Format (1-12) an.

%j

Zeigt den Tagesnummer des Jahres (1-366) an.

%m

Zeigt die Monatsnummer (1-12) an.

%M

Zeigt die Minute (0-59) an.

%n

Fügt ein beliebiges Leerzeichen ein.

%p

Zeigt gegebenenfalls die lokale Entsprechung für "am" oder "pm" an.

%r

Zeigt die Uhrzeit im 12-Stunden-Format an: Stunde:Minute:Sekunde am/pm – entspricht der Eingabe von %I:%M:%S %p. Wenn "t_fmt_ampm" im lokalen Abschnitt "LC_TIME" leer ist, ist das Verhalten nicht definiert.

%r

Zeigt die Uhrzeit im 24-Stunden-Format an: Stunde:Minute – entspricht der Eingabe von %H:%M.

%S

Zeigt die Sekunden an (0-60 – 60 kann für Schaltsekunden angezeigt werden).

%t

Zeigt ein beliebiges Leerzeichen an.

%T

Zeigt die Uhrzeit im 24-Stunden-Format an: Stunde:Minute:Sekunde – entspricht der Eingabe von %H:%M:%S.

%U

Zeigt die Wochennummer an. Der Sonntag ist der erste Tag der Woche (0-53). Der erste Sonntag im Januar ist der erste Tag von Woche 1.

%w

Zeigt die Wochentagnummer (0-6) an, wobei gilt: Sonntag = 0.

%W

Zeigt die Wochennummer an, wobei der Montag der erste Tag der Woche (0-53) ist. Der erste Montag im Januar ist der erste Tag von Woche 1.

%x

Zeigt das Datum im lokalen Datumsformat an.

%X

Zeigt die Uhrzeit im lokalen Zeitformat an.

%y

Zeigt das Jahr im aktuellen Jahrhundert (0-99) an. Wenn kein Jahrhundert angegeben ist, beziehen sich Werte im Bereich 69-99 auf Jahre im 20. Jahrhundert (1969-1999). Werte, die im Bereich 00-68 liegen, beziehen sich auf Jahre im 21. Jahrhundert (2000-2068).

%Y

Zeigt das Jahr einschließlich Jahrhundert an (beispielsweise 1991).

%z

Zeigt eine RFC-822/ISO 8601-Standardspezifikation für Zeitzonen an. Diese Spezifikation ist unter Windows nicht verfügbar.

Das CA Enterprise Log Manager-Standardformat für das Token für Datum/Uhrzeit ist:

%d/%b/%Y:%H:%M:%S %z

Hinzufügen eines benutzerdefinierten Tokens zur Bibliothek

Sie können benutzerdefinierte Analyse-Tokens zur Token-Bibliothek hinzufügen, so dass sie für andere Benutzer zur Verfügung stehen. Wenn Sie beispielsweise bei der Erstellung einer Nachrichtenanalysedatei ein benutzerdefiniertes Token erstellen, das auch für andere Analyseaufgaben nützlich wäre, können Sie es der Bibliothek zur erneuten Verwendung hinzufügen.

Im nachfolgenden Verfahren wird davon ausgegangen, dass Sie Tokens während der Erstellung von Analysedateien oder -filtern hinzufügen.

So fügen Sie ein benutzerdefiniertes Analyse-Token zur Bibliothek hinzu:

1. Öffnen Sie den Assistenten für die Analyse von Nachrichten, und fahren Sie mit dem Schritt "Zuordnen und analysieren" fort.
2. Öffnen Sie den Assistenten für Analysedateifilter, und fahren Sie mit dem Schritt "Regulärer Ausdruck" fort.
3. Klicken Sie auf "Neuer regulärer Ausdruck", um ein Analyse-Token zu erstellen, und geben Sie die zugehörige Syntax für reguläre Ausdrücke in das Fenster "Token-Details" ein.
4. Wählen Sie das neue Analyse-Token aus, und klicken Sie auf "Ausgewähltes Token zur Bibliothek hinzufügen".

   Ein Bestätigungsdialogfeld wird angezeigt.
5. Klicken Sie auf "Ja".
6. (Optional) Klicken Sie auf "Tokens zur Bibliothek hinzufügen oder daraus entfernen", um das neue Token anzuzeigen.

   Das Dialogfeld mit der Analyse-Token-Bibliothek wird angezeigt. Benutzerdefinierte Tokens werden darin schwarz und vordefinierte Tokens grün angezeigt.

Entfernen eines benutzerdefinierten Tokens aus der Bibliothek

Sie können nicht benötigte oder veraltete benutzerdefinierte Tokens aus der Token-Bibliothek entfernen. Vordefinierte Tokens lassen sich nicht entfernen.

So entfernen Sie benutzerdefinierte Tokens aus der Bibliothek:

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

   Die Ordnerliste "Protokollerfassung" wird angezeigt.

2. Klicken Sie auf den Pfeil neben dem Ordner "Ereignisverfeinerungs-Bibliothek", um ihn zu öffnen. Wählen Sie anschließend den Ordner "Zuordnen und analysieren" aus.

   Die Schaltflächen zur Produktintegration werden im Fenster "Details" angezeigt.

3. Klicken Sie auf "Regel zum Analysieren neuer Nachrichten": 

   Der Assistent für Analysedateien wird geöffnet.

4. Fahren Sie mit dem Schritt "Zuordnen und analysieren" fort.

5. Wählen Sie einen Vorübereinstimmungsfilter aus, und klicken Sie auf "Bearbeiten", oder klicken Sie oben in der Analysefilterliste auf "Analysefilter hinzufügen".

   Der Assistent für Analysedateifilter wird geöffnet.

6. Fahren Sie mit dem Schritt "Regulärer Ausdruck" fort.

7. Klicken Sie auf "Tokens zur Bibliothek hinzufügen oder daraus entfernen".

   Das Dialogfeld mit der Analyse-Token-Bibliothek wird angezeigt. Benutzerdefinierte Tokens werden darin schwarz und vordefinierte Tokens grün angezeigt.

8. Wählen Sie das benutzerdefinierte Token beziehungsweise die benutzerdefinierten Tokens aus, die entfernt werden sollen, und klicken Sie auf "Ausgewähltes Token aus Bibliothek entfernen".

   Ein Bestätigungsdialogfeld wird angezeigt.

9. Klicken Sie auf "Ja" und anschließend auf "OK".

Importieren von Analyse-Tokens

Sie können Analyse-Tokens importieren, um auf einem anderen Managementserver erstellte benutzerdefinierte Analyse-Tokens Ihrem aktuellen Server hinzuzufügen, d. h. die Tokens zum Beispiel von einer Testumgebung auf Ihre Live-Umgebung zu übertragen.

So importieren Sie Analyse-Tokens:

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

   Die Ordnerliste "Protokollerfassung" wird angezeigt.

2. Klicken Sie auf den Pfeil neben dem Ordner "Ereignisverfeinerungs-Bibliothek", um ihn zu öffnen. Wählen Sie anschließend den Ordner "Zuordnen und analysieren" aus.

   Die Schaltflächen zur Produktintegration werden im Fenster "Details" angezeigt.

3. Klicken Sie auf "Regel zum Analysieren neuer Nachrichten": 

   Der Assistent für Analysedateien wird geöffnet.

4. Fahren Sie mit dem Schritt "Zuordnen und analysieren" fort.

5. Wählen Sie einen Vorübereinstimmungsfilter aus, und klicken Sie auf "Bearbeiten", oder klicken Sie oben in der Analysefilterliste auf "Analysefilter hinzufügen".

   Der Assistent für Analysedateifilter wird geöffnet.

6. Fahren Sie mit dem Schritt "Regulärer Ausdruck" fort.

7. Klicken Sie oben im Fenster "Analyse-Tokens" auf "Benutzer-Tokens importieren".

   Das Dialogfeld "Datei importieren" wird angezeigt.

8. Suchen Sie die Token-Datei (.tok), die importiert werden soll, und klicken Sie auf "OK".

   Ein Bestätigungsdialogfeld wird angezeigt.

9. Klicken Sie auf "Ja", um die Datei zu importieren, so dass alle anderen Benutzer-Tokens in der Bibliothek überschrieben werden.

Exportieren von Analyse-Tokens

Sie können Analyse-Tokens exportieren, die Sie der Token-Bibliothek hinzugefügt haben, um auf dem aktuellen Managementserver erstellte benutzerdefinierte Analyse-Tokens auf einen anderen Server zu verschieben. Beispielsweise könnten Sie Ihre benutzerdefinierten Tokens aus einer Testumgebung in Ihre Live-Umgebung verschieben.

So exportieren Sie Analyse-Tokens:

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

   Die Ordnerliste "Protokollerfassung" wird angezeigt.

2. Klicken Sie auf den Pfeil neben dem Ordner "Ereignisverfeinerungs-Bibliothek", um ihn zu öffnen. Wählen Sie anschließend den Ordner "Zuordnen und analysieren" aus.

   Die Schaltflächen zur Produktintegration werden im Fenster "Details" angezeigt.

3. Klicken Sie auf "Regel zum Analysieren neuer Nachrichten": 

   Der Assistent für Analysedateien wird geöffnet.

4. Fahren Sie mit dem Schritt "Zuordnen und analysieren" fort.

5. Wählen Sie einen Vorübereinstimmungsfilter aus, und klicken Sie auf "Bearbeiten", oder klicken Sie oben in der Analysefilterliste auf "Analysefilter hinzufügen".

   Der Assistent für Analysedateifilter wird geöffnet.

6. Fahren Sie mit dem Schritt "Regulärer Ausdruck" fort.

7. Klicken Sie oben im Fenster "Analyse-Tokens" auf "Benutzer-Tokens exportieren".

   Ein Dialogfeld für den Speicherort wird eingeblendet.

8. Wählen Sie den gewünschten Speicherort für die exportierte Datei aus, und klicken Sie auf "Speichern".

   Die exportierte Datei wird an dem von Ihnen ausgewählten Speicherort gespeichert.

Analysieren der XMP-Datei

Neue oder bearbeitete Dateien können mit dem Hilfsprogramm für die Analyse von Nachrichten analysiert werden. So lässt sich feststellen, wie effizient die Analysedatei ist. Anhand von Analysen können Sie die Funktion der Datei vor dem Speichern testen und die Datei entsprechend ändern.

Mit dem Hilfsprogramm wird eine XMP-Datei unter Verwendung der ausgewählten Beispielereignisse getestet. Dazu gehen Sie wie folgt vor:

1. Suchen Sie die Ereignisse, welche die in der XMP-Datei definierten Vorübereinstimmungs-Zeichenfolgen enthalten. Das Hilfsprogramm sucht nach den einzelnen Vorübereinstimmungs-Zeichenfolgen, um alle Ereignisse, die diese enthalten, zu finden.
2. Suchen Sie für jedes der Vorübereinstimmungs-Ereignisse nach dem ersten Analysefilter, mit dem das Ereignis in Token analysiert werden kann.

So analysieren Sie die XMP-Datei:

Öffnen Sie den Analyseassistenten, und fahren Sie mit dem Schritt zum Analysieren fort. Die Anzahl der Übereinstimmungen mit den Vorübereinstimmungs-Zeichenfolgen und -filtern wird angezeigt. Je mehr Übereinstimmungen es gibt, desto besser funktioniert die neue oder bearbeitete XMP-Datei. Zudem können Sie so herausfinden, ob es wichtige Informationen gibt, die nicht analysiert werden.

Bei einer großen XMP-Datei und vielen Beispielereignissen kann die Analyse etwas dauern. In der Regel nimmt sie aber nicht mehr als eine Minute in Anspruch. Wenn die Analyse zu lange dauert, brechen Sie den Vorgang ab, und analysieren Sie anschließend eine geringere Anzahl von Ereignissen.

Eine neu erstelle Regel wird als Version 1.0 gespeichert. Wird die Regel später bearbeitet, wird eine Kopie der Regel als neue Version gespeichert. Ältere Versionen können auf Wunsch angezeigt, angewendet und kopiert werden.

Erstellen von Datenzuordnungsdateien

Erstellen und bearbeiten Sie Datenzuordnungsdateien im Assistenten für Zuordnungsdateien. Datenzuordnungsdateien wandeln native Ereignisse in verfeinerte Ereignisse um, indem die analysierten Textzeichenfolgen oder Feld-Wert-Paare CEG-kompatiblen Feldern zugeordnet werden. Dazu können Sie mit dem Assistenten verschiedene Zuordnungstypen definieren und bearbeiten.

Die Erstellung oder Bearbeitung einer DM-Datei umfasst folgende Schritte:

1. Öffnen des Assistenten für Zuordnungsdateien.
2. Angeben von Dateidetails.
3. Suchen und Hinzufügen von Beispielereignissen mit Hilfe von Analysedateien.
4. Festlegen direkter Zuordnungen nach Bedarf.
5. Festlegen von Funktionszuordnungen nach Bedarf.
6. Festlegen bedingter Zuordnungen nach Bedarf.
7. Festlegen von Blockzuordnungen nach Bedarf.

   Hinweis: Direkte Zuordnungen oder Funktionszuordnungen können mit Hilfe von Blockzuordnungen festgelegt werden. Sie sind eine Alternative zur Festlegung von Zuordnungen mit Schritt 4 und 5.
8. Analysieren und Speichern der fertigen DM-Datei

Beachten Sie beim Erstellen einer DM-Datei die Priorität der Datenzuordnung sowie die Zuordnungstypen der Datei. Die Ereignisinformationen werden von der fertigen DM-Datei in der Reihenfolge der Fenster für den Zuordnungstyp (Schritt 4 bis 7 im Assistenten) überprüft. Bei doppelt vorhandenen Zuordnungstypen wird der zuletzt von der DM-Datei gefundene Wert zugewiesen.

Beispiel: Findet eine DM-Datei für ein bestimmtes natives Ereignis eine direkte Zuordnung und danach eine bedingte Zuordnung für den gleichen Ereigniswert, wird die bedingte Zuordnung für das verfeinerte Ereignis verwendet.

Doppelte Zuordnungen *innerhalb* eines bestimmten Zuordnungstyps werden je nach Typ unterschiedlich gehandhabt:

- Direkte Zuordnungen und Funktionszuordnungen: Die DM-Datei verwendet den zuletzt gefundenen Übereinstimmungswert. Bei einer doppelten Funktionszuordnung wird die zuletzt gefundene Funktion aufgerufen. Sie könnten beispielsweise eine doppelte Zuordnung festlegen, um eine zweite Funktion aufzurufen, wenn die erste nicht gefunden wird oder nicht wie erwartet funktioniert.
- Bedingte Zuordnungen und Blockzuordnungen: Die DM-Datei wendet den zuerst gefundenen Wert an, und die Suche wird beendet. Um die Leistung zu verbessern, platzieren Sie am Anfang der Datei gemeinsame Bedingungen für beide dieser Zuordnungstypen.

Weitere Informationen über die Auswirkungen der Zuordnungsreihenfolge erhalten Sie in den Abschnitten zu den einzelnen Zuordnungstypen.

Weitere Informationen

Festlegen von Blockzuordnungen (siehe Seite 613)
Durchführen von Zuordnungsanalysen (siehe Seite 615)

Öffnen des Assistenten für Zuordnungsdateien

Zum Erstellen einer neuen oder zum Bearbeiten einer vorhandenen Datenzuordnungsdatei öffnen Sie den Assistenten für Zuordnungsdateien.

So öffnen Sie den Assistenten für Zuordnungsdateien:

1. Klicken Sie auf die Registerkarte "Verwaltung" und anschließend auf die Unterregisterkarte "Bibliothek".
2. Klicken Sie auf den Pfeil neben dem Ordner "Ereignisverfeinerungs-Bibliothek", um ihn zu öffnen. Wählen Sie anschließend den Ordner "Zuordnen und analysieren" aus.

   Die Schaltflächen zur Produktintegration werden im Fenster "Details" angezeigt.
3. Klicken Sie auf "Neue Zuordnungsdatei": 

   Der Assistent für Zuordnungsdateien wird angezeigt.

   Beachten Sie bei Verwendung des Assistenten Folgendes:

   - Klicken Sie auf "Speichern", um die Datei zu speichern, ohne den Assistenten zu schließen.
   - Klicken Sie auf "Speichern und schließen", um die Datei zu speichern und den Assistenten zu schließen.
   - Klicken Sie auf "Zurücksetzen", um die Ansicht im Assistenten auf die zuletzt gespeicherten Einstellungen zurückzusetzen.

Weitere Informationen

Festlegen der Verkettungsfunktionszuordnung (siehe Seite 610)
Festlegen von Blockzuordnungen (siehe Seite 613)
Durchführen von Zuordnungsanalysen (siehe Seite 615)

Angaben von Dateidetails

Geben Sie die Details für die neue DM-Datei an. Abonnementdateien können als benutzerdefinierte Dateien unter einem anderen Namen gespeichert werden.

So geben Sie die Details der Zuordnungsdatei an:

1. Öffnen Sie den Assistenten für Zuordnungsdateien.
2. Benennen Sie die DM-Datei. Der Dateiname ist erforderlich und darf folgende Zeichen nicht enthalten: / \ : * ? “ < > ^;'`,&{}[]. oder |.
3. Wählen Sie aus der Dropdown-Liste "Analysedatei" den Namen und die Version der Analysedatei aus, die Sie für de Analyse der Beispielereignisse verwenden möchten.

   Das Feld "Protokollname" wird automatisch mit dem Namen der eingegebenen Analysedatei ausgefüllt.
4. (Optional) Geben Sie eine Beschreibung ein.
5. (Optional) Klicken Sie im Bereich "Supportinformationen" auf "Produkt hinzufügen", um zu Referenzzwecken Produktnamen und -versionen einzugeben.
6. Klicken Sie auf den entsprechenden Pfeil, der Sie zu dem Schritt im Assistenten führt, mit dem Sie fortfahren möchten, oder klicken Sie auf "Speichern und schließen".

   Wenn Sie auf "Speichern und schließen" klicken, erscheint die neue Datei im Ordner "Zuordnungsdateibenutzer", andernfalls wird der ausgewählte Schritt angezeigt.

Bereitstellen von Beispielereignissen

Suchen Sie mit dem Assistenten für Zuordnungsdateien nach Beispielereignissen, um die DM-Datei zu testen. Durchsuchen Sie den Ereignisprotokollspeicher, oder entnehmen Sie die Beispiele direkt aus einer Protokolldatei. Beispielereignisse dienen als Vorlage, um die Analyseausgabe im letzten Schritt im Assistenten testen.

So geben Sie Beispielereignisse an:

1. Öffnen Sie den Assistenten für Zuordnungsdateien, und fahren Sie mit dem Schritt zum Laden von Beispielereignissen fort.

   Das Fenster für Beispielereignisse wird geöffnet.

2. Aktivieren Sie im Bereich zum Suchen von Beispielereignissen die Optionsschaltfläche "Protokollspeicher" oder "Protokolldatei".
3. Wenn Sie "Protokollspeicher" auswählen, gehen Sie wie folgt vor:
   a. Wählen Sie im Menü "Analysespalte" den Quelltyp des gewünschten Beispielereignisses aus. Für WMI-Ereignisquellen wählen Sie "result_string", für Syslog-Ereignisquellen "raw_event" aus.
   b. Wählen Sie in der Liste für Abfragekennungsfilter und Abfragen die Abfrage aus, mit der die Beispielereignisse abgerufen werden sollen.

      Die Abfrage wird mit den Beispielereignissen angezeigt.

      Hinweis: Beispielereignisse können mit einer beliebigen verfügbaren oder benutzerdefinierten Abfrage abgerufen werden. Soll eine benutzerdefinierte Abfrage verwendet werden, empfiehlt es sich, diese vor Erstellung der Datenzuordnungsdatei zu erstellen und zu testen.
4. Wenn Sie "Protokolldatei" auswählen, gehen Sie wie folgt vor:
   a. Suchen Sie die gewünschte Protokolldatei, und klicken Sie auf "Hochladen".

      Die Ereignisse aus der Protokolldatei werden im Bereich mit den Beispielereignissen angezeigt.

      Hinweis: Im Assistenten wird davon ausgegangen, dass jede Zeile in der Datei einem Ereignis entspricht. Mehrzeilige Ereignisse werden nicht unterstützt.
   b. Klicken Sie auf "Dynamische Felder extrahieren", wenn Ihre Beispielprotokolldatei dynamische Paarwerte enthält, die Sie im analysierten Beispiel berücksichtigen möchten.
5. Klicken Sie auf den entsprechenden Pfeil, der Sie zu dem Schritt im Assistenten führt, mit dem Sie fortfahren möchten, oder klicken Sie auf "Speichern und schließen".

   Wenn Sie auf "Speichern und schließen" klicken, erscheint die neue Datei im Ordner "Zuordnungsdateibenutzer", andernfalls wird der ausgewählte Schritt angezeigt.

Weitere Informationen

Dynamisches Analysieren (siehe Seite 591)

Festlegen direkter Zuordnungen

Mit direkten Zuordnungen wird eine Eins-zu-Eins-Übereinstimmung zwischen dem Wert eines nativen Ereignisses und dem eines verfeinerten Ereignisses festgelegt. Daher bieten sich direkte Zuordnungen nur für Standardwerte oder gemeinsame Werte an, die selten geändert werden. Ein Beispiel ist das Feld "ideal_model".

Mit Hilfe von Zuordnungen lassen sich verfeinerte Ereigniswerte wie folgt abrufen:

Textwert

Entspricht dem Text in einem bestimmten CEG-Feld. Der Wert wird immer dann angezeigt, wenn ein entsprechendes Ereignis zugeordnet wird. Beispiel: Wird das CEG-Feld "ideal_model" auf "Firewall" gesetzt, wird für alle Regeln, die diese Zuordnung enthalten, der Wert "Firewall" angezeigt.

Feldwert

Der Wert im Feld eines Rohereignisses, dessen Inhalt Teil eines bestimmten CEG-Feldes oder analysierten Feldes ist. Feldwerte unterscheiden sich von Textwerten dadurch, dass vor dem Wert ein Dollarzeichen ($) steht. Wird beispielsweise das CEG-Feld "event_logname" auf "$Log" gesetzt, wird bei jeder Ereigniszuordnung genau der Text angezeigt, der im Protokollfeld des nativen Ereignisses steht.

So legen Sie direkte Zuordnungen fest:

1. Öffnen Sie den Assistenten für Zuordnungsdateien, geben Sie für die Zuordnungsdatei einen Namen ein, und wählen Sie einen Protokollnamen aus. Fahren Sie dann mit dem Schritt für direkte Zuordnungen fort.

   Das Fenster "Direkte Zuordnungen" wird mit den aktuellen Zuordnungen oder den Standardzuordnungen aufgerufen. In der Spalte "Name" steht der Name des CEG-Feldes oder des analysierten Feldes. Die Spalte "Wert" enthält entweder einen Text- oder einen Feldwert.

   Hinweis: Wählen Sie im Schritt zur Bereitstellung von Beispielereignissen eine Analysedatei aus, damit analysierte Feldwerte angezeigt werden.

2. Um am Ende der Tabelle eine neue Zuordnung einzufügen, klicken Sie auf "Direkte Zuordnung hinzufügen". Wählen Sie diese danach aus, oder bearbeiten Sie eine bestehende direkte Zuordnung.

   Die direkten Zuordnungen des Feldes (wenn vorhanden) werden unter den Zuordnungsdetails angezeigt.

3. Wählen Sie im Dropdown-Menü "Feld" ein CEG-Feld oder, wenn vorhanden, ein analysiertes Ereignisfeld für die Zuordnung aus. Wenn Sie mit der Eingabe beginnen, wird die Liste der verfügbaren CEG-Felder von der Funktion zum automatischen Ausfüllen weiter eingeschränkt.
4. Geben Sie im Feld "Wert hinzufügen" einen neuen Wert ein, und klicken Sie daneben auf "Direkte Zuordnung hinzufügen". Zur Kennzeichnung von Feldwerten setzen Sie ein Dollarzeichen ($) vor den Wert.

   Der Wert wird im Bereich "Ausgewählte Felder" angezeigt.
5. (Optional) Sie können mehrere direkte Zuordnungen für ein Feld eingeben und die Reihenfolge, in der diese in der Datenzuordnungsdatei berücksichtigt werden, mit Hilfe der Pfeilschaltflächen festlegen. Die von der DM-Datei zuletzt gefundene direkte Zuordnung wird im verfeinerten Ereignis ausgegeben.

   Hinweis: Je mehr Werte Sie hinzufügen, desto schlechter funktioniert die Zuordnung. Daher sollte dies nur in Ausnahmefällen erfolgen.
6. (Optional) Über die Wechselsteuerung können Sie nicht benötigte Werte in den Bereich "Verfügbare Felder" verschieben. So können Sie verhindern, dass sie bei der aktuellen Zuordnung berücksichtigt werden.
7. Nachdem Sie alle direkten Zuordnungen hinzugefügt haben, klicken Sie auf den Pfeil, der Sie zu dem Schritt im Assistenten führt, mit dem Sie fortfahren möchten, oder klicken Sie auf "Speichern und schließen".

Wenn Sie auf "Speichern und schließen" klicken, erscheint die neue Datei im Ordner "Zuordnungsdateibenutzer", andernfalls wird der ausgewählte Schritt angezeigt.

Festlegen von Funktionszuordnungen

Mit Funktionszuordnungen wird ein CEG-Feld mit einem Wert verknüpft. Dabei werden die Daten des verfeinerten Ereignisses mit Hilfe einer Funktion abgerufen oder ermittelt. Funktionszuordnungen bestehen aus dem Namen eines CEG-Feldes, einem vordefinierten Wert bzw. einem Klassenfeldwert und der Funktion.

In einer Funktionszuordnung können beispielsweise mehrere native Ereigniswerte über die Verkettungsfunktion mit einem einzelnen CEG-Feld verbunden sein.

Bei doppelten Funktionszuordnungen wird die von der DM-Datei zuletzt gefundene Zuordnung berücksichtigt. Sie könnten beispielsweise eine doppelte Zuordnung festlegen, um eine zweite Funktion aufzurufen, wenn die erste nicht gefunden wird oder nicht wie erwartet funktioniert.

So legen Sie Funktionszuordnungen fest:

1. Öffnen Sie den Assistenten für Zuordnungsdateien, geben Sie für die Zuordnungsdatei einen Namen ein, und wählen Sie einen Protokollnamen aus. Fahren Sie dann mit dem Schritt für Funktionszuordnungen fort.

   Im Fenster "Funktionszuordnungen" werden aktuelle Zuordnungen oder Standardzuordnungen angezeigt. In der Spalte "Name" steht der Name des CEG-Feldes oder des analysierten Feldes, in der Spalte "Funktion" die aktuelle Verknüpfungsfunktion und in der Spalte "Wert" ein Text- oder Feldwert.

   Hinweis: Wählen Sie im Schritt zur Angabe von Dateidetails eine Analysedatei aus, damit analysierte Feldwerte angezeigt werden.

2. Um eine neue Funktionszuordnung hinzuzufügen, klicken Sie auf "Funktionszuordnung hinzufügen", oder wählen Sie eine vorhandene Zuordnung zum Bearbeiten aus.

   Der Zuordnungseintrag wird im Fenster "Zuordnungsdetails" angezeigt.

3. Wählen Sie im Dropdown-Menü "Feld" ein CEG-Feld aus, das zugeordnet werden soll. Wenn Sie mit der Eingabe beginnen, wird die Liste der verfügbaren CEG-Felder von der Funktion zum automatischen Ausfüllen weiter eingeschränkt.

4. Wählen Sie im Dropdown-Menü "Funktion" eine Funktion für die Zuordnung aus.

   Hinweis: Im Gegensatz zu anderen Funktionen werden für die Verkettungsfunktion mehrere Zielwerte angegeben. Ausführliche Informationen finden Sie im Abschnitt zum Festlegen von Verkettungsfunktionszuordnungen.

5. Geben Sie im Feld "Wert hinzufügen" einen Zielwert für die Zuordnung ein, und klicken Sie daneben auf die Schaltfläche "Wert hinzufügen". Zur Kennzeichnung von Feldwerten setzen Sie ein Dollarzeichen ($) vor den Wert.

   Der Wert wird im Bereich "Ausgewählte Felder" angezeigt.

6. (Optional) Sie können mehrere Zuordnungen für ein Feld eingeben und die Reihenfolge, in der diese in der DM-Datei berücksichtigt werden, mit Hilfe der Pfeilschaltflächen festlegen.

   Hinweis: Je mehr Werte Sie hinzufügen, desto schlechter funktioniert die Zuordnung. Verwenden Sie eigenständige Funktionszuordnungen daher nur in Ausnahmefällen.

7. (Optional) Verschieben Sie nicht mehr benötigte Werte mit Hilfe der Wechselsteuerung in den Bereich der verfügbaren Felder, damit sie bei der aktuellen Zuordnung nicht berücksichtigt werden.

8. Nachdem Sie alle Funktionszuordnungen hinzugefügt haben, klicken Sie auf den Pfeil, der Sie zu dem Schritt im Assistenten führt, mit dem Sie fortfahren möchten, oder klicken Sie auf "Speichern und schließen".

   Wenn Sie auf "Speichern und schließen" klicken, erscheint die neue Datei im Ordner "Zuordnungsdateibenutzer", andernfalls wird der ausgewählte Schritt angezeigt.

Festlegen der Verkettungsfunktionszuordnung

Eine Verkettungsfunktionszuordnung ist eine Funktionszuordnungsart. Im Gegensatz zu anderen Funktionszuordnungen, die ein Zielfeld oder einen Zielwert angeben, gibt die Verkettungsfunktionszuordnung mehrere Zuordnungsziele an, die zu einem CEG-Feld verkettet werden.

Mit Hilfe des Assistenten zum Zuordnen von Daten können Sie Verkettungsfunktionszuordnungen erstellen. Da sich Verkettungszuordnungen von anderen Funktionszuordnungen unterscheiden, werden die Verkettungszuordnungen auch etwas anders erstellt.

So legen Sie die Verkettungsfunktionszuordnung fest:

1. Öffnen Sie den Assistenten für Zuordnungsdateien, geben Sie für die Zuordnungsdatei einen Namen ein, und wählen Sie einen Protokollnamen aus. Fahren Sie dann mit dem Schritt für Funktionszuordnungen fort.

   Im Fenster "Funktionszuordnungen" werden aktuelle Zuordnungen oder Standardzuordnungen angezeigt. In der Spalte "Name" wird ein CEG-Feld, in der Spalte "Funktion" die aktuelle Verknüpfungsfunktion und im Feld "Wert" ein Text- oder Feldwert angezeigt.

2. Klicken Sie auf "Funktionszuordnung hinzufügen", um einen neuen Zuordnungseintrag hinzuzufügen.

   Der Zuordnungseintrag wird im Fenster "Zuordnungsdetails" angezeigt.

3. Wählen Sie im Dropdown-Menü "Feld" ein CEG-Feld aus, das zugeordnet werden soll.

4. Wählen Sie im Dropdown-Menü "Funktion" die Verkettungsfunktion aus.

   Die Felder "Format" und "Wert" werden angezeigt.

   Hinweis: Der Wert der Verkettungsfunktion wird im Fenster "Funktionszuordnungen" als {...} angezeigt. Das bedeutet, dass anstelle nur eines Werts eine Gruppe von Werten vorhanden ist.

5. (Optional) Geben Sie im Feld "Format" einen Bezeichner ein, um die Platzierung der Zielfelder zu bestimmen. Der Formatbezeichner "%s" gibt eine Feldposition an. Alles andere außer "%s" wird als statische Unterstützungsdaten betrachtet, die in das letzte Tabellensammlungsfeld eingefügt werden sollen. Um beispielsweise zwei Zielfelder mit einem Doppelpunkt voneinander zu trennen, geben Sie im Feld "Format" Folgendes ein: "%s:%s".

6. Klicken Sie im Bereich "Verkettete Werte" auf "Verketteten Wert hinzufügen", um ein Zieleingabe-Zielwert-Paar hinzuzufügen.

7. Geben Sie im Eingabefeld "Wert hinzufügen" einen Wert ein, und klicken Sie auf "Wert hinzufügen".

   Der Wert wird im Bereich "Ausgewählte Felder" angezeigt.

8. Wiederholen Sie die Schritte 6 und 7, um weitere zu verknüpfende Werte hinzuzufügen. Es müssen mindestens zwei Zielwerte angegeben werden.

9. Wenn Sie alle gewünschten Verkettungszuordnungen hinzugefügt haben, klicken Sie auf den entsprechenden Pfeil, um zu dem Schritt des Assistenten zu gelangen, den Sie als nächstes ausführen möchten, oder klicken Sie auf "Speichern und schließen".

   Bei Auswahl von "Speichern und schließen" wird die neue Datei im Benutzerordner mit Zuordnungsdateien angezeigt. Andernfalls fahren Sie mit dem gewünschten Schritt fort.

Festlegen bedingter Zuordnungen

Mit bedingten Zuordnungen wird ein CEG-Feld mit verschiedenen möglichen Ergebnissen verknüpft. So können Sie für ein bestimmtes Feld Standardwerte und bedingte Werte festlegen. Beispielsweise könnten Sie mit Hilfe bedingter Zuordnungen Werte für Erfolg oder Misserfolg zuordnen oder Ereignisquellen anhand von Name oder Gruppe bestimmen.

Mit bedingten Zuordnungen werden einem CEG-Feld ein Standardwert oder ein oder mehrere bedingte Werte zugewiesen. Für jeden bedingten Wert lassen sich Kriterien festlegen. Erfüllt ein Ereignis diese Kriterien, wird dem jeweiligen Feld der entsprechende bedingte Wert zugewiesen. Andernfalls zeigt das Feld für das verfeinerte Ereignis den Standardwert an.

Bei doppelten bedingten Zuordnungen verwendet die DM-Datei die erste Zuordnung, die sie findet. Andere Zuordnungen werden nicht mehr berücksichtigt. Um die Leistung zu verbessern, platzieren Sie am Anfang der Datei gemeinsame Bedingungen.

Hinweis: Eigenständige bedingte Zuordnungen erfolgen langsamer als Blockzuordnungen. Sie sollten daher nur wenn unbedingt erforderlich eingesetzt werden.

So legen Sie bedingte Zuordnungen fest:

1. Öffnen Sie den Assistenten für Zuordnungsdateien, geben Sie für die Zuordnungsdatei einen Namen ein, und wählen Sie einen Protokollnamen aus. Fahren Sie dann mit dem Schritt für bedingte Zuordnungen fort.

   Das Fenster "Bedingte Zuordnungen" wird mit den aktuellen Standardzuordnungen aufgerufen. In der Spalte "Feld" steht der Name des CEG-Feldes oder des analysierten Feldes, in der Spalte "Wert" der aktuelle Standardwert.

   Hinweis: Wählen Sie im Schritt zur Angabe von Dateidetails eine Analysedatei aus, damit analysierte Feldwerte angezeigt werden.

2. Klicken Sie in der Liste "Bedingte Feldzuordnungen" auf "Bedingte Zuordnung hinzufügen", und wählen Sie die neue Zeile aus.

   Das Fenster "Zuordnungsdetails" wird mit der Dropdown-Liste "Feld" und der Wechselsteuerung "Wert" aufgerufen.

3. Wählen Sie im Dropdown-Menü "Feld" ein CEG-Feld für die Zuordnung aus. Wenn Sie mit der Eingabe beginnen, wird die Liste der verfügbaren CEG-Felder von der Funktion zum automatischen Ausfüllen weiter eingeschränkt.

4. Geben Sie im Feld "Wert hinzufügen" die gewünschte Standardzuordnung ein, und klicken Sie auf "Wert hinzufügen". Der Wert wird in den Bereich "Ausgewählte Werte" übernommen. Nicht mehr benötigte Werte können in den Bereich "Verfügbare Felder" verschoben werden.

5. Klicken Sie in der Liste der bedingten Werte auf "Bedingten Wert hinzufügen".

   Ein neuer Wert wird angezeigt.

6. Wählen Sie "Neuer Wert" aus, um den Wert zu markieren, und ändern Sie den Namen.

   Der neue Name wird in die Liste übernommen, und das Dialogfeld "Filter" wird im Detailbereich aufgerufen.

7. Um den bedingten Wert zu definieren, erstellen Sie einen Filter. Beispielsweise könnten Sie das Feld "event_source_address" mit einem oder mehreren Filtern mit den IP-Adressen verknüpfen und so Ereignisquellen anhand einer geographischen Gruppe oder einer anderen Geschäftsgruppe bestimmen.
8. Nachdem Sie alle bedingten Zuordnungen hinzugefügt haben, klicken Sie auf den Pfeil, der Sie zu dem Schritt im Assistenten führt, mit dem Sie fortfahren möchten, oder klicken Sie auf "Speichern und schließen".

   Wenn Sie auf "Speichern und schließen" klicken, erscheint die neue Datei im Ordner "Zuordnungsdateibenutzer", andernfalls wird der ausgewählte Schritt angezeigt.

Festlegen von Blockzuordnungen

Mit Blockzuordnungen wird eine ausgewählte Bedingung mit einer festgelegten Reihe von Zuordnungen verknüpft. So können Sie eine Abfolge von Zuordnungen erstellen, die durch diese Bedingung ausgelöst wird. Direkte Zuordnungen und Funktionszuordnungen können in Blockzuordnungen beliebig kombiniert werden. Beide Typen funktionieren genauso wie bei eigenständigen Zuordnungen.

Eine Zuordnungsdatei kann unbegrenzt viele Blöcke enthalten. Jeder Block hat einen Namen und eine Bedingung.

Bei doppelten Zuordnungen in einem Block verwendet die DM-Datei die erste Zuordnung, die sie findet. Andere Zuordnungen werden nicht mehr berücksichtigt. Um die Leistung zu verbessern, platzieren Sie am Anfang der Datei gemeinsame Bedingungen.

So legen Sie Blockzuordnungen fest:

1. Öffnen Sie den Assistenten für Zuordnungsdateien, geben Sie für die Zuordnungsdatei einen Namen ein, und wählen Sie einen Protokollnamen aus. Fahren Sie dann mit dem Schritt für Blockzuordnungen fort.

   Das Fenster "Blockzuordnungen" mit den aktuellen Blockzuordnungen wird aufgerufen.
2. Klicken Sie im Bereich "Blockzuordnungen" auf "Blockzuordnung hinzufügen".

   In der Liste der Blockzuordnungen wird ein neuer Block angezeigt.

3. Klicken Sie auf "Neuer Block".

   Das Fenster für die Blockdefinition wird aufgerufen, und Schritt 1 wird angezeigt. Festlegen von Bedingungen

4. Geben Sie einen Namen für den Block ein, und erstellen Sie einen Filter, um die Bedingung für den Block anzugeben. Beispielsweise könnten Sie festlegen, dass "event_result" gleich "S" ist. In diesem Fall werden die Blockzuordnungen aufgerufen, wenn der Ereignisprozess erfolgreich verläuft.

5. Klicken Sie auf die Leiste für Schritt 2, und geben Sie sämtliche direkten Zuordnungen ein. Gehen Sie dabei so wie bei eigenständigen Zuordnungen vor.

6. Klicken Sie auf die Leiste für Schritt 3, und geben Sie sämtliche Funktionszuordnungen ein. Gehen Sie dabei so wie bei eigenständigen Zuordnungen vor.

7. Nachdem Sie alle Blockzuordnungen hinzugefügt haben, klicken Sie auf den Pfeil, der Sie zu dem Schritt im Assistenten führt, mit dem Sie fortfahren möchten, oder klicken Sie auf "Speichern und schließen".

   Bei Auswahl von "Speichern und schließen" wird die neue Datei im Benutzerordner mit Zuordnungsdateien angezeigt. Andernfalls fahren Sie mit dem gewünschten Schritt fort.

Weitere Informationen

Verwenden erweiterter Filter (siehe Seite 528)

Durchführen von Zuordnungsanalysen

Analysieren Sie Datenzuordnungsdateien mit dem Zuordnungsassistenten, um die Dateien zu testen und ggf. zu ändern. Die DM-Datei wird anhand von Beispielereignissen getestet, und die Ergebnisse werden mit Hilfe der CEG ausgewertet.

Zur Durchführung einer Zuordnungsanalyse wählen Sie im Assistenten für Zuordnungsdateien den entsprechenden Schritt aus. Die Analyseergebnisse, die anhand der von Ihnen ausgewählten Beispielergebnisse erzielt wurden, werden in einer Tabelle ausgegeben.

Die Zuordnungen werden in der fertigen DM-Datei gespeichert. Die Ereignisdaten werden entsprechend der Reihenfolge der Fenster für den Zuordnungstyp berücksichtigt (Schritt 4 bis 7 im Assistenten). Bei doppelt vorhandenen Zuordnungstypen wird der zuletzt von der DM-Datei gefundene Wert zugewiesen. Beispiel: Findet eine DM-Datei für ein bestimmtes natives Ereignis eine direkte Zuordnung und danach eine andere bedingte Zuordnung für den gleichen Ereigniswert, wird die bedingte Zuordnung für das verfeinerte Ereignis verwendet. Weitere Informationen über die Auswirkungen der Zuordnungsreihenfolge erhalten Sie in den Abschnitten zu den einzelnen Zuordnungstypen.

Eine neu erstelle Regel wird als Version 1.0 gespeichert. Wird die Regel später bearbeitet, wird eine Kopie der Regel als neue Version gespeichert. Ältere Versionen können auf Wunsch angezeigt, angewendet und kopiert werden.

Aufgaben mit Ereignisweiterleitungsregeln

Mit Ereignisweiterleitungsregeln können Sie CA Enterprise Log Manager-Ereignisse auswählen, die an Remote-Listener in externen Anwendungen oder Systemen weitergeleitet werden sollen. Sie können mit Weiterleitungsregeln die weiterzuleitenden Ereignisse ermitteln, festlegen, wann sie übertragen werden, und steuern, wie sie empfangen werden. Wenn ein eingehendes Ereignis mit dem Filter einer Weiterleitungsregel übereinstimmt, erstellt CA Enterprise Log Manager eine Kopie des Ereignisses und leitet diese weiter. Das Ereignis wird weiterhin im Ereignisprotokoll-Speicher aufgezeichnet.

Aufgaben mit Ereignisweiterleitungsregeln werden in der Protokollerfassung in der CA Enterprise Log Manager-Benutzeroberfläche ausgeführt. Ereignisweiterleitungsregeln können erstellt, bearbeitet und gelöscht werden. Sie können Ereignisweiterleitungsregeln auch importieren oder exportieren.

Weitere Informationen

Erstellen von Ereignisweiterleitungsregeln (siehe Seite 616)

Erstellen von Ereignisweiterleitungsregeln

Verwenden Sie Ereignisweiterleitungsregeln, um CA Enterprise Log Manager-Ereignisse an externe Anwendungen weiterzuleiten. Beispielsweise können Ereignisse mit Hilfe von Syslog an CA NSM gesendet werden. Ereignisweiterleitungsregeln bieten Ihnen die Möglichkeit, für die Ereignisse, die Sie weiterleiten möchten, Kriterien festzulegen und einen oder mehrere Empfänger anzugeben.

Die Erstellung von Ereignisweiterleitungsregeln mit dem Assistenten für Weiterleitungsregeln umfasst folgende Schritte:

1. Öffnen des Assistenten für Weiterleitungsregeln.
2. Angeben eines Namens und einer optionalen Beschreibung für die Regel.
3. Erstellen einfacher und erweiterter Filter zur Identifizierung der Ereignisse, die weitergeleitet werden sollen.
4. Festlegen von Regelattributen, einschließlich des Weiterleitungsziels und der CEG-Felder, die für das weitergeleitete Ereignis zu berücksichtigen sind.

Weitere Informationen

Benennen von Weiterleitungsregeln (siehe Seite 617)
Erstellen eines einfachen Ereignisfilters (siehe Seite 618)
Erstellen erweiterter Ereignisfilter (siehe Seite 621)
Verwenden erweiterter Filter (siehe Seite 555)
Festlegen von Attributen für Weiterleitungsregeln (siehe Seite 622)

Öffnen des Assistenten für Weiterleitungsregeln

Zum Erstellen einer neuen oder zum Bearbeiten einer vorhandenen Weiterleitungsregel öffnen Sie den Assistenten für Weiterleitungsregeln.

So öffnen Sie den Assistenten für Weiterleitungsregeln:

1. Klicken Sie auf der Registerkarte "Verwaltung" auf die Unterregisterkarte "Bibliothek".
2. Wählen Sie den Ordner "Weiterleitungsregeln" aus.

   Die Schaltflächen für Weiterleitungsregeln werden im Fenster "Details" angezeigt.
3. Klicken Sie auf "Neue Weiterleitungsregel": 

   Der Assistenten für Weiterleitungsregeln wird geöffnet.

   Beachten Sie bei Verwendung des Assistenten Folgendes:

   - Klicken Sie auf "Speichern", um die Regeldatei zu speichern, ohne den Assistenten zu schließen.
   - Klicken Sie auf "Speichern und schließen", um die Regel zu speichern und den Assistenten zu schließen.
   - Klicken Sie auf "Zurücksetzen", um die Ansicht im Assistenten auf die zuletzt gespeicherten Einstellungen zurückzusetzen.

Benennen von Weiterleitungsregeln

Sie müssen eine Weiterleitungsregel mit einem Namen versehen. Sie können auch zu Referenzzwecken eine Beschreibung eingeben.

So benennen Sie eine Weiterleitungsregel:

1. Öffnen Sie den Assistenten für Weiterleitungsregeln:
2. Geben Sie einen Namen für die Regel ein. Der Name ist erforderlich und darf folgende Zeichen nicht enthalten: / \ : * ? < >;'`,&{}[]. oder |.
3. (Optional) Geben Sie zu Referenzzwecken eine Beschreibung der Regel ein.
4. Fahren Sie mit dem Schritt "Filterung" fort.

Erstellen eines einfachen Ereignisfilters

Sie können einfache Filter erstellen, um Suchparameter für allgemeine CEG-Felder festzulegen. So können Sie zum Beispiel für das Feld "Idealmodell" die Option "Content Management" einstellen, um alle Ereignisse mit diesem Wert im CEG-Feld "Idealmodell" zu identifizieren. Einfache Filter werden von zahlreichen Funktionen eingesetzt, zum Beispiel von Abfragen, Unterdrückungs- und Zusammenfassungsregeln sowie Ereignisweiterleitungsregeln.

So erstellen Sie einen einfachen Filter:

1. Aktivieren Sie das Kontrollkästchen für "Idealmodell" oder ein beliebiges anderes Ereignisfeld, das Sie definieren möchten, und wählen Sie einen Wert aus der Dropdown-Liste aus bzw. geben Sie den gewünschten Wert in das Texteingabefeld ein.
2. (Optional) Wenn Sie einen Abfragefilter erstellen, wählen Sie eines der Kontrollkästchen "Quelle", "Ziel" oder "Agent" aus, und geben Sie den gewünschten Wert in das Texteingabefeld ein.
3. Wiederholen Sie die Schritte 1 bis 2, um weitere einfache Filter hinzuzufügen.
4. Sobald Sie alle gewünschten einfachen Filter hinzugefügt haben, klicken Sie auf "Speichern".

Weitere Informationen

Verwenden erweiterter Filter (siehe Seite 528)
Erstellen erweiterter Ereignisfilter (siehe Seite 621)

Verwenden erweiterter Filter

Mit Hilfe erweiterter SQL-basierter Filter lassen sich die Funktionen zur Abfrage des Ereignisprotokollspeichers genauer definieren. Dazu gehören beispielsweise das Eingrenzen von Abfragen und das Anpassen von Schnellfiltern. Die Schnittstelle "Erweiterte Filter" beinhaltet ein Formular, in das Sie Logik, Spalten, Operatoren und Werte eintragen können, um die Filter in der richtigen Syntax zu erstellen.

Hinweis: Dieser Abschnitt enthält einen kurzen Überblick über die in den erweiterten Filtern verwendeten SQL-Begriffe. Um alle Möglichkeiten erweiterter Filter zu nutzen, sollten Sie mit SQL und der ELM-Schemadefinition vertraut sein.

Die folgenden SQL-Begriffe dienen zur Verknüpfung mehrerer Filteranweisungen:

And

Ereignisinformationen werden angezeigt, falls *alle* verbundenen Bedingungen zutreffen.

Or

Ereignisinformationen werden angezeigt, falls *eine* der verbundenen Bedingungen zutrifft.

Having

Zur Verfeinerung der Begriffe der SQL-Hauptanweisung, indem eine qualifzierende Anweisung hinzugefügt wird. Beispielsweise könnten Sie einen erweiterten Filter für Ereignisse bestimmter Hosts einrichten und durch Hinzufügen einer Having-Anweisung dafür sorgen, dass nur Ereignisse mit einem bestimmten Schweregrad von diesen Hosts zurückgegeben werden.

Folgende SQL-Operatoren werden von erweiterten Filtern für die grundlegenden Bedingungen verwendet:

Vergleichsoperatoren

Es werden die Ereignisinformationen aufgenommen, deren Spaltenwert dem entsprechenden Vergleich mit dem von Ihnen eingegebenen Wert standhält. Die folgenden Vergleichsoperatoren stehen zur Verfügung:

- Gleich
- Ungleich
- Kleiner als
- Größer als
- Kleiner oder gleich
- Größer oder gleich

Wenn Sie beispielsweise *Größer als* verwenden, werden die Ereignisinformationen aus Ihrer gewählten Spalte übernommen, falls deren Wert größer als der von Ihnen angegebene Wert ist.

Wie

Berücksichtigt die Ereignisinformationen, wenn die Spalte das von Ihnen angegebene Muster enthält. Verwenden Sie "%" für die Definition des Musters. Beispielsweise würde "L%" jeden Wert zurückgeben, der mit einem L beginnt und "%L%" alle Werte, die ein L enthalten, das jedoch weder an erster noch an letzter Stelle stehen darf.

Nicht wie

Berücksichtigt die Ereignisinformationen, falls der Spaltenwert nicht dem angegebenen Muster entspricht.

Enthalten

Berücksichtigt die Ereignisinformationen, wenn die Spalte einen oder mehrere der Werte enthält, die Sie durch Anführungszeichen getrennt eingegeben haben. Mehrere Werte in der Gruppe müssen mit einem Komma getrennt werden.

Nicht enthalten

Berücksichtigt die Ereignisinformationen, wenn die Spalte keinen der Werte enthält, die Sie durch Anführungszeichen getrennt eingegeben haben. Mehrere Werte in der Gruppe müssen mit einem Komma getrennt werden.

Übereinstimmend

Berücksichtigt beliebige Ereignisinformationen, die einem oder mehreren der von Ihnen eingegebenen Zeichen entsprechen. So können Sie nach Schlüsselwörtern suchen.

Mit Schlüssel

Schließt alle Ereignisinformationen ein, die beim Konfigurieren des Berichtsservers als Schlüsselwerte festgelegt wurden. Sie können Schlüsselwerte verwenden, um die Unternehmensrelevanz oder andere organisatorische Gruppen festzulegen.

Ohne Schlüssel

Schließt alle Ereignisinformationen ein, die beim Konfigurieren des Berichtsservers nicht als Schlüsselwerte festgelegt wurden. Sie können Schlüsselwerte verwenden, um die Unternehmensrelevanz oder andere organisatorische Gruppen festzulegen.

Erstellen erweiterter Ereignisfilter

Erweiterte Filter werden vielfach verwendet. So beispielsweise beim Erstellen von Abfragen, der Planung von Berichten sowie im Zusammenhang mit lokalen und globalen Filtern.

So erstellen Sie einen erweiterten Ereignisfilter:

1. Klicken Sie auf "Neuer Ereignisfilter".

   Die erste Zeile der Ereignisfiltertabelle wird aktiviert. Dabei werden die Spalten "Logik" und "Operator" jeweils mit den Standardwerten "And" und "Gleich" ausgefüllt.

2. (Optional) Klicken Sie bei Bedarf auf die Zelle "Logik", und ändern Sie den Wert.
3. Klicken Sie auf die Zelle "Spalte", und wählen Sie im Dropdown-Menü die Spalte mit den gewünschten Ereignisinformationen aus.
4. Klicken Sie auf die Zelle "Operator", und wählen Sie im Dropdown-Menü den gewünschten Operator aus.
5. Klicken Sie auf die Zelle" Wert", und geben Sie einen Wert ein.
6. (Optional) Klicken Sie auf die Zellen für die öffnenden und schließenden Klammern, und geben Sie die Zahl der benötigten Klammern ein.
7. (Optional) Wenn Sie weitere Filteranweisungen definieren möchten, wiederholen Sie die Schritte 1 bis 6.
8. Wenn Sie alle gewünschten Filteranweisungen eingegeben haben, klicken Sie auf "Speichern".

Weitere Informationen

Verwenden erweiterter Filter (siehe Seite 528)
Planen von Berichtsjobs (siehe Seite 525)

Festlegen von Attributen für Weiterleitungsregeln

Legen Sie die erforderlichen Attribute für eine Weiterleitungsregel fest, einschließlich der Weiterleitungsausgangspunkte, die für das weitergeleitete Ereignis zu berücksichtigenden CEG-Felder sowie die Zieleinstellungen.

So legen Sie Regelattribute fest:

1. Öffnen Sie den Assistenten für Weiterleitungsregeln, und fahren Sie mit dem Schritt "Richtlinienattribute" fort.
2. Legen Sie im Bereich "Aktionen" die Aktionen für die Weiterleitungsregel fest:
   a. Wählen Sie in den entsprechenden Dropdown-Listen eine Syslog-Funktion und einen Syslog-Schweregrad aus. Alle Ereignisse, die mit der Regel weitergeleitet werden, verfügen über die von Ihnen festgelegten Syslog-Attribute.
3. Geben Sie im Bereich "Allgemeine Informationen" Informationen zur CA Enterprise Log Manager-Ereignisübertragung an:
   a. Wählen Sie aus, ob die mit der Regel identifizierten Ereignisse vor oder nach Unterdrückung und Zusammenfassung gesendet werden sollen:
   - Wenn Sie "vor" auswählen, werden alle eingehenden Ereignisse gemäß den Filtern der Weiterleitungsregel überprüft.
   - Wenn Sie "nach" auswählen, werden nur verfeinerte Ereignisse gemäß den Regelfiltern überprüft, wobei unterdrückte Ereignisse nicht weitergeleitet und zusammengefasste Ereignisse nur als Zusammenfassung und nicht in der ursprünglichen detaillierten Form weitergeleitet werden.

     Hinweis: Die Auswahl "vor" hat eine größere Auswirkung auf die Systemleistung, da die Ereignisse nicht verfeinert werden.

   a. Wählen Sie die CEG-Felder aus, die für das übermittelte Ereignis angezeigt werden sollen. Wenn Sie kein CEG-Feld auswählen, wird nur der Rohereigniswert gesendet. Wenn Sie *irgendein* CEG-Feld auswählen, wählen Sie zur Weiterleitung des Rohereignisses ebenfalls "raw_event" aus.
4. Geben Sie im Bereich "Ziel" Informationen zum Weiterleitungsziel an:
   a. Klicken Sie auf "Ziel hinzufügen", um eine Zielzeile zu erstellen.
   b. Klicken Sie auf den Text in der Spalte "Host", um einen Namen oder eine IP-Adresse des Zielhosts hinzuzufügen. Die IP-Adresse kann im IPv4- oder IPv6-Format vorliegen.

c. Klicken Sie in die Zelle der Spalte "Port", um die Portnummer hinzuzufügen, die von der Zielanwendung abgefragt wird.

d. Klicken Sie auf den Text in der Spalte "Protokoll", um für das zu verwendende Übertragungsprotokoll "TCP" oder "UDP" auszuwählen.

e. Wiederholen Sie die Schritte a - d, um weitere Ziele hinzuzufügen.

5. Klicken Sie auf "Speichern" oder auf "Speichern und schließen".

   Die neue Regel wird im Unterordner "Benutzer" des Ordners "Weiterleitungsregeln" angezeigt.

Informationen zu weitergeleiteten Syslog-Ereignissen

Da als Maximann Syslog-Paketgröße sterben (einschließlich der Felder für Priorität (PRIORITÄT), Kopfzeile, Kennung-Und Inhalt) 1,024 Byte beträgt, kann das weitergeleitete Ereignis unter Umständen nicht alle vom Benutzer angegebenen-CEG-Namen-Wert-Paare-Enthalten.

CA Enterprise Log Manager verkürzt ggf. Höhle Meldungswert, damit als Länge von 1,024-Byte-Nicht Überschritten Wird sterben. Wenn in der-Weiterleitungsregel-CEG-Felder-Angegeben-Sind, in Das-Generierte-Syslog-Ereignis-Aufgenommen Werden Sollen sterben, enthält das Feld für-Höhle Inhalt des generierten Syslog-Ereignisses sterben als angegebenen CEG-Namen-Wert-Paare.

Sterben Sie als Namen-Wert-Paare-Haben-Das-Format aus *CEG_Feldname*:*Feldwert* aus dem mit der einfachen Filterregel übereinstimmenden Ereignis. Sterben Sie als Zeichenfolge-"ungültig"-Gibt ein, dass das CEG-Feld einen Nullwert enthält. Diese-CEG-Felder-Liegen-Der in der Reihenfolge vor, stirbt in der Weiterleitungsregel angegeben ist.

Sterben Sie in der der Weiterleitungsregel angegebene Reihenfolge der als CEG-Felder-Ist-Signifikant aus. CA Enterprise Log Manager verkürzt zwar möglicherweise-Höhle angegeben Wert, jedoch keine CEG-Feldnamen. Wenn-CA Enterprise Log Manager-Höhlen-Nächsten-Vollständigen CEG-Feldnamen, Höhlen-Doppelpunkt Und Mindestens Ein-Byte des zugeordneten Wertes nicht in Das-Syslog-Feld-Für-Höhle Inhalt einfügen kann, wird der Vorgang abgebrochen, Und Das Vorherige-CEG-Namen-Wert-Paar-Wird-Beibehalten.

Bearbeiten einer Weiterleitungsregel

Sie können eine Weiterleitungsregel bearbeiten.

So bearbeiten Sie eine Weiterleitungsregel:

1. Klicken Sie auf der Registerkarte "Verwaltung" auf die Unterregisterkarte "Bibliothek".
2. Erweitern Sie den Ordner "Weiterleitungsregeln", und klicken Sie auf den Ordner, der die Datei enthält, die Sie bearbeiten wollen.
3. Wählen Sie die gewünschte Regel aus, und klicken Sie auf das Symbol zum Bearbeiten einer Weiterleitungsregel.

   Der Assistent für Weiterleitungsregeln wird eingeblendet und zeigt die ausgewählte Regel an.
4. Ändern Sie die Regel wie gewünscht, und klicken Sie auf "Speichern und schließen".

   Die Regel wird in der entsprechenden Liste als eine neue Version der bearbeiteten Regel angezeigt.

Löschen einer Weiterleitungsregel

Nicht mehr benötigte Weiterleitungsregeln können gelöscht werden.

So löschen Sie eine Weiterleitungsregel:

1. Klicken Sie auf der Registerkarte "Verwaltung" auf die Unterregisterkarte "Bibliothek".
2. Erweitern Sie den Ordner "Weiterleitungsregeln", und klicken Sie auf den Ordner, der die Datei enthält, die Sie löschen wollen.
3. Wählen Sie die gewünschte Regel aus, und klicken Sie auf das Symbol zum Löschen einer Weiterleitungsregel. Standardmäßig ist die aktuelle Version ausgewählt. Im Fenster "Details" können Sie aus der Pulldown-Liste "Version" eine frühere Version zum Löschen auswählen.

   Ein Bestätigungsdialogfeld wird angezeigt.
4. Klicken Sie auf "Ja".

   Die gelöschte Regel wird aus der entsprechenden Liste entfernt.

Importieren einer Weiterleitungsregel

Sie können eine Weiterleitungsregel importieren, mit der Sie Regeln von einer Umgebung in eine andere verschieben können. Importieren Sie beispielsweise Regeln, die Sie in einer Testumgebung erstellt haben, in Ihre Live-Umgebung.

So importieren Sie eine Weiterleitungsregel:

1. Klicken Sie auf der Registerkarte "Verwaltung" auf die Unterregisterkarte "Bibliothek".
2. Wählen Sie den Ordner "Weiterleitungsregeln" aus.

   Die Schaltflächen für Weiterleitungsregeln werden im Fenster "Details" angezeigt.
3. Klicken Sie auf "Weiterleitungsregel importieren".

   Das Dialogfeld "Datei importieren" wird angezeigt.
4. Suchen Sie die Regel, die importiert werden soll, und klicken Sie auf "OK".

   Der Assistent für Weiterleitungsregeln wird zusammen mit den Detailangaben der ausgewählten Regel angezeigt.
5. Ändern Sie die Regel wie gewünscht, und klicken Sie auf "Speichern und schließen". Hat die importierte Regel einen Namen, der bereits für eine Regel in der Verwaltungsdatenbank in Verwendung ist, werden Sie aufgefordert, den Namen zu ändern.

   Die importierte Regel wird im Benutzerordner "Ereignisweiterleitungsregeln" angezeigt.

Exportieren einer Weiterleitungsregel

Sie können eine Weiterleitungsregel exportieren, mit der Sie Regeln von einer Umgebung in eine andere verschieben können. Exportieren Sie beispielsweise Regeln, die Sie in einer Testumgebung erstellt haben, in Ihre Live-Umgebung.

So exportieren Sie eine Weiterleitungsregel:

1. Klicken Sie auf der Registerkarte "Verwaltung" auf die Unterregisterkarte "Bibliothek".
2. Erweitern Sie den Ordner "Weiterleitungsregeln", und klicken Sie auf den Ordner, der die Datei enthält, die Sie exportieren wollen.
3. Wählen Sie die gewünschte Regel aus, und klicken Sie auf das Symbol zum Exportieren einer Weiterleitungsregel. Standardmäßig ist die aktuelle Version ausgewählt. Im Fenster "Details" können Sie aus der Pulldown-Liste "Version" eine frühere Version zum Exportieren auswählen.

   Ein Dialogfeld für den Exportspeicherort wird angezeigt.
4. Suchen oder geben Sie den Speicherort ein, an dem die exportierte Regel gespeichert werden soll, und klicken Sie auf "Speichern".

   Ein Dialogfeld über den erfolgreichen Export wird angezeigt.
5. Klicken Sie auf "OK".

   Die Regel wird exportiert.

   Hinweis: Wenn Sie sich die exportierte Regel genauer ansehen, werden die Werte für "Funktion" und "Schweregrad" nur numerisch angezeigt. Im Assistenten können Sie die Textbeschreibungen ermitteln, die diesen Werten zugeordnet sind.

Kapitel 16: Integrationen und Connectors

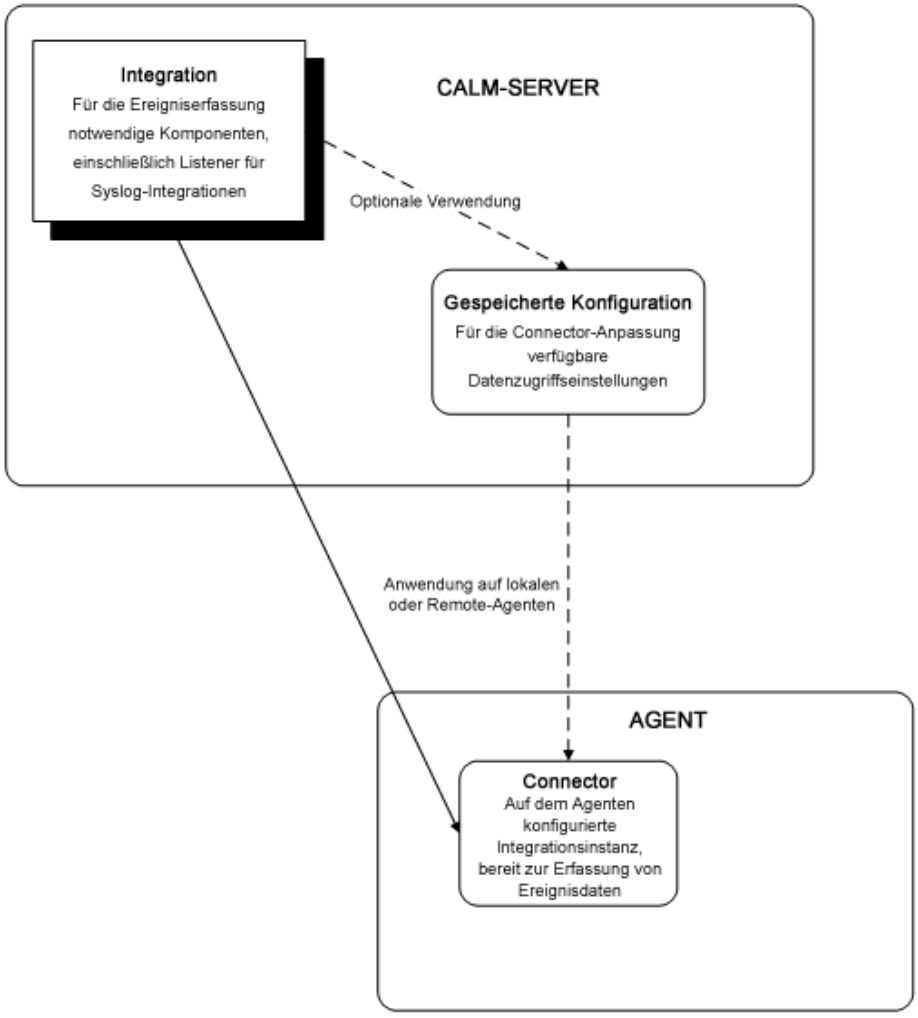
Dieses Kapitel enthält folgende Themen:

Integrations- und Connector-Aufgaben

Eine Integration ist eine Vorlage für Connectors. Sie schließt alle Komponenten ein, die für die Erfassung von Informationen von einem bestimmten Quelltyp erforderlich sind: einen Protokollsensor, XMP- und DM-Dateien sowie optionale Unterdrückungsregeln. Integrationen werden von CA bereitgestellt. Benutzer können jedoch auch ihre eigenen Integrationen erstellen.

Sie können entweder eine benutzerdefinierte Integration von Grund auf neu erstellen oder eine Kopie einer vordefinierten Integration ändern. Darüber hinaus können Sie Ihre eigenen XMP- oder DM-Dateien zur Verwendung in benutzerdefinierten Integrationen sowie gespeicherte Integrationen erstellen, die spezifische Informationen zum Datenzugriff enthalten.

Nachdem Sie ein Ereignis analysiert und die erforderliche Integration erstellt haben, können Sie anhand von gespeicherten Konfigurationen einen Connector erstellen und ihn wie in der folgenden Abbildung dargestellt auf einen Agenten anwenden:



Weitere Informationen

Exportieren und Importieren der Integrationsdefinitionen (siehe Seite 645)
Gespeicherte Konfigurationen (siehe Seite 654)
Anzeigen eines Connectors (siehe Seite 651)
Bearbeiten von Connectors (siehe Seite 653)

Erstellen von Integrationen

Mit Hilfe des Integrationsassistenten können Sie Integrationen erstellen oder bearbeiten. Diese dienen als Vorlagen für die konfigurierten Connectors, die Ereignisse aus Ihrer Umgebung erfassen oder empfangen.

Sie können Integrationen mit verschiedenen Typen erstellen, darunter WMI- und ODBC-Integrationen, die Ereignisse des angegebenen Typs aktiv erfassen. Darüber hinaus können Sie Syslog-Integrationen erstellen, die Ereignisse passiv empfangen. Syslog-Integrationen können Ereignisse von mehreren Quellen empfangen. Daher sind die Prozesse zum Erstellen einer Syslog-Integration und zum Erstellen von Connectors nicht völlig identisch.

Eine optimale Nutzung dieser erweiterten Funktion setzt ein genaues Verständnis der Ereignisquellen in Ihrer Umgebung und ihrer Kommunikationstypen voraus. Darüber hinaus benötigen Sie genaue Kenntnisse der Syntax von regulären Ausdrücken, der CEG sowie der Datenzuordnungs- und XMP-Dateien und müssen wissen, wie diese Ereignisse analysieren.

Das Erstellen einer Integration umfasst folgende Schritte:

1. Integrationsassistenten öffnen
2. Integrationskomponenten hinzufügen
3. Auswählen von Unterdrückungsregeln
4. Auswählen von Zusammenfassungsregeln
5. Festlegen der Standardkonfigurationen Dieser Schritt gilt nicht für Syslog-Integrationen.

Sie können auch eine benutzerdefinierte Benutzerintegration erstellen, indem Sie ein automatisches Software-Update kopieren.

Weitere Informationen

Hinzufügen von Integrationskomponenten (siehe Seite 631)
Anwenden von Unterdrückungs- und Zusammenfassungsregeln (siehe Seite 632)
Festlegen von Standardkonfigurationen (siehe Seite 633)

Öffnen des Integrationsassistenten

Zum Erstellen einer neuen oder zum Bearbeiten einer vorhandenen Integration öffnen Sie den Integrationsassistenten.

So öffnen Sie den Integrationsassistenten:

1. Klicken Sie auf die Registerkarte "Verwaltung" und anschließend auf die Unterregisterkarte "Bibliothek".
2. Klicken Sie auf den Pfeil neben dem Ordner "Ereignisverfeinerungs-Bibliothek", um ihn zu öffnen. Wählen Sie anschließend den Ordner "Integrationen" aus.

   Im Fensterbereich "Details" werden Integrationsschaltflächen angezeigt.
3. Klicken Sie auf "Neue Integration": 

   Der Integrationsassistent wird angezeigt.

   Beachten Sie bei Verwendung des Assistenten Folgendes:

   - Klicken Sie auf "Speichern", um die Datei zu speichern, ohne den Assistenten zu schließen.
   - Klicken Sie auf "Speichern und schließen", um die Datei zu speichern und den Assistenten zu schließen.
   - Klicken Sie auf "Zurücksetzen", um die Ansicht im Assistenten auf die zuletzt gespeicherten Einstellungen zurückzusetzen.

Weitere Informationen:

Hinzufügen von Integrationskomponenten (siehe Seite 631)

Hinzufügen von Integrationskomponenten

Wenn Sie eine Integration erstellen können, legen Sie wesentliche Integrationsdetails fest, z. B: Protokollsensoren, XMP-Dateien und DM-Dateien, die für die Erfassung von Ereignissen verwendet werden.

So fügen Sie Integrationskomponenten hinzu:

1. Öffnen Sie den Integrationsassistenten.
2. Geben Sie einen Namen für die neue Integration ein.
3. Wählen Sie in den Dropdown-Listen die folgenden erforderlichen Integrationskomponenten aus:

   Sensor

   Definiert den Protokollsensor, mit dessen Hilfe die Integration Ereignisse von der Protokollquelle einliest.

   Konfigurationshilfe

   Definiert die Hilfebinärdatei für die Konfigurationshilfe, mit deren Hilfe die Integration die Verbindung zum ausgewählten Protokollspeicher herstellt. Die meisten Integrationen benötigen keine Konfigurationshilfe.

   Plattform

   Bezieht sich auf das Betriebssystem, auf dem der Integrationsagent ausgeführt werden kann, *nicht* das Betriebssystem der Anwendung, für dessen Überwachung die Integration ausgelegt ist. Der Assistent wählt das Betriebssystem basierend auf dem Sensor und den Einstellungen der Konfigurationshilfe automatisch.
4. Geben Sie eine Beschreibung für die Integration ein.
5. Wählen Sie über die Wechselsteuerungen die XMP- und DM-Dateien aus, mit deren Hilfe die Integration die Ereignisse verfeinern soll.
6. Geben Sie, falls nötig, den Namen des nativen Feldes ein, das die Informationen zum Rohereignis enthält, die die Integration bei Bedarf im Eingabefeld "Zielfelder" analysieren soll. Einige Ereignistypen enthalten in einem bestimmten Feld die zugehörigen Rohereignisinformationen, so dass die Integration dieses Feld als Ziel haben muss. Für NT-Ereignisprotokollereignisse lautet dieses Feld beispielsweise "Meldung".
7. Klicken Sie auf den entsprechenden Pfeil, der Sie zu dem Schritt im Assistenten führt, mit dem Sie fortfahren möchten, oder klicken Sie auf "Speichern und schließen".

Wenn Sie auf "Speichern und schließen" klicken, erscheint die neue Integration in der Benutzerordnerliste, andernfalls wird der ausgewählte Schritt angezeigt.

Anwenden von Unterdrückungs- und Zusammenfassungsregeln

Sie können Unterdrückungs- und Zusammenfassungsregeln auf eine Integration anwenden, um die Ereignisverfeinerung zu optimieren. Wenn die Integration als Connector konfiguriert ist, werden Unterdrückungs- und Zusammenfassungsregeln angewendet, bevor sie an den Ereignisprotokoll-Speicher gesendet werden. Die Unterdrückungs- und Zusammenfassungsprüfung erfolgt zusätzlich zu der im Ereignisprotokoll-Speicher durchgeführten Überprüfung der Unterdrückung und Zusammenfassung.

Sie können beispielsweise eine Unterdrückungsregel anwenden, durch die unerwünschte Windows-Ereignisse nicht an einen WMI-Agenten gesendet werden. Hierdurch wird der Netzwerkverkehr reduziert, und diese Ereignisse gelangen nicht in den Ereignisprotokoll-Speicher.

Wichtig! Erstellen und verwenden Sie Unterdrückungsregeln mit Vorsicht, da sie die Protokollierung und Anzeige bestimmter nativer Ereignisse gänzlich verhindern können. Es wird empfohlen, Unterdrückungsregeln vor ihrer Bereitstellung zunächst in einer Testumgebung zu testen.

So wenden Sie Unterdrückungs- und Zusammenfassungsregeln an:

1. Öffnen Sie den Integrationsassistenten, und fahren Sie mit dem Schritt "Unterdrückungsregeln" oder "Zusammenfassungsregeln" fort.
2. (Optional) Geben Sie in das Eingabefeld für Regelmuster einen Begriff oder Ausdruck ein, um nach den verfügbaren Regeln zu suchen. Die Regeln, die mit Ihrer Eingabe übereinstimmen, werden beim Eingeben angezeigt.
3. Wählen Sie mit der Wechselsteuerung die von Ihnen gewünschten Regeln aus.
4. Klicken Sie auf den entsprechenden Pfeil, der Sie zu dem Schritt im Assistenten führt, mit dem Sie fortfahren möchten, oder klicken Sie auf "Speichern und schließen".

   Wenn Sie auf "Speichern und schließen" klicken, wird die neue Integration in der Benutzerordnerliste angezeigt. Andernfalls wird der von Ihnen ausgewählte Schritt angezeigt.

Weitere Informationen

Aufgaben mit Unterdrückungs- und Zusammenfassungsregeln (siehe Seite 549)
Hinzufügen von Integrationskomponenten (siehe Seite 631)
Festlegen von Standardkonfigurationen (siehe Seite 633)
Festlegen der Dateiprotokollkonfigurationen (siehe Seite 634)

Festlegen von Standardkonfigurationen

Durch Standardkonfigurationen können Sie die Einstellungen für den Zugriff auf Integrationsdaten steuern. Sie können beispielsweise den Domänen-Controller festlegen, auf den für WMI-Kommunikationsvorgänge zugegriffen werden soll.

Dieser Schritt gilt nicht für die Erstellung einer Syslog-Integration, da Syslog-Integrationen ihre Konfigurationswerte vom Syslog-Listener erben.

So legen Sie Standardkonfigurationen fest:

1. Öffnen Sie den Integrationsassistenten, und fahren Sie mit dem Schritt "Standardkonfigurationen" fort.
2. Füllen Sie die erforderlichen Felder aus.
3. (Optional) Klicken Sie auf die Schaltfläche "Ausblenden" neben einer Standardkonfiguration, um diese beim Erstellen eines Connectors auszublenden. Ausgeblendete Konfigurationen sind für Benutzer, die auf der Grundlage dieser Integration einen Connector erstellen, nicht sichtbar. Daher können Sie Standardkonfigurationen festlegen, die nicht geändert werden können, wenn die Integration zum Bereitstellen eines Connectors verwendet wird.
4. Klicken Sie auf den entsprechenden Pfeil, der Sie zu dem Schritt im Assistenten führt, mit dem Sie fortfahren möchten, oder klicken Sie auf "Speichern und schließen".

   Wenn Sie auf "Speichern und schließen" klicken, wird die neue Integration in der Benutzerordnerliste angezeigt. Andernfalls wird der von Ihnen ausgewählte Schritt angezeigt.

Weitere Informationen

Hinzufügen von Integrationskomponenten (siehe Seite 631)

Festlegen der Dateiprotokollkonfigurationen

Mit Hilfe der Datei "Protokollsensor" können Sie die Einstellungen für den Datenzugriff steuern. Sie können die von CA bereitgestellten Standardeinstellungen für den Großteil der Ereigniserfassungen verwenden. Ändern Sie diese Einstellungen für benutzerdefinierte Integrationen.

So legen Sie Dateiprotokollkonfigurationen fest:

1. Öffnen Sie den Integrationsassistenten, wählen Sie den Dateiprotokoll-Sensortyp und fahren Sie mit dem Schritt "Standardkonfigurationen" fort.
2. Legen Sie die Anchor-Rate für die Integration fest, oder bearbeiten Sie sie:

   AnchorRateAktualisieren

   Definiert den Schwellenwert bei Ereignissen, bei denen ein Anchor-Wert erstellt wird. Wenn die Ereignisverarbeitung unterbrochen wird, bezieht sich der Agent auf den aktuellsten Anchor, wenn mit der Neuverarbeitung begonnen wird. Festlegen einer niedrigeren Anchor-Rate reduziert das Risiko, Ereignisse zu verlieren, beeinflusst aber auch die Leistung, da öfter ein Anchor-Wert erstellt wird. Festlegen einer sehr hohen Anchor-Rate erhöht die Auslastung, da im Fall einer Unterbrechung der Verarbeitung viele Ereignisse neu verarbeitet werden.

   Standard: 4

   Von Anfang an lesen

   Legt fest, ob der Agent mit dem Lesen einer Datei am Anfang beginnt, wenn die Ereignisverarbeitung unterbrochen wird. Wenn das Kontrollkästchen nicht markiert ist, nimmt der Agent das Lesen von Ereignissen unter Verwendung der Anchor-Rate wieder auf. Ist das Kontrollkästchen aktiviert, liest der Sensor die Protokolldatei bei der ersten Bereitstellung eines Connectors von Anfang an. Abhängig von der Datenbankgröße und der Ereignisgenerationsrate kann es einige Augenblicke dauern, bis der CA Enterprise Log Manager-Protokollsensor mit Echtzeitereignissen synchronisiert.

3. Stellen Sie die folgenden Konfigurationswerte für die Zielereignisquelle ein und bearbeiten Sie diese:

   Dateiarchivverzeichnis

   Definiert den Pfad, unter der die Protokolldateien nach der Rotation gespeichert werden. Das Archivverzeichnis und der Verzeichnisname können identisch sein.

   Dateimaske

   Hier wird eine Zeichenfolge eingegeben, die die Protokolldatei der Ereignisquelle identifiziert. In der Dateimaske können Platzhalterzeichen verwendet werden. Um beispielsweise eine Protokolldatei mit dem Namen "messages.txt" zu finden, können Sie "*messages**" eingeben.

Dateirotationstyp

Legt fest, dass die Integration mit dem Dateirotationstyp übereinstimmt, der von dem Produkt verwendet wird, von dem sie Ereignisse empfängt. Der tatsächliche Rotationstyp wird durch dieses Produkt bestimmt. Die folgenden Einstellungen werden durch CA Enterprise Log Manager-Integrationen unterstützt:

- NeueDatei: wird verwendet, wenn das Integrationsziel durch ein Hilfsprogramm wie z. B. "logrotate" rotiert wird.
- DateiGröße: wird verwendet, wenn das Integrationsziel auf einem voreingestellten Schwellenwert basiert.
- DateiAlter: wird verwendet, wenn das Integrationsziel auf einem voreingestellten Zeitraum basiert. Die Aktualisierung erfolgt normalerweise etwa um Mitternacht.

Verzeichnisname

Legt den Pfad für die Protokolldatei der Ereignisquelle fest.

Ereignisbegrenzer

Definiert den regulären Ausdruck zur Trennung einzelner Protokolleinträge in einer mehrzeiligen Protokolldatei. Jedes Mal, wenn der Protokollsensor auf das angegebene Trennzeichen stößt, beginnt er mit einem Lesevorgang zur Ermittlung neuer Ereignisse. Auf diese Weise kann CA Enterprise Log Manager mehrere Ereigniseinträge aus einer einzelnen Protokolldatei empfangen. Wenn zum Beispiel jeder Protokolldateieintrag einen eindeutigen Zeit-/Datumsstempel enthält, können Sie den regulären Ausdruck für dieses Zeitstempelformat als Trennzeichen verwenden.

4. (Optional) Klicken Sie zum Hinzufügen zusätzlicher Ereignisquellenwerte auf "Wiederholen": 

   Ein weiterer Satz von Konfigurationswerte-Feldern wird angezeigt, der es Ihnen ermöglicht, Werte für die Ereigniserfassung von einer anderen Ereignisquelle einzugeben.

5. Klicken Sie auf den entsprechenden Pfeil, der Sie zu dem Schritt im Assistenten führt, mit dem Sie fortfahren möchten, oder klicken Sie auf "Speichern und schließen".

   Wenn Sie auf "Speichern und schließen" klicken, erscheint die neue Integration in der Benutzerordnerliste, andernfalls wird der ausgewählte Schritt angezeigt.

Erstellen von Syslog-Listener

Mit dem Listener-Assistenten können Sie Syslog-Listener erstellen oder bearbeiten. Der Listener bestimmt, wie Syslog-Ereignisse an den CA Enterprise Log Manager-Server weitergeleitet werden.

Hinweis: Sie können den vordefinierten Syslog-Listener für nahezu alle Zwecke verwenden. Einige Benutzer möchten ihren Syslog-Empfang möglicherweise anpassen, indem sie benutzerdefinierte Listener verwenden. Für solche Benutzer sind die folgenden Anleitungen gedacht.

Um diese erweiterte Funktionalität vollständig zu nutzen, müssen Sie über eine umfassende Kenntnis der Quellen für Syslog-Ereignisse in Ihrem System verfügen.

Das Erstellen einer Integration umfasst folgende Schritte:

1. Öffnen des Listener-Assistenten
2. Hinzufügen von Komponenten
3. Auswählen von Unterdrückungsregeln
4. Auswählen von Zusammenfassungsregeln
5. Festlegen der Standardkonfigurationen

Weitere Informationen

Öffnen des Listener-Assistenten (siehe Seite 638)
Hinzufügen von Listener-Komponenten (siehe Seite 639)
Festlegen von Standardkonfigurationen (siehe Seite 641)
Anwenden von Unterdrückungs- und Zusammenfassungsregeln (siehe Seite 640)
Hinzufügen einer Syslog-Zeitzone (siehe Seite 643)

Öffnen des Listener-Assistenten

Öffnen Sie, um einen neuen Syslog-Listener zu erstellen, den Listener-Assistenten.

So öffnen Sie den Listener-Assistenten:

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

   Die Ordnerliste "Protokollerfassung" wird angezeigt.

2. Klicken Sie auf den Pfeil neben dem Ordner "Ereignisverfeinerungs-Bibliothek", um ihn zu erweitern, und wählen Sie dann den Ordner "Listener".

   Im Fensterbereich "Details" werden Integrationsschaltflächen angezeigt.

3. Klicken Sie auf "Neuer Listener": 

   Der Listener-Assistent wird angezeigt.

   Beachten Sie bei Verwendung des Assistenten Folgendes:

   - Klicken Sie auf "Speichern", um die Datei zu speichern, ohne den Assistenten zu schließen.
   - Klicken Sie auf "Speichern und schließen", um die Datei zu speichern und den Assistenten zu schließen.
   - Klicken Sie auf "Zurücksetzen", um die Ansicht im Assistenten auf die zuletzt gespeicherten Einstellungen zurückzusetzen.

Hinzufügen von Listener-Komponenten

Zum Erstellen eines Syslog-Listeners stellen Sie Details wie einen Namen und eine Konfigurationshilfe ein.

So fügen Sie Listener-Komponenten hinzu:

1. Öffnen Sie den Listener-Assistenten.
2. Geben Sie einen Namen für den neuen Listener ein.
3. (Optional) Wählen Sie die folgende Komponente aus der Dropdown-Liste:

   Konfigurationshilfe

   Definiert die Hilfebinärdatei für die Konfigurationshilfe, mit deren Hilfe die Integration die Verbindung zum ausgewählten Protokollspeicher herstellt. Die meisten Integrationen benötigen keine Konfigurationshilfe.

   Hinweis: Der Sensortyp für einen Listener ist immer Syslog.
4. (Optional) Geben Sie eine Beschreibung für den Listener ein.
5. Klicken Sie auf den entsprechenden Pfeil, der Sie zu dem Schritt im Assistenten führt, mit dem Sie fortfahren möchten, oder klicken Sie auf "Speichern und schließen".

   Wenn Sie auf "Speichern und schließen" klicken, wird die neue Integration in der Benutzerordnerliste angezeigt. Andernfalls wird der von Ihnen ausgewählte Schritt angezeigt.

Anwenden von Unterdrückungs- und Zusammenfassungsregeln

Sie können sowohl Unterdrückungs- als auch Zusammenfassungsregeln auf einen Syslog-Listener anwenden, um die Ereignisverfeinerung zu rationalisieren. Wenn der Listener mit einem Connector verwendet wird, werden eingehende Ereignisse anhand der angewandten Unterdrückungs- und Zusammenfassungsregeln überprüft, bevor Sie an CA Enterprise Log Manager gesendet werden.

Wenn Sie z. B. einen Listener erstellen möchten, der nur CA-Zugangskontrollereignisse empfangen soll, könnten Sie die Zugangsregel "CA-Zugangskontrolle - erfolgreiche Datei" anwenden. So vermeiden Sie überflüssige Verarbeitungsvorgänge, da nur erforderliche Regeln zur Überprüfung eingehender Ereignisse verwendet werden.

Wichtig! Erstellen und verwenden Sie Unterdrückungsregeln mit Vorsicht, da sie die Protokollierung und Anzeige bestimmter nativer Ereignisse gänzlich verhindern können. Es wird empfohlen, Unterdrückungsregeln vor ihrer Bereitstellung zunächst in einer Testumgebung zu testen.

So wenden Sie Unterdrückungs- oder Zusammenfassungsregeln an:

1. Öffnen Sie den Listener-Assistenten und fahren Sie fort mit dem Schritt "Unterdrückungsregeln" bzw. "Zusammenfassungsregeln".
2. (Optional) Geben Sie in das Eingabefeld für Regelmuster einen Begriff oder Ausdruck ein, um nach den verfügbaren Regeln zu suchen. Die Regeln, die mit Ihrer Eingabe übereinstimmen, werden beim Eingeben angezeigt.
3. Wählen Sie mit der Wechselsteuerung die von Ihnen gewünschten Regeln aus.
4. Klicken Sie auf den entsprechenden Pfeil, der Sie zu dem Schritt im Assistenten führt, mit dem Sie fortfahren möchten, oder klicken Sie auf "Speichern und schließen".

   Wenn Sie auf "Speichern und schließen" klicken, wird der neue Listener in der Liste der Benutzerordner angezeigt. Andernfalls wird der von Ihnen ausgewählte Schritt eingeblendet.

Festlegen von Standardkonfigurationen

Sie können die Datenzugriffseinstellungen für den Syslog-Listener mit Hilfe von Standardkonfigurationen steuern. Z. B. können Sie vertrauenswürdige Hosts oder Standardkommunikationsanschlüsse festlegen.

So legen Sie Standardkonfigurationen fest:

1. Öffnen Sie den Listener-Assistenten und fahren Sie fort mit dem Schritt "Standardkonfigurationen".
2. Ändern Sie oder fügen Sie die gewünschten Werte hinzu, einschließlich:

   Ereignisreihenfolge

   Stellt sicher, dass die Ereignisse in derselben Reihenfolge zum Ereignisprotokoll-Speicher gesendet werden, wie sie empfangen wurden. Wird die Ereignisreihenfolge deaktiviert, kann sie geändert werden, wenn einige Ereignisse schneller als andere analysiert und weitergeleitet werden. Wenn "Ereignisreihenfolge" aktiviert ist, kann dies aufgrund einer langsameren Ereignisbearbeitung und -übergabe die Leistung beeinflussen.

   Thread-Anzahl pro Warteschlange

   Bestimmt die Anzahl der Verarbeitungs-Threads der einzelnen Protokolle. Bei deaktivierter Ereignisreihenfolge kann die Verarbeitung mit Hilfe vieler Verarbeitungs-Threads beschleunigt werden. Wird die Ereignisreihenfolge aktiviert, hat die Anzahl der Threads keine Auswirkungen. Die Verwendung vieler Threads kann sich auf die Leistung auswirken.

   Warteschlangengröße

   Legt die Warteschlangengröße für eingehende Ereignisse als Anzahl der Ereignisse fest. Die Warteschlange dient zur Bearbeitung und Übergabe von Ereignissen. Wenn der Puffer ausgelastet ist, können erst dann weitere Ereignisse empfangen werden, wenn bearbeitete Ereignisse Platz im Puffer frei geben.

Ports

Legt die Ports fest, die der Listener verwendet, um Ereignisse über UDP oder TCP zu erfassen. Wenn Sie mehrere Ports festlegen, versucht der Dienst, sich nacheinander mit diesen Ports zu verbinden. Die Standard-Syslog-Ports sind bereits festgelegt. Wenn Sie Syslog-Ereignisse an andere Ports weitergeleitet haben, stellen Sie Ihre CA Enterprise Log Manager-Empfängerports entsprechend ein.

Wichtig! Wenn der Agent als Nicht-Root-Benutzer auf einem UNIX-System ausgeführt wird, ändern Sie die Syslog-Listener-Portnummern auf Nummern über 1024. In diesem Fall wird der Standard-UDP-Port 514 nicht geöffnet, und es werden keine Syslog-Ereignisse erfasst.

Vertrauenswürdiger Host

Gibt vertrauenswürdige IP-Adressen für IPv4 oder IPv6 an. Es werden ausschließlich Nachrichten von vertrauenswürdigen Hosts akzeptiert. Wenn Sie keinen vertrauenswürdigen Host festlegen, werden Ereignisse von allen verfügbaren Syslog-Ereignisquellen akzeptiert. Geben Sie die genaue IP-Adresse an, so wie sie im Feld "event_source_address" für vertrauenswürdige Hosts verzeichnet ist. Platzhalterzeichen oder Subnet-Adressen sind nicht zulässig.

Zeitzonen

Hier können Sie Zeitzonen für Syslog-Ereignisquellen-Computer hinzufügen. Syslog erfasst in der Regel keine Uhrzeit. Identifizieren Sie die Quellsysteme anhand der vollständigen IP-Adresse und der Zeitzone, um Ereignisse von Syslog-Quellen zu empfangen und anzupassen, die sich in einer anderen Zeitzone als der CA Enterprise Log Manager-Server befinden. Listen Sie Syslog-Quellen nicht in derselben Zeitzone auf wie den Server.

3. Klicken Sie auf den entsprechenden Pfeil, der Sie zu dem Schritt im Assistenten führt, mit dem Sie fortfahren möchten, oder klicken Sie auf "Speichern und schließen".

   Wenn Sie auf "Speichern und schließen" klicken, wird der neue Listener in der Liste der Benutzerordner angezeigt. Andernfalls wird der von Ihnen ausgewählte Schritt eingeblendet.

Hinzufügen einer Syslog-Zeitzone

Fügen Sie eine Zeitzone für ein oder mehrere Syslog-Ereignisquellencomputer ein, um Ereignisse aus Syslog-Quellen zu erfassen und korrekt anzupassen, die sich in einer anderen Zeitzone als der CA Enterprise Log Manager-Server befinden.

Eine Syslog-Zeitzone kann beim Erstellen einer Integration, bei der Konfiguration eines Connectors oder beim Erstellen einer gespeicherten Konfiguration hinzugefügt werden.

Hinweis: Beim Hinzufügen einer Zeitzone zu einer Umgebung, in der Sommerzeit gilt, müssen Sie darauf achten, dass auf dem Agentenhostrechner ein passender Eintrag für die Zeitzone vorhanden ist. Ohne diesen Eintrag kann die Syslog-Zeitzone den Wechsel zur Sommerzeit nicht verarbeiten, und für die Ereignisse wird während der Sommerzeit ein falscher Zeitstempel angezeigt.

So fügen Sie eine Syslog-Zeitzone hinzu:

1. Rufen Sie die Benutzeroberfläche für die Syslog-Zeitzone auf. Hierzu haben Sie folgende Möglichkeiten:
   - Öffnen Sie die Syslog-Integration, der Sie Zeitzonen hinzufügen möchten, und fahren Sie mit dem Schritt "Standardkonfiguration" fort.
   - Öffnen Sie den Syslog-Connector, dem Sie Zeitzonen hinzufügen möchten, und fahren Sie mit dem Schritt "Connector-Konfiguration" fort.
   - Öffnen Sie die gespeicherte Konfiguration, der Sie Zeitzonen hinzufügen möchten.

   Die Benutzeroberfläche für die Syslog-Zeitzone wird angezeigt.
2. Klicken Sie oben im Bereich "Zeitzonen" auf "Ordner erstellen".

   Im Listenbereich wird ein neuer Zeitzonenordner und im rechten Fenster eine Dropdown-Liste mit der Bezeichnung "Zeitzone" angezeigt.
3. Wählen Sie in der Dropdown-Liste eine Zeitzone aus.

   Die ausgewählte Zone wird neben dem Ordner angezeigt.
4. Klicken Sie auf den Pfeil neben dem Ordner.

   Der Ordner wird erweitert, so dass ein unbenannter Ereignisquellcomputer für diese Zeitzone angezeigt wird.
5. Wählen Sie das Computersymbol aus.

   Das Eingabefeld für die IP-Adresse wird angezeigt.

6. Geben Sie eine IP-Adresse ein.

   Die Adresse wird bei der Eingabe neben dem Computersymbol angezeigt.

7. (Optional) Um weitere Ereignisquellcomputer hinzuzufügen, wählen Sie eine vorhandene Ereignisquelle aus, und klicken Sie auf "Element hinzufügen".

   Der Ordner wird geschlossen. Öffnen Sie ihn, um einen neuen unbenannten Ereignisquellcomputer anzuzeigen. Fahren Sie mit Schritt 6 fort.

8. (Optional) Um weitere Zeitzonen hinzuzufügen, klicken Sie auf "Ordner erstellen".

   Ein neuer unbenannter Zeitzonenordner wird angezeigt. Fahren Sie mit Schritt 3 fort.

9. Wenn Sie alle gewünschten Zeitzonenordner und Elemente für Ereignisquelladressen erstellt haben, klicken Sie auf "Speichern".

Weitere Informationen

Festlegen von Connector-Konfigurationen (siehe Seite 650)
Erstellen einer gespeicherten Konfiguration (siehe Seite 655)

Erstellen von neuen Integrationsversionen

Sie können aus einer bestehenden benutzererstellten (benutzerdefinierten) Integration eine neue Version erstellen.

So erstellen Sie eine neue Integrationsversion:

1. Klicken Sie auf die Registerkarte "Verwaltung" und anschließend auf die Unterregisterkarte "Bibliothek".
2. Erweitern Sie die Ordner "Ereignisverfeinerungs-Bibliothek" und "Integrationen" und navigieren Sie zu dem Benutzerordner, der die gewünschte Integration enthält.
3. Wählen Sie die Benutzerintegration aus, und klicken Sie auf "Neue Version erstellen".
4. Der Assistent für neue Integrationen wird mit den Details der von Ihnen ausgewählten Integration angezeigt.
5. Nehmen Sie die gewünschten Änderungen vor, und klicken Sie auf "Speichern und schließen".

   Die neue Integrationsversion wird in der Liste angezeigt.

Löschen von Integrationen

Sie können eine benutzerdefinierte Integration löschen. Ein automatisches Software-Update kann nicht gelöscht werden.

So löschen Sie eine benutzerdefinierte Integration:

1. Klicken Sie auf die Registerkarte "Verwaltung" und anschließend auf die Unterregisterkarte "Bibliothek".
2. Erweitern Sie die Ordner "Ereignisverfeinerungs-Bibliothek" und "Integrationen" und wählen Sie den Benutzerordner aus, der die gewünschte Integration enthält.
3. Wählen Sie die Integration aus, die Sie aus der Liste löschen möchten.
4. Klicken Sie oben in der Liste auf "Löschen".

   Ein Bestätigungsdialogfeld wird angezeigt.
5. Klicken Sie auf "Ja".

   Die Integration wird aus der Liste entfernt.

Exportieren und Importieren der Integrationsdefinitionen

Sie können Detailinformationen zur Integration exportieren und importieren, um sie auf anderen Verwaltungsservern zu verwenden. Dies ermöglicht es Ihnen, erfolgreiche benutzerdefinierte Integrationen zwischen verschiedenen CA Enterprise Log Manager-Umgebungen bzw. von einer Test- auf eine Live-Umgebung zu übertragen.

Weitere Informationen

Integrationsdefinitionen importieren (siehe Seite 646)
Exportieren von Integrationsdefinitionen (siehe Seite 647)

Integrationsdefinitionen importieren

Sie können XML-Dateien mit Integrationsdefinitionen für die Verwendung auf dem lokalen Verwaltungsserver importieren.

So importieren Sie Integrationsdetails:

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

   Die Ordnerliste "Protokollerfassung" wird angezeigt.

2. Erweitern Sie den Ordner "Integrationen", und navigieren Sie zu dem Unterordner, in den Sie eine Integration importieren möchten.

3. Klicken Sie auf "Integration importieren".

   Das Dialogfeld "Datei importieren" wird geöffnet.

4. Geben Sie den Speicherort für die Dateien an, die Sie importieren möchten, oder suchen Sie danach, und klicken Sie auf "OK".

   Die entsprechenden Dateien werden in den aktuellen Ordner importiert, und ein Bestätigungsdialogfeld wird eingeblendet.

5. Klicken Sie auf "OK".

Exportieren von Integrationsdefinitionen

Sie können Detailinformationen zur Integration exportieren, um sie auf anderen Verwaltungsservern zu verwenden. Die exportierten Daten werden als XML-Datei gespeichert.

So exportieren Sie Integrationsdetails:

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

   Die Ordnerliste "Protokollerfassung" wird angezeigt.

2. Erweitern Sie den Ordner "Integrationen", und navigieren Sie zu dem Unterordner, der die Integration enthält, die Sie exportieren möchten.

3. Klicken Sie auf "Integrationen exportieren".

   Ein Dialogfeld für das Herunterladen wird eingeblendet.

4. Geben Sie den Speicherort für die XML-Exportdateien an, oder suchen Sie danach, und klicken Sie auf "Speichern".

   Die entsprechenden Dateien werden an dem von Ihnen gewählten Ablageort gespeichert, und ein Bestätigungsdialogfeld wird angezeigt.

5. Klicken Sie auf "OK".

Erstellen von Connectors

Sie können einen Connector erstellen, durch den Ereignisse von einer bestimmten Plattform oder einem bestimmten Gerät in Ihrer Umgebung erfasst werden. Zum Erstellen eines Connectors legen Sie eine Integration oder einen Listener als Vorlage zu Grunde und verwenden den Assistenten für neue Connectors. Jeder neue Connector wird auf einen Agenten in Ihrer Umgebung angewendet.

Sie können Connectors mit verschiedenen Typen erstellen, darunter WMI- und ODBC-Connectors, die Ereignisse des angegebenen Typs aktiv erfassen. Darüber hinaus können Sie Syslog-Connectors erstellen, die Ereignisse passiv empfangen. Syslog-Connectors können Ereignisse im Gegensatz zu anderen Connector-Typen von mehreren Quellen empfangen. Daher ist der Prozess zum Erstellen eines Syslog-Connectors nicht völlig identisch.

Das Erstellen einer Connectors beinhaltet folgende Schritte:

1. Assistenten für Connectors öffnen
2. Connector-Details hinzufügen, einschließlich Auswahl eines Listeners für Syslog-Connectors
3. Unterdrückungsregeln anwenden
4. Zusammenfassungsregeln anwenden
5. Connector-Konfigurationen festlegen

Weitere Informationen

Öffnen des Assistenten für Connectors (siehe Seite 648)
Hinzufügen von Connector-Details (siehe Seite 649)
Anwenden von Unterdrückungs- und Zusammenfassungsregeln (siehe Seite 650)
Festlegen von Connector-Konfigurationen (siehe Seite 650)

Öffnen des Assistenten für Connectors

Zum Erstellen eines neuen oder zum Bearbeiten eines vorhandenen Connectors öffnen Sie den Assistenten für Connectors.

So öffnen Sie den Assistenten für Connectors:

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

   Die Ordnerliste "Protokollerfassung" wird angezeigt.

2. Blenden Sie den Ordner "Agenten-Explorer" ein, und wählen Sie die Agentengruppe aus, der Sie einen Connector hinzufügen oder für die Sie einen Connector bearbeiten möchten.

   Die zu der von Ihnen ausgewählten Gruppe gehörenden Agenten werden angezeigt.

3. Wählen Sie den Agenten aus, für den Sie einen Connector hinzufügen oder bearbeiten möchten.

   Die Schaltflächen zur Verwaltung von Agenten werden im Detailbereich angezeigt.

4. Klicken Sie auf "Neuer Connector": 

   Der Assistent für Connectors wird angezeigt.

   Beachten Sie bei Verwendung des Assistenten Folgendes:

   - Klicken Sie auf "Speichern", um die Datei zu speichern, ohne den Assistenten zu schließen.
   - Klicken Sie auf "Speichern und schließen", um die Datei zu speichern und den Assistenten zu schließen.
   - Klicken Sie auf "Zurücksetzen", um die Ansicht im Assistenten auf die zuletzt gespeicherten Einstellungen zurückzusetzen.

Hinzufügen von Connector-Details

Zur Identifikation des Connectors können Sie diesem einen Namen und eine Beschreibung hinzufügen. Darüber hinaus müssen Sie die Integration auswählen, die Sie als Vorlage für den Connector verwenden möchten.

So fügen Sie Connector-Details hinzu:

1. Öffnen Sie den Assistenten für das Connector-Design.

   Der Assistent wird geöffnet, und die Plattform und Plattformversion für den aktuellen Agenten wird oben am Bildschirm angezeigt.

2. Geben Sie einen Namen für den Connector ein.
3. Wählen Sie das Optionsfeld "Listener" aus, falls Sie einen Syslog-Connector erstellen möchten. Für jeden anderen Typ wählen Sie das Optionsfeld "Integration" aus.
4. Wählen Sie die Integration aus, die Sie als Vorlage verwenden möchten. Die Dropdown-Liste "Integration" enthält alle verfügbaren Integrationen für die aktuelle Plattformversion und den aktuellen Ereignisquellentyp.
5. (Optional) Wählen Sie "Überprüfung der Plattformversion umgehen" aus, um Integrationen für *alle* Versionen der Agentenplattform in der Dropdown-Liste "Integration" verfügbar zu machen.
6. Geben Sie eine Beschreibung für den Connector ein.
7. Fahren Sie mit dem Schritt fort, den Sie als nächstes ausführen möchten, oder klicken Sie auf "Speichern und schließen".

   Wenn Sie auf "Speichern und schließen" klicken, wird der Connector anschließend in der Liste der Connectors angezeigt.

Anwenden von Unterdrückungs- und Zusammenfassungsregeln

Beim Erstellen oder Bearbeiten eines Connectors können Sie Unterdrückungs- und Zusammenfassungsregeln auswählen, die auf die vom Connector verarbeiteten Ereignisse angewendet werden sollen. Jede Unterdrückungs- oder Zusammenfassungsregel, die Sie hinzufügen, wird vor der Übertragung der Ereignisse an den CA Enterprise Log Manager-Server angewendet.

So wenden Sie Unterdrückungs- oder Zusammenfassungsregeln an:

1. Öffnen Sie den Assistenten "Connector-Design" und fahren Sie fort mit dem Schritt "Unterdrückungsregeln anwenden" bzw. "Zusammenfassungsregeln anwenden".

   Eine Liste der verfügbaren Unterdrückungsregeln wird angezeigt.

2. (Optional) Geben Sie in das Eingabefeld für Regelmuster einen Begriff oder Ausdruck ein, um nach den verfügbaren Regeln zu suchen. Die Regeln, die mit Ihrer Eingabe übereinstimmen, werden beim Eingeben angezeigt.

3. Wählen Sie mit Hilfe der Wechselsteuerung die Unterdrückungsregel(n) aus, die Sie anwenden möchten.

4. Fahren Sie mit dem Schritt fort, den Sie als nächstes ausführen möchten, oder klicken Sie auf "Speichern und schließen".

   Wenn Sie auf "Speichern und schließen" klicken, wird der Connector anschließend in der Liste der Connectors angezeigt.

Festlegen von Connector-Konfigurationen

Beim Erstellen oder Bearbeiten eines Connectors können Sie einzelne Konfigurationen festlegen, die bestimmen, wie der Connector Ereignisse empfängt und überträgt. Sie können die Konfigurationen entweder für jeden Connector festlegen oder gespeicherte Konfigurationen verwenden.

Gespeicherte Konfigurationen sind Sammlungen von Datenzugriffseinstellungen, die Sie wiederverwenden können. Sie können gespeicherte Konfigurationen auf mehrere Connectors anwenden.

So legen Sie Connector-Konfigurationen fest:

1. Öffnen Sie den Assistenten für das Connector-Design, und fahren Sie mit dem Schritt "Connector-Konfiguration" fort.

2. Falls Sie den Syslog-Listener/Protokollsensor aktiviert haben, wählen Sie die Integrationen aus, die dieser Connector verwenden soll.

3. Wählen Sie in der Dropdown-Liste die gewünschte gespeicherte Konfiguration aus, oder ändern Sie die angezeigten Konfigurationswerte. Connectors erben ihre Konfigurationswerte von ihrer Integration oder (im Falle von Syslog-Connectors) vom Listener.
4. (Optional) Klicken Sie auf den Link "Hilfe", um das Connector-Handbuch für die ausgewählte Integration anzuzeigen. Im angezeigten Handbuch finden Sie weitere Informationen.
5. Klicken Sie auf "Speichern und schließen".

   Der neue Connector wird in der Connector-Liste angezeigt.

Anzeigen eines Connectors

Sie können die Connector-Liste jedes Agenten öffnen, um Connectors anzuzeigen und zu bearbeiten, die mit diesem Agenten verbunden sind.

So zeigen Sie einen Connector an:

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

   Die Ordnerliste "Protokollerfassung" wird angezeigt.
2. Erweitern Sie den Agenten-Explorer und die Agentengruppenordner, um die einzelnen Agenten anzuzeigen.
3. Wählen Sie den Agenten aus, wo der Connector, den Sie anzeigen möchten, bereitgestellt ist.
4. Klicken Sie auf "Connectors anzeigen": 

   Die Liste "Agent-Connectors" mit den im ausgewählten Agenten bereitgestellten Connectors wird eingeblendet.

Anzeigen einer Connector-Anleitung

Sie können für jeden Typen von CA Enterprise Log Manager-Connector eine Anleitung mit Informationen zur Einrichtung und Konfiguration anzeigen. Die Anleitung enthält Anweisungen für die Konfiguration des Zielprodukts und des Connectors, um Ereignisse empfangen zu können.

Sie enthält außerdem Informationen, wie z. B. Connector-Protokollnamen und Angaben darüber, welche Typen von Ereignissen der Connector an CA Enterprise Log Manager überträgt.

So zeigen Sie eine Connector-Anleitung an:

1. Klicken Sie auf die Registerkarte "Verwaltung" und anschließend auf die Unterregisterkarte "Bibliothek".
2. Öffnen Sie die Ordner "Ergebnisverfeinerungs-Bibliothek", "Integrationen" und "Software-Update", um die individuellen Integrationen darzustellen.
3. Wählen Sie die Integration, die Sie für die Erstellung eines Connectors verwenden möchten.

   Im rechten Fenster erscheinen die Integrationsdetails.
4. Klicken Sie auf den blauen Hilfe-Link direkt über dem Integrationsnamen.

   Die Connector-Anleitung für diese Integration erscheint in einem neuen Browser-Fenster.

Bearbeiten von Connectors

Sie können einen vorhandenen Connector bearbeiten. Durch das Bearbeiten eines Connectors wird eine neue Version erstellt.

So bearbeiten Sie einen Connector:

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

   Die Ordnerliste "Protokollerfassung" wird angezeigt.

2. Erweitern Sie den Agenten-Explorer und die Agentengruppenordner, um die einzelnen Agenten anzuzeigen.

3. Wählen Sie den Agenten aus, wo der Connector, den Sie anzeigen möchten, bereitgestellt ist.

4. Klicken Sie auf "Connectors anzeigen": 

   Die Liste "Agent-Connectors" mit den im ausgewählten Agenten bereitgestellten Connectors wird eingeblendet.

5. Klicken Sie auf "Bearbeiten" neben dem Connector, den Sie bearbeiten möchten.

   Der Connector-Assistent öffnet sich und zeigt den ausgewählten Connector an.

6. Nehmen Sie die gewünschten Änderungen vor, und klicken Sie auf "Speichern und schließen".

   Der bearbeitete Connector wird in der Liste angezeigt.

Gespeicherte Konfigurationen

Eine gespeicherte Konfiguration ist eine wiederverwendbare Sammlung von Einstellungen, mit denen ein Connector Ereignisse von einem Gerät oder einer Protokollquelle erfassen kann. Sie können gespeicherte Konfigurationen verwenden, um einen gewissen Grad von benutzerdefinierter Anpassung zu ermöglichen, ohne dass dies eine vollkommen neue Integration erfordern würde.

Konfigurationen unterscheiden sich nach dem Integrationstyp. Beispielsweise können Sie vertrauenswürdige Hosts für einen Syslog-Connector speichern oder WMI-Serverkontaktinformationen für einen WMI-Connector.

Gespeicherte Konfigurationen ermöglichen es Ihnen, diese gruppierten Informationen beizubehalten und auf mehrere Connectors anzuwenden. Da jede gespeicherte Konfiguration mit einer bestimmten Integration verbunden ist, können Sie eine gespeicherte Konfiguration nur für die Connectors verwenden, von denen diese Integration verwendet wird.

Weitere Informationen

Erstellen einer gespeicherten Konfiguration (siehe Seite 655)
Integrations- und Connector-Aufgaben (siehe Seite 627)

Erstellen einer gespeicherten Konfiguration

Sie können eine gespeicherte Konfiguration erstellen und sie mit einer bestimmten Integration verbinden.

So erstellen Sie eine gespeicherte Konfiguration:

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

   Die Ordnerliste "Protokollerfassung" wird angezeigt.

2. Öffnen Sie den Ordner "Ereignisverfeinerungs-Bibliothek" und navigieren Sie zu der Integration, wo Sie eine gespeicherte Konfiguration erstellen möchten.

   Die Details zu der betreffenden Integration werden im Detailfenster angezeigt.

3. Klicken Sie auf "Gespeicherte Konfigurationen": 

   Die Liste gespeicherter Konfigurationen wird angezeigt.

4. Klicken Sie auf "Neu".

   Das Dialogfeld "Gespeicherte Konfigurationen" wird geöffnet, und die Standardkonfigurationswerte für die ausgewählte Integration werden angezeigt.

5. Geben Sie die gewünschten Konfigurationswerte ein, und klicken Sie auf "Speichern und schließen".

   Eine Bestätigungsmeldung wird angezeigt.

6. Klicken Sie auf "OK".

   Die gespeicherte Konfiguration wird in der Liste angezeigt.

Vorgehensweise bei der Massenkonfiguration von Connectors

Sie können Ereigniserfassungsquellen konfigurieren, indem Sie mehrere Connectors gleichzeitig erstellen. Sie haben die Möglichkeit, mehrere Connectors mit denselben Integrationseinstellungen zu erstellen und auf verschiedenen Agenten in Ihrer Umgebung bereitzustellen.

Der Konfigurationsprozess umfasst die Auswahl von Ereignisquellen, die Anwendung von Unterdrückungs- und Zusammenfassungsregeln sowie das Festlegen der Connector-Konfigurationen. Erstellen Sie vor Verwendung dieser Funktion eine Liste der benötigten Identifikationsinformationen (Hostnamen und IP-Adressen) für die Ereignisquellen, die Sie konfigurieren möchten. Diese Liste muss im CSV-Format (kommagetrennte Werte) vorliegen.

Die Konfiguration von Erfassungsquellen mit Hilfe des Assistenten zur Massenbereitstellung von Connectors umfasst folgende Schritte:

1. Öffnen des Assistenten zur Massenbereitstellung von Connectors
2. Auswählen der Details zur Quelle
3. Anwenden von Unterdrückungsregeln
4. Anwenden von Zusammenfassungsregeln
5. Konfigurieren der Connector-Einstellungen
6. Auswählen der Agenten und Zuordnen der Quellen

Weitere Informationen

Öffnen des Assistenten zur Konfiguration von Erfassungsquellen (siehe Seite 657)
Auswählen der Details zur Quelle (siehe Seite 658)
Anwenden von Unterdrückungsregeln (siehe Seite 659)
Anwenden von Zusammenfassungsregeln (siehe Seite 659)
Connector-Konfiguration (siehe Seite 660)
Auswählen der Agenten und Zuordnen der Quellen (siehe Seite 661)

Öffnen des Assistenten zur Konfiguration von Erfassungsquellen

Zur Erstellung von Connectors für Agenten können Sie den Assistenten zur Massenbereitstellung von Connectors verwenden.

So öffnen Sie den Assistenten zur Massenbereitstellung von Connectors:

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

   Die Ordnerliste "Protokollerfassung" wird angezeigt.

2. Klicken Sie auf den Ordner "Agenten-Explorer" und anschließend auf das Symbol zum Konfigurieren von Erfassungsquellen: 

   Der Assistent zur Konfiguration von Erfassungsquellen wird geöffnet.

   Beachten Sie bei Verwendung des Assistenten Folgendes:

   - Klicken Sie auf "Speichern", um die Updates zu übernehmen, ohne den Assistenten zu schließen. Eine Bestätigungsmeldung wird angezeigt.
   - Klicken Sie auf "Speichern und schließen", um die Updates zu übernehmen und den Assistenten zu schließen. Es wird keine Bestätigungsmeldung angezeigt.

Auswählen der Details zur Quelle

Wählen Sie die Details zur Quelle aus, und geben Sie an, welche Integration mit welchen Ereignisquellen verbunden werden soll. Zur Durchführung dieses Schritts benötigen Sie eine Liste mit den erforderlichen Ereignisquellendetails als CSV-Datei.

Hinweis: Die CSV-Datei enthält die für die Erstellung der Connectors benötigten Informationen. Jede Spalte in der CSV-Datei gibt ein Connector-Konfigurationsfeld an und enthält die Werte für dieses Feld. Beispielsweise können Sie eine Spalte "IP-Adresse" einrichten, in der die IP-Adressen der Hosts aufgelistet sind, von denen Sie Ereignisse erfassen möchten.

Der Abschnitt "Erstellen von Integrationen (siehe Seite 629)" enthält Informationen zu bestimmten Konfigurationsfeldern nach Protokollsensortyp.

So wählen Sie Details zur Quelle aus:

1. Öffnen Sie den Assistenten zur Massenbereitstellung von Connectors.
2. Wählen Sie aus der Dropdown-Liste "Integration" die für Ihre Quellen verwendete Integration aus.
3. Wählen Sie aus der Dropdown-Liste "Version" die Integrationsversion aus.
4. Wechseln Sie zu dem Speicherort, an dem die Erfassungsquelldatei gespeichert ist, die Sie verwenden möchten. Die Erfassungsquelle muss eine CSV-Datei sein.

   Die ersten 100 Zeilen der Erfassungsquelldatei, die Sie auswählen, werden im Bereich "Inhalt der Quelldatei" zur Überprüfung angezeigt. Die erste Zeile ist als Spaltenkopf definiert und bleibt als Spaltenkopf bestehen, auch wenn Sie den Beispielwert in Schritt 5 ändern.
5. Verwenden Sie die Dropdown-Listen "Von Zeile" und "Bis Zeile", um den zu verwendenden Teil der Erfassungsquelldatei einzugrenzen.

   Der Teil der Erfassungsquelldatei, den Sie auswählen, wird im Bereich "Inhalt der Quelldatei" zur Überprüfung angezeigt. Die Spaltenköpfe ändern sich nicht, wenn Sie für "Von Zeile" einen Wert größer 1 festlegen.
6. Fahren Sie mit dem nächsten Schritt fort.

Weitere Informationen:

Erstellen von Integrationen (siehe Seite 629)

Anwenden von Unterdrückungsregeln

Sie können auswählen, welche Unterdrückungsregeln bei der Massenkonfigurationsänderung angewendet werden sollen.

So wenden Sie Unterdrückungsregeln an:

1. Öffnen Sie den Assistenten zur Massenbereitstellung von Connectors, und fahren Sie mit dem Schritt "Unterdrückungsregeln anwenden" fort.
2. Wählen Sie mit Hilfe der Wechselsteuerung aus, welche der verfügbaren Regeln angewendet werden sollen.

   Hinweis: Sie können im Feld "Muster für Unterdrückungsregeln" nach Unterdrückungsregeln suchen.
3. Fahren Sie mit dem nächsten Schritt fort.

Anwenden von Zusammenfassungsregeln

Sie können auswählen, welche Zusammenfassungsregeln bei der Massenkonfigurationsänderung angewendet werden sollen.

So wenden Sie Zusammenfassungsregeln an:

1. Öffnen Sie den Assistenten zur Massenbereitstellung von Connectors, und fahren Sie mit dem Schritt "Zusammenfassungsregeln anwenden" fort.
2. Wählen Sie mit Hilfe der Wechselsteuerung aus, welche der verfügbaren Regeln angewendet werden sollen.

   Hinweis: Sie können im Feld "Muster für Zusammenfassungsregeln" nach Unterdrückungsregeln suchen.
3. Fahren Sie mit dem nächsten Schritt fort.

Connector-Konfiguration

Sie können die Connector-Konfigurationen für die Massenerstellung von Verbindungen festlegen. Die Konfigurationseinstellungen, die Sie in diesem Schritt vornehmen, werden von sämtlichen Connectors, die Sie erstellen, verwendet, wobei entweder die in Schritt 1 aus der CSV-Datei gesammelten Quellen oder gespeicherte Konfigurationen verwendet werden.

So legen Sie Connector-Konfigurationen fest:

1. Öffnen Sie den Assistenten zur Massenbereitstellung von Connectors, und fahren Sie mit dem Schritt "Connector-Konfiguration" fort.

   Auf der Seite werden die Quellfelder angezeigt, die Sie in Schritt 1 festgelegt haben. Jede Spaltenüberschrift in der Quelldatei wird als ein Quellfeld angezeigt. Außerdem wird auf der Seite im Bereich "Sensorkonfiguration" die standardmäßige Sensorkonfiguration für die von Ihnen ausgewählte Integration angezeigt.

2. Sie haben zwei Möglichkeiten zur Durchführung der Connector-Konfiguration:

   - Wählen Sie aus der entsprechenden Dropdown-Liste eine gespeicherte Konfiguration aus.
   - Nehmen Sie einzelne Konfigurationseinstellungen im Bereich "Sensorkonfiguration" vor, indem Sie Quellfeldeinträge in die gewünschten Eingabefelder für die Konfiguration ziehen. Führen Sie für erforderliche Felder, für die keine Quellfeldwerte vorhanden sind, manuelle Einstellungen durch.

     Nehmen Sie zum Beispiel an, Ihre Quellenliste enthält die Spalte "Benutzername". Ziehen Sie diese in das Feld "Benutzername-Sensorkonfiguration", sofern ein solches Feld für den von Ihnen konfigurierten Sensortyp existiert.

3. (Optional) Klicken Sie auf "Wiederholen", um bei Bedarf weitere Sensorkonfigurationsfelder hinzuzufügen.
4. Fahren Sie mit dem nächsten Schritt fort.

Auswählen der Agenten und Zuordnen der Quellen

Sie können die Agenten auswählen, für die Sie die konfigurierten Connectors erstellen möchten. Ordnen Sie die in Schritt 1 ausgewählten Ereignisquellen den Agenten zu, die Sie als Ziel für die Connector-Bereitstellung verwenden möchten.

So wählen Sie Agenten aus und ordnen Quellen zu:

1. Öffnen Sie den Assistenten zur Massenbereitstellung von Connectors, und fahren Sie mit dem Schritt "Agenten auswählen und Quellen zuordnen" fort.

   Auf der Seite wird entsprechend in Schritt 1 hochgeladenen Quellen eine Liste mit Quellen angezeigt. Sämtliche Quellen sind in der Reihenfolge der Zeilen nummeriert, d. h. Quelle 1 entspricht der ersten Zeile, die Sie in Ihrer Quellenliste angegeben haben.

2. Suchen Sie die zu verwendenden Agenten nach Agentengruppe, Plattform oder Agentenname.

3. Ziehen Sie die gewünschte Quelle bzw. die gewünschten Quellen auf die einzelnen Zielagentenordner, und klicken Sie, um die betreffende Connector-Zuordnung zu speichern.

4. Klicken Sie auf "Speichern" oder auf "Speichern und schließen".

   Daraufhin werden Connectors auf Basis der von Ihnen ausgewählten Quellen für die ausgewählten Agenten konfiguriert.

Aktualisierung mehrerer Connector-Konfigurationen

Sie können mehrere Connectors, die denselben Protokollsensor verwenden, aktualisieren, indem Sie eine oder mehrere Standardkonfigurationen ändern. Sie können z. B. mit Hilfe des Protokolldateisensors den Rotationstyp der Protokolldatei an mehreren Connectors ändern.

So aktualisieren Sie mehrere Connector-Konfigurationen:

1. Klicken Sie auf die Registerkarte "Verwaltung" und anschließend auf die Unterregisterkarte "Bibliothek".
2. Öffnen Sie die Ordner "Ergebnisverfeinerung", "Integrationen" und "Automatisches Software-Update".
3. Wählen Sie eine Integration, die den Protokollsensor des Typs verwendet, auf den die Konfigurationsänderungen angewendet werden sollen.
4. Klicken Sie auf "Batch-Aktualisierung auf Connectors anwenden": 

   Der Assistent "Connectors aktualisieren" erscheint und zeigt die Seite "Standardkonfigurationen" an.
5. Wählen Sie die Connectors aus, auf die Sie die Aktualisierungen anwenden möchten, und gehen Sie weiter zur Seite "Standardkonfigurationen".
6. Geben Sie den gewünschten Wert in alle Felder ein, die Sie aktualisieren möchten, und aktivieren Sie das Kontrollkästchen daneben.
7. Klicken Sie auf "Ausführen".

   Eine Bestätigungsmeldung wird angezeigt.

Kapitel 17: Ereigniskorrelation und Incident-Verwaltung

Dieses Kapitel enthält folgende Themen:

Kapitel 18: Korrelationsregelaufgaben

Korrelationsregeln können über Muster von Ereignissen berichten, die Ihnen dabei helfen, verdächtige Aktivitäten oder gefährliche Bedingungen in Ihrer Umgebung zu erkennen. Jedes Mal, wenn Kriterien der Korrelationsregel übereinstimmen, erstellt CA Enterprise Log Manager einen Incident.

Benutzer mit Administratorrolle können folgende Korrelationsregelaufgaben ausführen:

- Korrelationsregeln erstellen, bearbeiten oder löschen
- Korrelationsregelgruppen erstellen
- Korrelationsregeln importieren oder exportieren.
- Korrelationsregeln anwenden und Benachrichtigungsziele in Ihrer Umgebung zuweisen.

Dieses Kapitel enthält folgende Themen:

Informationen zu Korrelationsregeln

Sie können vordefinierte Korrelationsregeln anwenden, den Assistenten für Korrelationsregeln verwenden, um benutzerdefinierte Korrelationsregeln für Ihre Umgebung zu erstellen, oder um vorhandene Regeln zu ändern. Korrelationsregeln ermöglichen es Ihnen, Ereignisgruppen zu erkennen, die möglicherweise auf Angriffe oder auf andere Sicherheitsrisiken schließen lassen. Sie müssen die Administratorrolle besitzen, um Korrelationsregeln zu erstellen oder zu bearbeiten.

Wenn Sie eine Korrelationsregel erstellen, müssen Sie auswählen, welche der drei Typen erstellt werden soll. Die Regelvorlage steuert, welches Ereignis bzw. welche Ereignisse als Incident betrachtet werden. Es werden folgende Vorlagen bereitgestellt:

- Einfacher Filter - ermöglicht es Ihnen, nach einem einzelnen Ereignis oder Status zu suchen. Diese Vorlagen erstellen einen Incident aus einem einzelnen Ereignis.
- Zählvorlage - ermöglicht es Ihnen, nach einer Reihe von identischen Ereignissen zu suchen. Sie können steuern, nach wie vielen Ereignissen des gleichen Typs die Regel suchen soll. Jedes Mal, wenn die Regel die Anzahl der festgelegten Ereignisse erkennt, wird ein Incident ausgelöst.
- Statusübergangsvorlage - ermöglicht es Ihnen, nach einer zugehörigen Reihe an Ereignissen zu suchen. Wenn ein bestimmtes Ereignis oder ein bestimmter Status eintritt, gefolgt von einem oder mehreren anderen, erstellt die Regel einen Incident. Sie können die Status, nach denen die Regel sucht, definieren und die Anzahl an Status festlegen.

Hinweis: Eine effektive Korrelation erfordert einen klaren Überblick über anstehende Ereignisse. Aus diesem Grund sollten Sie die Anwendung von Unterdrückungs- oder Zusammenfassungsregeln auf Agentenebene eher vermeiden. Unterdrückte oder zusammengefasste Ereignisse auf Agentenebene werden für Korrelation und Incident-Erstellung nicht berücksichtigt.

Ereigniskorrelation kann erheblichen Netzwerkverkehr zur Folge haben. Aus diesem Grund ist es empfehlenswert, einen dedizierten Korrelationsserver zuzuweisen. Weitere Informationen über Serverrollen finden Sie im *CA Enterprise Log Manager-Implementierungshandbuch*.

Wenn zu viele Incident-Meldungen zur Verarbeitung durch den Korrelationsservice anstehen, behält der Service bis zu 10 000 Meldungen in der Warteschlange. Über diesen Wert hinaus eingehende Meldungen gehen verloren. Falls dies eintritt, generiert CA Enterprise Log Manager ein selbstüberwachendes Ereignis.

Weitere Informationen:

Informationen zu Incident-Benachrichtigungen (siehe Seite 673)

Verwenden von vordefinierten Korrelationsregeln

CA Enterprise Log Manager stellt eine große Anzahl an vordefinierten Korrelationsregeln für die Verwendung in Ihrer Umgebung bereit, die nach Typen oder Vorschriften angeordnet sind. Zum Beispiel finden Sie im Korrelationsregelordner der Bibliotheken-Schnittstelle einen Ordner mit dem Namen "PCI", der Regeln für verschiedene PCI-Anforderungen enthält. Sie finden auch einen Ordner mit dem Namen "Identität", der universelle Regeln bezüglich der Autorisierung und Authentifizierung enthält.

Es gibt drei Haupttypen von Regeln, von denen entweder eine oder alle in jede Kategorie eingeschlossen werden kann. Dieses Thema gibt ein Beispiel, wie jeder Regeltyp ausgewählt und angewendet wird.

Beispiel - Auswählen und Anwenden einer einfachen Regel

Einfache Korrelationsregeln erkennen, dass ein Status oder ein Vorkommnis vorhanden ist. Sie können beispielsweise eine Regel anwenden, die Sie vor Kontoerstellungsaktionen außerhalb der normalen Geschäftszeiten warnt. Bevor Sie eine Regel anwenden, sollten sie sicherstellen, dass Sie die gewünschten Benachrichtigungsziele für Ihre Umgebung erstellt haben.

So können Sie die Regel "Kontoerstellung außerhalb der normalen Geschäftszeiten" auswählen und anwenden

1. Klicken Sie auf Registerkarte "Administration" und anschließend auf die Unterregisterkarte "Bibliothek", und blenden Sie den Ordner "Korrelationsregeln" ein.
2. Blenden Sie den Ordner "PCI" und anschließend den Ordner "Anforderung 8" ein, und wählen die Regel "Erstellen eines neuen Kontos außerhalb der normalen Geschäftszeiten" aus.

   Die Regeldetails werden im rechten Fensterbereich angezeigt.
3. Überprüfen Sie die Regeldetails, um sicherzustellen, dass die Regel für Ihre Umgebung geeignet ist. In diesem Fall definieren Filter die Kontoerstellungsaktion und legen die normalen Geschäftszeiten nach Zeit und Wochentag fest.
4. (Optional) Klicken Sie oben im Fenster auf "Bearbeiten", um die bei Bedarf die Filtereinstellungen zu ändern. Zum Beispiel könnten Sie die normalen Arbeitsstunden ändern, um Ihre lokalen Spezifikationen anzupassen.

   Der Assistent für die Regelverwaltung wird geöffnet. Die Regeldetails sind bereits eingetragen.

5. Fügen Sie bei Bedarf Benachrichtigungsdetails in den Assistenten für Regelverwaltung hinzu. Benachrichtigungsdetails stellen den Meldungsinhalt bereit, der, wie in "Benachrichtigungsziele" angegeben, geliefert wird.
6. Sobald Sie die Regel fertiggestellt haben, klicken Sie im Assistenten auf "Speichern und schließen". Wenn Sie eine vordefinierte Korrelationsregel bearbeiten und speichern, erstellt CA Enterprise Log Manager automatisch eine neue Version und behält die Originalversion bei.
7. Klicken Sie auf die Unterregisterkarte "Services", und blenden Sie den Knoten "Korrelationsservice" ein.
8. Wählen Sie den Server aus, auf dem Sie die Regel anwenden möchten. Wenn Sie einen Korrelationsserver ermittelt haben, sollten Sie diesen Server auswählen.
9. Klicken Sie im Bereich "Regelkonfiguration" auf "Anwenden", und wählen Sie die neue Version der Regel "Erstellen eines neuen Kontos außerhalb der normalen Geschäftszeiten", zu der Sie das Benachrichtigungsziel zuweisen möchten, aus.
10. Klicken Sie auf "OK", um das Dialogfeld zu schließen und die Regel zu aktivieren.

Beispiel - Auswählen und Anwenden einer Zählregel

Zählkorrelationsregeln ermitteln eine Reihe von identischen Status oder Vorkommnissen. Sie können beispielsweise eine Regel anwenden, die Sie vor fünf oder mehreren fehlgeschlagenen Anmeldungen, die durch ein Administratorkonto erfolgt sind, warnt. Bevor Sie eine Regel anwenden, sollten sie sicherstellen, dass Sie die gewünschten Benachrichtigungsziele für Ihre Umgebung erstellt haben.

So können Sie die Regel "5 fehlgeschlagene Anmeldeversuche durch Administratorkonten" auswählen und anwenden

1. Klicken Sie auf Registerkarte "Administration" und anschließend auf die Unterregisterkarte "Bibliothek", und blenden Sie den Ordner "Korrelationsregeln" ein.
2. Blenden Sie den Ordner "Bedrohungsverwaltung" und anschließend den Ordner "Verdächtige Aktivitäten am Konto und bei der Anmeldung" ein, und wählen Sie die Regel "5 fehlgeschlagene Anmeldeversuche durch Administratorkonten" aus.

   Die Regeldetails werden im rechten Fensterbereich angezeigt.

3. Überprüfen Sie die Regeldetails, um sicherzustellen, dass die Regel für Ihre Umgebung geeignet ist. In diesem Fall definieren die Filter ein Administratorkonto als Benutzernamen, die zu der Schlüsselliste "Administratoren" gehört, und legt den Ereigniszähler auf 5 Ereignisse in 60 Minuten fest.
4. (Optional) Klicken Sie oben im Fenster auf "Bearbeiten", um die bei Bedarf die Filtereinstellungen zu ändern. Zum Beispiel könnten Sie in 30 Minuten den Zeitschwellenwert auf 3 Ereignisse ändern.

   Der Assistent für die Regelverwaltung wird geöffnet. Die Regeldetails sind bereits eingetragen.
5. Fügen Sie bei Bedarf Benachrichtigungsdetails in den Assistenten für Regelverwaltung hinzu. Benachrichtigungsdetails stellen den Meldungsinhalt bereit, der, wie in "Benachrichtigungsziele" angegeben, geliefert wird.
6. Sobald Sie die Regel fertiggestellt haben, klicken Sie im Assistenten auf "Speichern und schließen". Wenn Sie eine vordefinierte Korrelationsregel bearbeiten und speichern, erstellt CA Enterprise Log Manager automatisch eine neue Version und behält die Originalversion bei.
7. Klicken Sie auf die Unterregisterkarte "Services", und blenden Sie den Knoten "Korrelationsservice" ein.
8. Wählen Sie den Server aus, auf dem Sie die Regel anwenden möchten. Wenn Sie einen Korrelationsserver ermittelt haben, sollten Sie diesen Server auswählen.
9. Klicken Sie im Bereich "Regelkonfiguration" auf "Anwenden", und wählen Sie die neue Version der Regel "5 fehlgeschlagene Anmeldeversuche durch Administratorkonten", zu der Sie das Benachrichtigungsziel zuweisen möchten, aus.
10. Klicken Sie auf "OK", um das Dialogfeld zu schließen und die Regel zu aktivieren.

Beispiel - Auswählen und Anwenden einer Regel des Statusübergangs

Die Korrelationsregeln des Statusübergangs ermitteln eine Reihe an Status oder Vorkommnissen. Sie können beispielsweise eine Regel anwenden, die Sie vor fehlgeschlagenen Anmeldungen, gefolgt von einer erfolgreichen Anmeldung, die durch das gleiche Benutzerkonto erfolgt ist, warnt. Bevor Sie eine Regel anwenden, sollten sie sicherstellen, dass Sie die gewünschten Benachrichtigungsziele für Ihre Umgebung erstellt haben.

1. Klicken Sie auf Registerkarte "Administration" und anschließend auf die Unterregisterkarte "Bibliothek", und blenden Sie den Ordner "Korrelationsregeln" ein.
2. Blenden Sie den Ordner "Identität" und anschließend den Ordner "Authentifizierung" ein, und wählen Sie die Regel "Erfolgreiche Anmeldung nach fehlgeschlagenen Anmeldungen" aus.

   Die Regeldetails werden im rechten Fensterbereich angezeigt.
3. Überprüfen Sie die Regeldetails, um sicherzustellen, dass die Regel für Ihre Umgebung geeignet ist. In diesem Fall zeigt der Detailbereich die zwei Status an, die die Regel verfolgt. Der erste Status ist fünf oder mehr fehlgeschlagene Anmeldungen durch das gleiche Benutzerkonto oder die gleiche Identität. Das zweite Status ist eine erfolgreiche Anmeldung durch den gleichen Benutzer oder die gleiche Identität.
4. (Optional) Klicken Sie oben im Fenster auf "Bearbeiten", um die bei Bedarf die Statuseinstellungen zu ändern.

   Der Assistent für die Regelverwaltung wird geöffnet, und die zwei Status, aus denen die Regel besteht, werden angezeigt.
5. Doppelklicken Sie auf den Status, den Sie ändern möchten.

   Der Assistent für die Statusdefinition erscheint, und die Details des Status werden angezeigt.
6. Nehmen Sie im ausgewählten Status die gewünschten Änderungen vor, und klicken Sie auf "Speichern und schließen", um zum Assistenten für die Regelverwaltung zurückzukehren. Der erste Status überprüft beispielsweise 5 fehlgeschlagene Anmeldungen in 10 Minuten. Sie können den fehlgeschlagenen Schwellenwert der Anmeldung, die Zeit oder beide Werte ändern.
7. Fügen Sie bei Bedarf Benachrichtigungsdetails in den Assistenten für Regelverwaltung hinzu. Benachrichtigungsdetails stellen den Meldungsinhalt bereit, der, wie in "Benachrichtigungsziele" angegeben, geliefert wird.
8. Sobald Sie die Regel fertiggestellt haben, klicken Sie im Assistenten auf "Speichern und schließen". Wenn Sie eine vordefinierte Korrelationsregel bearbeiten und speichern, erstellt CA Enterprise Log Manager automatisch eine neue Version und behält die Originalversion bei.
9. Klicken Sie auf die Unterregisterkarte "Services", und blenden Sie den Knoten "Korrelationsservice" ein.
10. Wählen Sie den Server aus, auf dem Sie die Regel anwenden möchten. Wenn Sie einen Korrelationsserver ermittelt haben, sollten Sie diesen Server auswählen.

11. Klicken Sie im Bereich "Regelkonfiguration" auf "Anwenden", und wählen Sie die neue Version der Regel "Erfolgreiche Anmeldung nach fehlgeschlagenen Anmeldungen", zu der Sie das Benachrichtigungsziel zuweisen möchten, aus.
12. Klicken Sie auf "OK", um das Dialogfeld zu schließen und die Regel zu aktivieren.

Weitere Informationen:

Informationen zu Incident-Benachrichtigungen (siehe Seite 673)
Informationen zu Korrelationsregeln (siehe Seite 666)
Festlegen von Benachrichtigungsstandards (siehe Seite 676)

Verwenden von Schlüssellisten mit Korrelationsregeln

Alle Korrelationsregeln bestehen aus einem oder mehreren Filtern. Einige vordefinierte Berichtsfilter haben das Ziel, alle Werte aus einer bestimmten Tabelle zu wählen, in der ein bestimmtes Attributfeld einen Wert enthält, der als Kriterium für die Erstellung einer Schlüsselwerteliste dient.

Sie können Schlüssellisten bei der Erstellung oder Anwendung von Korrelationsregeln verwenden, um vordefinierte oder benutzerdefinierte Werte für Regelfilter anzugeben. Sie können die Schlüssellisten auch manuell oder automatisch aktualisieren, um die Listen auf dem aktuellsten Stand zu halten. Sie können Schlüssellisten mit Korrelationsregeln verwenden, ähnlich wie bei Berichten.

Weitere Informationen zu Schlüssellisten finden Sie im Kapitel "Abfragen und Berichte" dieses Handbuchs.

Weitere Informationen:

Vorbereiten auf die Verwendung von Berichten mit Schlüssellisten (siehe Seite 366)
Möglichkeiten der Verwaltung von Schlüssellisten (siehe Seite 371)
Erstellen von Schlüsselwerten für vordefinierte Berichte (siehe Seite 380)

Beispiel: Eine CSV-Datei zu Testzwecken erstellen

Dieses Beispiel veranschaulicht die Erstellung einer CSV-Datei für das Testen einer Korrelationsregel. Es soll eine Regel für eine Suche nach 5 fehlgeschlagenen Anmeldung, gefolgt von einer erfolgreichen Anmeldung, die durch einen Benutzer erfolgt sind, getestet werden.

So erstellen Sie eine CSV-Datei, um eine fehlgeschlagene Anmeldung, gefolgt von einer Erfolgsregel, zu testen

1. Melden Sie sich bei CA Enterprise Log Manager als ein Administrator an, und klicken Sie auf die Registerkarte "Abfragen und Berichte".
2. Suchen Sie nach der Abfrage "Fünf fehlgeschlagene Anmeldungen in der letzten Stunde nach Benutzer".
3. Führen Sie sie aus und zeigen Sie die Ergebnisse an. Wenn Ergebnisse vorhanden sind, fahren Sie mit dem nächsten Schritt fort. Wenn keine vorhanden sind, erstellen Sie einen Dummy-Benutzer, melden Sie sich ab und führen Sie mithilfe des neuen Dummy-Benutzers fehlgeschlagene Anmeldungen durch.
4. Exportieren Sie die Abfrage in eine CSV-Datei und öffnen Sie sie in Excel.
5. Fügen Sie nach Bedarf weitere Benutzerdetails hinzu. Fügen Sie beispielsweise Informationen hinzu, die die erfolgreiche Anmeldung wiedergeben.
6. Speichern Sie die CSV-Datei ab, wenn sie alle benötigten Ereignisinformationen enthält.
7. Öffnen Sie die zu testende Regel im Bibliotheken-Explorer, und klicken Sie im Fenster "Details" auf die Registerkarte "Regeltest".
8. Laden Sie die CSV-Datei, und bestätigen Sie, dass die entsprechenden Incidents erstellt wurden.

Informationen zu Incident-Benachrichtigungen

Sie können Benachrichtigungen festlegen, die Informationen zu einem Incident übergeben und bei der Erstellung eines Incidents automatisch ausgelöst werden. Nachdem der Incident angezeigt wurde, können die Benachrichtigungen auch manuell gestartet werden. In jedem Fall müssen Sie zunächst die Benachrichtigungsziele angeben, die Sie in Ihrer Umgebung verwenden möchten.

Sie müssen Benachrichtigungen in zwei Teilen erstellen:

1. Benachrichtigungsziel, das eine Kombination der verfügbaren Zieltypen enthalten kann. Ein Ziel kann beispielsweise E-Mail-Adressen, SNMP-Serveranmeldeinformationen und einen IT-PAM-Prozessnamen enthalten. Ziele können zu mehreren Regeln zugewiesen werden.
2. Benachrichtigungsdetails, die individuellen Regeln hinzugefügt werden und die von der Benachrichtigung gelieferte Informationen enthalten: z. B. E-Mail-Betreff und -Text, SNMP-Daten, IT-PAM-Prozessparameter.

Automatische Benachrichtigungen benötigen eine Korrelationsregel mit Benachrichtigungsdetails und ein zugewiesenes Benachrichtigungsziel. Wenn beide Komponenten vorhanden sind, wird jedes Mal, wenn die Regel einen Incident erstellt, eine automatische Benachrichtigung zum angegebenen Ziel oder zu den angegebenen Zielen gesendet. Die Kombination aus Zielen und Details ermöglicht es Ihnen, Modulbenachrichtigungen einzurichten. Zum Beispiel könnten Sie die gleichen Benachrichtigungsinformationen an unterschiedlichen regionalen Service Desks oder IT-Personal übertragen.

Sie können auch Ziele von vorhandenen Incidents zuweisen. Wenn Sie einen Incident öffnen und ein Benachrichtigungsziel zuweisen, werden die in der Regel angegebenen Benachrichtigungsdetails sofort gesendet. Die Regel muss Benachrichtigungen enthalten, um manuelle Benachrichtigungen zu senden.

Weitere Informationen:

Festlegen von Benachrichtigungsstandards (siehe Seite 676)
Informationen zu Korrelationsregeln (siehe Seite 666)

So können Sie Incidents-Benachrichtigungen entwerfen und anwenden

Sie können Benachrichtigungen für Ihre Korrelationsregeln einrichten. Benachrichtigungen ermöglichen es Ihnen, Schlüsselinformationen auf entdeckten Incidents an angegebene Mitarbeiter zu übergeben oder CA IT PAM-Service Desk-Tickets automatisch zu erstellen.

Nehmen Sie folgenden Prozess vor, um Benachrichtigungen in Ihrer Umgebung einzurichten:

1. Planen und erstellen Sie Benachrichtigungsziele.
2. Wählen Sie die vordefinierten Korrelationsregeln aus oder erstellen Sie benutzerdefinierte Regeln, die Sie in Ihrer Umgebung verwenden möchten.
3. Fügen Sie den Regeln Benachrichtigungsdetails hinzu, für die Sie Benachrichtigungen festlegen möchten.
4. Wenden Sie Korrelationsregeln auf den CA Enterprise Log Manager-Server an, und weisen Sie Benachrichtigungsziele zu.

Weitere Informationen:

Informationen zu Korrelationsregeln (siehe Seite 666)
Festlegen von Benachrichtigungsstandards (siehe Seite 676)
Hinweise zum Korrelationsservice (siehe Seite 169)

Festlegen von Benachrichtigungsstandards

Sie können Benachrichtigungsdetails in einer Regel festlegen, die Benachrichtigungsinhalte aber keine Benachrichtigungsziele angeben. Sie können beispielsweise Betreffzeile und Text der E-Mail festlegen, jedoch nicht die Lieferadressen, die durch Benachrichtigungsziele gesteuert werden. Dieses System ermöglicht es Ihnen, Standardinhalte (mithilfe von Details) einzurichten, der an verschiedene Empfänger geliefert werden kann (mithilfe von Zielen).

Sie können eine Kombination aus verfügbaren Benachrichtigungstypen in den Benachrichtigungsdetails einer einzelnen Regel einschließen.

So legen Sie Benachrichtigungsdetails fest

1. Öffnen Sie den Assistenten für Korrelationsregeln, geben Sie die erforderlichen Regeldefinitionen ein, und fahren Sie mit dem Schritt "Details zu Benachrichtigungen" fort.
2. Wählen Sie die Registerkarte "E-Mail" aus, und verwenden Sie folgende Schritte, um E-Mail-Benachrichtigungsinformationen hinzuzufügen:
   a. Geben Sie eine Betreffzeile für die E-Mail-Benachrichtigung ein.
   b. (Optional) Wenn Sie in beiden Feldern der Registerkarte "E-Mail" Text eingeben, können Sie die Drop-down-Liste "Datenfelder" und die Schaltfläche "Hinzufügen" verwenden, um Datenfeldvariablen einzufügen. Sie könnten beispielsweise "agent_address" auswählen und auf "Hinzufügen" klicken.

      "%agent_address%" wird im Textfeld angezeigt. Wenn eine Regel eine E-Mail generiert, wird der Wert des Felds "agent_address" statt der Variablen angezeigt.
   c. Geben Sie einen Nachrichtentext für die Benachrichtigungs-E-Mail ein.

      Hinweis: Der Nachrichtentext wird in HTML erstellt, so dass der gesamte Text, den Sie eingeben, in einer Zeile angezeigt wird. Um einen Zeilenumbruch zu erstellen, geben Sie am Ende der Textzeile <BR/> ein.
3. Wählen Sie die Registerkarte "Prozess" aus, und verwenden Sie folgende Schritte, um CA IT PAM-Prozessparameter hinzuzufügen:
   a. Geben Sie den Namen eines IT PAM-Prozesses ein, zu dem Sie Incident-Informationen übertragen möchten, wie z. B.:
      `/CA_ELM/EventAlertOutput`
   b. Klicken Sie auf "Parameter hinzufügen", um einen Parameter und dessen Wert anzugeben.

      Das Dialogfeld "Prozessparameter hinzufügen" wird angezeigt.

c. Geben Sie im Namensfeld ein Parameterkennwort ein, z. B. "Severity".

d. Geben Sie einen Wert an, indem Sie eine Eingabe im Wertbereich vornehmen oder ein CEG-Feld aus der Drop-down-Liste auswählen und auf "Datenfeld hinzufügen" klicken. Ereignisinformationen aus dem angegebenen CEG-Feld werden an den genannten Parameter übergeben. Wenn Sie mit dem vorherigen Beispiel fortfahren, könnten Sie "event_severity" auswählen, um den Wert des event_severity-Felds als Parameter für den IT PAM-Schweregrad anzuzeigen.

e. Wiederholen Sie Schritte a bis c, um zusätzliche Parameter und Werte nach Bedarf hinzuzufügen.

f. Wenn Sie alle CEG-Felder für den aktuellen Parameter hinzugefügt haben, klicken Sie auf "OK".

Hinweis: Sie können mehrere CEG-Felder nach Bedarf eingeben und hinzufügen, um einen Parameter zu definieren. Wenn Sie beispielsweise den Parameter "Beschreibung" für eine Benachrichtigung definieren möchten, die mit einer Regel zum Erraten der Kontoinformationen verwendet wird, könnten Sie Folgendes eingeben:

```
Dieser Incident berichtet von vier fehlgeschlagenen Anmeldungen von
%dest_identity_unique_name% auf %dest_hostname% innerhalb von 10 Minuten.
```

Die *%value%*-Struktur ist das Ergebnis aus Schritt b, in dem ein CEG-Feld ausgewählt und die Schaltfläche "Datenfeld hinzufügen" verwendet wurde.

4. Wählen Sie die Registerkarte "SNMP" aus, und verwenden Sie folgende Schritte, um SNMP-Trap-Einstellungen hinzuzufügen:

a. Stellen Sie nach Bedarf die benutzerdefinierte Trap-ID mithilfe Ihres SNMP-Übertragungsziels ein.

b. Geben Sie den Namen eines CEG-Felds ein, das Sie im Eingabebereich senden möchten. Wenn Sie Eingaben in diesem Feld vornehmen, werden verfügbare Optionen entsprechend in der Drop-down-Liste eingegrenzt.

c. Klicken Sie auf "Hinzufügen".

d. Der CEG-Feldname wird im ausgewählten Felderbereich angezeigt. Ereignisinformationen in diesem Feld werden Regeln gesendet, die diese Benachrichtigungsvorlage verwenden. Sie müssen mindestens ein CEG-Feld auswählen.

e. Wiederholen Sie die Schritte b und c, um zusätzliche CEG-Felder zu senden.

5. Klicken Sie auf den entsprechenden Pfeil, der Sie zu dem Schritt im Assistenten führt, mit dem Sie fortfahren möchten, oder klicken Sie auf "Speichern und schließen".

   Wenn Sie auf "Speichern und schließen" klicken, wird die neue Regel im entsprechenden Ordner angezeigt. Andernfalls wird der von Ihnen ausgewählte Schritt angezeigt.

Weitere Informationen:

Informationen zu Korrelationsregeln (siehe Seite 666)
Informationen zu Incident-Benachrichtigungen (siehe Seite 673)

Kapitel 19: Incident-Verwaltungsaufgaben

Ein CA Enterprise Log Manager-Incident besteht aus einem oder mehreren Ereignissen, wie sie durch eine Korrelationsregel identifiziert und verknüpft werden. Jedes Mal, wenn eine Korrelationsregel ein Ereignis oder Ereignisse entdeckt, die ihre Kriterien erfüllen, erstellt CA Enterprise Log Manager einen Incident.

Benutzer mit Administratorrolle können folgende Incident-Verwaltungsaufgaben ausführen:

- Incident-Details anzeigen, die von den Korrelationsregeln in Ihrer Umgebung erstellt wurden.
- Incident-Liste filtern oder Ergebnisbedingungen festlegen, um nach bestimmten Incidents oder Incident-Typen zu suchen, oder um Ihre Incidents-Ansicht einzugrenzen.
- Benachrichtigungsziele auf vorhandene Incidents durch Steuerung von Antworten, z. B. E-Mail-Benachrichtigungen, anwenden.
- Incident-Informationen exportieren.
- Incident-basierte Aktionsalarme planen.
- Vorhandene Incidents in einen neuen Incident einfügen.

Hinweis: Detaillierte Informationen zu Aufgaben der Incident-Verwaltung finden Sie in der *CA Enterprise Log Manager-Online-Hilfe.*

Incident-Details anzeigen

In Ihrer Umgebung können Sie Incidents-Details, einschließlich Informationen über Status, Priorität und Verlauf anzeigen. Sie können nur jene Incidents anzeigen, die an den Korrelationsserver, auf dem Sie angemeldet sind, weitergeleitet werden. Sie können steuern, wie CA Enterprise Log Manager-Server Ereignisse weiterleiten, indem Sie den Korrelationsservice konfigurieren.

So zeigen Sie Incident-Details an

1. Klicken Sie auf die Registerkarte "Incidents", wählen Sie den zu überprüfenden Incident aus, und doppelklicken Sie in der Incident-Zeile.

   Das Dialogfeld "Details" erscheint und zeigt die grundlegenden Incident-Details, einschließlich Name, Datum und Schweregrad an.

2. Ändern Sie mithilfe der entsprechenden Drop-down-Menüs die Einstellungen zu "Priorität" oder "Status".

3. (Optional) Klicken Sie auf die Registerkarte "Verlauf", um Informationen wie die Anzahl und den Zeitpunkt der Ereignisse, die dem Incident hinzugefügt wurden, oder automatisch ausgelöste Benachrichtigungen anzuzeigen.

4. Klicken Sie auf "OK" oder "Anwenden".

Weitere Informationen:

Hinweise zum Korrelationsservice (siehe Seite 169)

Kapitel 20: Agenten

Dieses Kapitel enthält folgende Themen:

Planen von Agenteninstallationen

Beim Planen einer Agenteninstallation muss der Planer bestimmen, wie viele Agenten benötigt werden und wo diese zu installieren sind. Diese Planung kann entweder von der Person, die die Agenten installiert, oder von einem Netzwerkadministrator oder Systemarchitekten durchgeführt werden.

So planen Sie Agenteninstallationen:

1. Erstellen Sie eine elektronische Version der Planungstabelle für die Agenteninstallationen, die für die Erfassung der erforderlichen Informationen geeignet ist. Hierbei könnten Sie folgende Beispieltabelle und Spaltenüberschriften verwenden:

Plattform der Ereignisquelle	Hostname oder IP-Adresse des Ausführungsortes der Ereignisquelle	Eine der folgenden: - Ohne Agent – direkt - Ohne Agent – Sammelpunkt - Agent auf Endpunkt	Hostname oder IP-Adresse des Installationsortes für den Agenten

2. Geben Sie jede Ereignisquelle an, die Ziel der Protokollerfassung sein soll, und erfassen Sie den Speicherort und die Plattform in Ihrer Agentenplanungstabelle.

3. Berücksichtigen Sie folgende Kosten und Vorteile jeder Lösung:

	Vorteil	Kosten oder Beschränkung
Ohne Agent – direkt von CA Enterprise Log Manager – kein installierter Agent	Es ist keine Agenteninstallation erforderlich.	Es ist eine Erfassung nur derjenigen Ereignisquellen möglich, die mit der Soft-Appliance-Plattform kompatibel sind. Es fallen auch Kosten für den Sammelpunkt ohne Agent an.
Ohne Agent – Agent auf Sammelpunkt	Es muss kein Agent auf dem Host installiert werden, auf dem die Ereignisquelle ausgeführt wird. Die Konsolidierung der Erfassung auf einem gemeinsamen Punkt reduziert die Anzahl der Agenten, die im Vergleich zur agentbasierten Erfassung installiert werden müssen.	Unterdrückungsregeln können nur auf dem CA Enterprise Log Manager -Server angewendet werden. Der Vorteil des geringeren Netzwerkverkehrs ist hierbei nicht vorhanden. Die Kommunikation von Ereignissen zwischen der Quelle und dem CA Enterprise Log Manager-Server ist nicht verschlüsselt. Es muss remote auf die Ereignisquelle zugegriffen werden können.
Agentbasiert – Agent auf Endpunkt	Sie können statt am CA Enterprise Log Manager-Server an der Quelle Unterdrückungsregeln anwenden. Hierdurch wird der Netzwerkverkehr zwischen dem Sammelpunkt und dem CA Enterprise Log Manager-Server reduziert. ie Kommunikation von Protokollen zwischen der Quelle und dem CA Enterprise Log Manager-Server ist verschlüsselt. Unter den drei Lösungen kann diese Lösung die größte Anzahl von Ereignissen verarbeiten.	Am Ausführungsort der Ereignisquelle muss ein Agent installiert werden.

4. Erfassen Sie Ihre bevorzugte Lösung für jede Ereignisquelle.

5. Sortieren Sie die Agentenplanungstabelle nach Spalte 3 und anschließend nach Spalte 2. Hierdurch werden alle agentbasierten Ereignisquellen, die auf demselben Host ausgeführt werden, in Blöcken angezeigt.
6. Suchen Sie für Ereignisquellen, die Sie der agentbasierten Lösung zugeordnet haben, nach dem ersten Vorkommen in einem Block mit identischem Namen, und kopieren Sie diese Daten von Spalte 2 in Spalte 4. Auf diese Weise wird nur ein Eintrag für jeden Host erstellt, auf dem eine oder mehrere Ereignisquellen ausgeführt werden. (Für einen bestimmten Host benötigen Sie unabhängig von der Anzahl der Ereignisquellen niemals mehr als einen Agenten.)
7. Planen Sie für Ereignisquellen, die Sie der Lösung "Ohne Agent – Agent auf Sammelpunkt" zugeordnet haben, an welchen Orten Agenten installiert werden sollen. Gehen Sie dazu wie folgt vor:
    a. Ermitteln Sie die Anzahl der Sammelpunkte, die benötigt werden, um die als Kandidaten für Remote-Agenten ermittelten Ereignisquellen aufzunehmen.
    b. Planen Sie durch einen gemeinsamen Speicherbereich im Netzwerk Gruppierungen von Ereignisquellen, die Sie als Kandidaten für Remote-Agenten ermitteln.
    c. Ermitteln Sie für jede Gruppe von Ereignisquellen den Server, der als Sammelpunkt verwendet werden soll. Hierbei kann es sich um einen dedizierten Server handeln. Halten Sie Ihre Entscheidung in Spalte 4 fest.
8. Falls Sie Ereignisquellen erfasst haben, für die keine zugeordnete Lösung vorhanden ist, und Sie mit einem älteren CA-Adapter arbeiten, finden Sie nähere *Details im Implementierungshandbuch von CA Enterprise Log Manager*.
9. Übergeben Sie die Daten, die Sie in der vierten Spalte der Agentenplanungstabelle erfasst haben, an den Benutzer, der die Agenten installieren wird.

Planen von Agentenkonfigurationen

Der Benutzer "EiamAdmin" installiert Agenten basierend auf der Festlegung der besten Erfassungsmethode. Folgende Methoden wurden bewertet:

- Protokollerfassung ohne Agent direkt vom CA Enterprise Log Manager-Server, auch direkte Erfassung genannt.
- Protokollerfassung ohne Agent von einem Erfassungspunkt aus.
- Agentenbasierte Protokollerfassung vom Host, auf dem die Ereignisquelle ausgeführt wird.

Bei der Analyse, die der Installation vorangeht, werden eventuell einige Informationen ermittelt, die der Administrator benötigt, der die Agenten und Connectors konfiguriert.

Der erste Schritt bei der Agentenkonfiguration besteht darin, von "EiamAdmin" die Agentenplanungstabelle oder das Alternativdokument zu erhalten, in dem der Installationsort der Agenten dokumentiert ist. Nach der Konfiguration des erstens Administrators stellt der Benutzer "EiamAdmin" dem Administrator das mit Anmerkungen versehene Arbeitsblatt zur Planung der Agenteninstallation zur Verfügung. Der erste Administrator wiederum plant die für die einzelnen Agenten erforderlichen Connectors, bevor er mit der Konfiguration beginnt.

Der Administrator führt die Konfiguration für jeden von "EiamAdmin" installierten Agenten durch. Darüber hinaus konfiguriert der Administrator unabhängig von der Erfassungsmethode ("Ohne Agent – direkt", "Ohne Agent – Sammelpunkt" oder "Agentbasiert") für jede Ereignisquelle einen Connector. Der Administrator konfiguriert Connectors auf jedem Agenten und ist dabei bei dem CA Enterprise Log Manager-Server angemeldet, der die von diesem Agenten erfassten Ereignisse empfangen soll.

Hinweis: Je weniger Connectors auf einem Agenten konfiguriert sind, desto besser ist die Performance.

Eine Ausnahme dieses Prozesses bildet die Situation, in der die Agenteninstallation automatisch ausgeführt wird. In diesem Fall werden die Connectors vom Installationsprogramm konfiguriert. Die auf einem Agenten konfigurierten Connectors ermöglichen es dem Agenten, Rohereignisse von spezifischen Ereignisquellen zu erfassen. Die Connectors übersetzen Rohereignisse in verfeinerte Ereignisse und übertragen die verfeinerten Ereignisse an CA Enterprise Log Manager.

Die Erstellung von Agentengruppen ist optional. Werden keine benutzerdefinierten Agentengruppen erstellt, werden die Agenten der Standard-Agentengruppe zugewiesen. Administratoren erstellen Agentengruppen aus folgenden Gründen:

- um die Berichterstellung von Ereignissen zu ermöglichen, die von Agenten in derselben Agentengruppe erfasst wurden
- um die Zuweisung eines anderen administrativen Benutzers zu anderen Agentengruppen zu ermöglichen (der Benutzerzugriff kann durch Zugriffsrichtlinien auf bestimmte Agentengruppen beschränkt werden)

Die erfassten Ereignisprotokolle werden zur Verarbeitung und anfänglichen Speicherung an einen CA Enterprise Log Manager-Server gesendet. Administratoren müssen den Server, der Protokolle empfangen soll, für jeden Agenten beziehungsweise jede Agentengruppe konfigurieren. Durch eine Zuweisung eines Servers zu einer Agentengruppe können Sie diesen Server schnell allen Agenten in der Agentengruppe zuweisen.

Planen einer direkten Protokollerfassung

CA Enterprise Log Manager wird mit einem Standardagenten installiert, der für die direkte Protokollerfassung verwendet werden kann. Dieser Vorgang wird als direkte Erfassung bezeichnet, weil für die Nutzung des Standardagenten keine Agenteninstallation erforderlich ist. Der Standardagent kann Ereignisse von nahezu jeder Ereignisquelle erfassen. Hierbei gelten folgende Beschränkungen:

- Der Protokollsensor muss auf der Soft-Appliance ausgeführt werden können. Manche Protokollsensoren, zum Beispiel der WMI-Protokollsensor, sind an eine spezifische Plattform gebunden.
- Es muss remote auf die Ereignisquelle zugegriffen werden können.

Sie konfigurieren den Standardagenten genauso wie einen separat installierten Agenten. Die direkte Protokollerfassung durch den Standardagenten eignet sich ideal für sehr kleine Systeme.

Ereignisquellen für die direkte Protokollerfassung

CA Enterprise Log Manager stellt Protokollsensoren bereit, die auf dem CA Enterprise Log Manager-Server ausgeführt werden, um die agentenlose direkte Protokollerfassung zu vereinfachen. Ab der Veröffentlichung dieses Dokuments werden folgende Sensoren unterstützt:

- Syslog
- WinRM
- ODBC
- TIBCO

So bestimmen Sie die vom Standardagenten unterstützten Integrationen:

1. Klicken Sie im Agenten-Explorer auf die Registerkarte "Verwaltung", und wählen Sie auf der Unterregisterkarte "Protokollerfassung" einen CA Enterprise Log Manager-Server aus.
2. Klicken Sie auf "Neuen Connector erstellen".

Die Dropdown-Liste "Integration" enthält die Integrationen, aus denen Sie einen Connector zur Bereitstellung für den Standardagenten erstellen können. Jede Integration, auf der Connectors basieren, ist auf das Abrufen von Ereignissen von einer spezifischen Ereignisquelle ausgelegt.

Eine vollständige Liste der unterstützten Protokollsensoren und Integrationen finden Sie unter Support auf der Seite zum CA Enterprise Log Manager-Produkt.

Hinweis: Ein Protokollsensor ist eine Integrationskomponente, die Daten aus einem bestimmten Protokolltyp lesen soll, wie z. B. aus Datenbank, Syslog, Datei oder SNMP.

Planen einer Protokollerfassung ohne Agent

Die Protokollerfassung ohne Agent kann implementiert werden, indem ein Agent auf einem Erfassungsserver installiert wird, der Ereignisse von mehreren Remote-Ereignisquellen erfasst.

Berücksichtigen Sie bei der Planung der Konfiguration der Protokollerfassung ohne Agent auf einem Erfassungsserver folgende Punkte:

- Je weniger Connectors auf einem Agenten bereitgestellt werden, desto besser ist die Performance.
- Wie hoch die maximale Anzahl von Connectors ist, die Sie auf einem bestimmten Agenten konfigurieren sollten, hängt davon ab, ob der Agent auf einem dedizierten Server installiert ist, wie leistungsfähig dieser Server ist und auf welche Arten von Ereignisquellen Sie abzielen. Als Faustformel gilt, dass Sie auf einem Agenten wahrscheinlich nicht mehr als 40 oder 50 Connectors konfigurieren sollten.
- Eine Gruppierung von Connectors desselben Typs, die auf verschiedenen Agenten desselben Erfassungsservers konfiguriert sind, bietet keinen Performance-Vorteil. Ebenso weist die Weiterleitung von Ereignissen von identischen Ereignisquellentypen an einen bestimmten CA Enterprise Log Manager-Server in einer Föderation keine Performance-Vorteile auf.

Planen einer agentbasierten Protokollerfassung

Nachdem ein Agent mit Hilfe eines Agenteninstallationsprogramms auf einem Server mit lokalen Ereignisquellen installiert wurde, konfigurieren Administratoren auf diesem Agenten einen Connector für jede lokal ausgeführte Ereignisquelle.

Falls viele Zielserver mit identischem Ereignisquellentyp vorhanden sind, sollten Sie diese Zielserver in einer Agentengruppe zusammenfassen und die Konfiguration auf der Ebene der Agentengruppe ausführen.

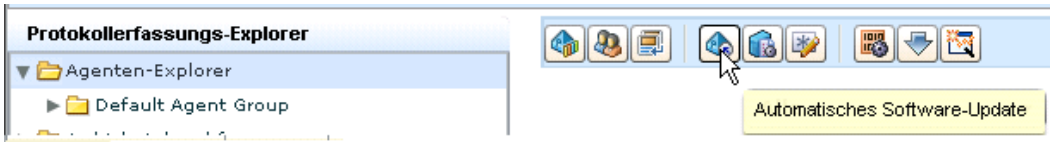
Die garantierte Übermittlung kann für die direkte Erfassung von Syslogs ein Problem darstellen. Um dem entgegenzuwirken, konfigurieren Sie einen Syslog-Listener auf einem mit der Syslog-Ereignisquelle installierten Agenten.

Wählen der Konfigurationsebene

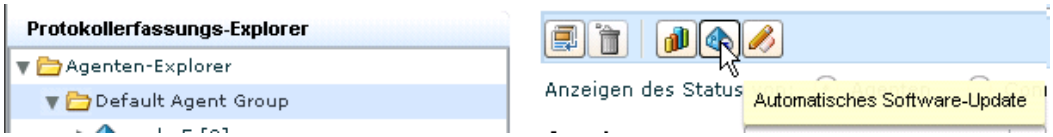
Die Optionen "Automatisches Software-Update", "Unterdrückungsregeln anwenden" und "Status und Befehl" können von verschiedenen Ebenen ausgewählt werden. Beispielsweise kann die Konfiguration "Automatisches Software-Update" von folgenden Ebenen aus gestartet werden:

- Agenten-Explorer
- Die Standard-Agentengruppe oder eine benutzerdefinierte Agentengruppe.
- Agent

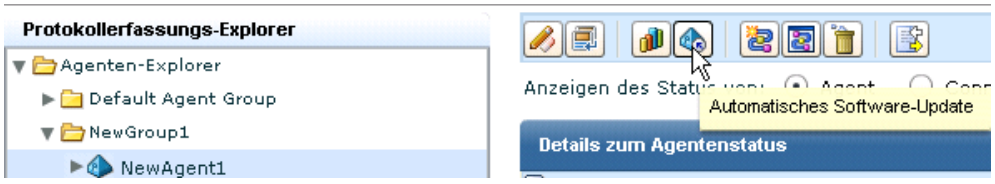
Um eine Option so zu konfigurieren, dass Sie für alle Agenten in allen Gruppen gilt, wählen Sie "Agenten-Explorer" und klicken dann auf die Schaltfläche der Aktion, die Sie durchführen möchten.



Um eine Option so zu konfigurieren, dass Sie für alle Agenten in einer bestimmten Gruppe gilt, wählen Sie den Gruppennamen und klicken dann auf die Schaltfläche der Aktion, die Sie durchführen möchten.



Um eine Option so zu konfigurieren, dass Sie nur für einen Agenten gilt, wählen Sie den Agenten und klicken dann auf die Schaltfläche der Aktion, die Sie durchführen möchten.



Agenten-Management-Aufgaben

Mit dem Agenten-Explorer können Sie die Ereigniserfassungsagenten in Ihrer Umgebung anzeigen und verwalten. Sie können in der Benutzeroberfläche für den Agenten-Explorer Management-Aufgaben in folgenden Bereichen durchführen:

- Agentenkonfiguration: Hiermit können Sie Agenten umbenennen und ihre zugehörigen sowie die verknüpften Gruppen konfigurieren.
- Agentengruppen: Hiermit können Agenten z. B. nach Gebiet, geschäftlicher Wichtigkeit oder Ereignisquelltyp gruppieren. Sie können gruppierte Agenten bei Bedarf auch verschiedenen CA Enterprise Log Manager-Servern zuordnen.
- Automatische Software-Updates: Hiermit können Sie verfügbare Updates für Agenten anzeigen und anwenden.
- Agentenbefehl und Status: Hiermit können Sie den aktuellen Status der Agenten anzeigen und sie nach Ihren Erfordernissen starten und stoppen.

Weitere Informationen

Herunterladen der Binärdateien des Agenten (siehe Seite 692)
Aktualisieren des Agentauthentifizierungsschlüssels (siehe Seite 691)
Erstellen von Agentengruppen (siehe Seite 701)
Anwenden automatischer Software-Updates (siehe Seite 711)
Konfigurieren der Agentenverwaltung (siehe Seite 704)

Aktualisieren des Agentauthentifizierungsschlüssels

Sie können den von den Agenten zur Registrierung für den CA Enterprise Log Manager-Server verwendeten Schlüssel anzeigen und aktualisieren. Durch Ändern dieses Schlüssels kann verhindert werden, dass nicht autorisierte Agenten in Ihrer Umgebung installiert werden. Standardmäßig wird für alle CA Enterprise Log Manager-Server in allen Anwendungsinstanzen derselbe Schlüssel verwendet. Sie können jedoch auch festlegen, dass für jede Anwendungsinstanz ein anderer Schlüssel verwendet wird.

Das Agenteninstallationsprogramm muss diesen Agentenschlüssel im Installationsassistenten als Authentifizierungscode eingeben.

So aktualisieren Sie den Authentifizierungsschlüssel des Agenten:

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

   Die Ordnerliste "Protokollerfassung" wird angezeigt.

2. Klicken Sie auf den Ordner "Agenten-Explorer".

   Die Schaltflächen zur Verwaltung von Agenten werden im Detailbereich angezeigt.

3. Klicken Sie auf "Authentifizierungsschlüssel des Agenten" 

   Das Fenster "Authentifizierungsschlüssel des Agenten" wird angezeigt.

4. Geben Sie in die Felder zur Schlüsseleingabe und -bestätigung einen neuen Schlüssel ein, und klicken Sie auf "Speichern".

   Es wird eine Meldung angezeigt, dass die Bestätigung erfolgreich war.

Herunterladen der Binärdateien des Agenten

Sie können die Binärdateien des Agenten herunterladen und ohne weitere Installationsmedien auf Ihrem lokalen Computer installieren.

Weitere Informationen zum Installieren eines Agenten finden Sie im *CA Enterprise Log Manager-Agent-Installationshandbuch*.

So laden Sie Binärdateien des Agenten herunter:

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

   Die Ordnerliste "Protokollerfassung" wird angezeigt.

2. Klicken Sie auf den Ordner "Agenten-Explorer".

   Im Detailfenster werden Schaltflächen für die Agentenverwaltung angezeigt.

3. Klicken Sie auf "Binärdateien des Agenten herunterladen". 

   Die Liste der Binärdateien des Agenten wird mit den verfügbaren Agenten und ihren aktuellen Versionen angezeigt.

4. Klicken Sie auf den Agenten, den Sie herunterladen möchten.

   Das Dialogfeld zum Herunterladen wird angezeigt.

5. Wählen Sie den gewünschten Speicherort für die Binärdatei des Agenten aus, und klicken Sie auf "Speichern".

   Die Datei wird an dem von Ihnen ausgewählten Speicherort gespeichert, und eine Bestätigungsmeldung wird angezeigt.

Agenten konfigurieren

Sie können einen installierten und registrierten Agenten konfigurieren, nachdem Sie ihn im Agenten-Explorer geöffnet haben.

So konfigurieren Sie Agenten:

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

   Die Ordnerliste "Protokollerfassung" wird angezeigt.

2. Klicken Sie auf den Ordner "Agenten-Explorer".

   Der Ordner öffnet sich und zeigt die Ordner der Agentengruppe an.

3. Wählen Sie den Agenten, den Sie konfigurieren möchten, und klicken Sie oben im Fenster auf "Bearbeiten".

   Die Agentendetails werden im Detailfenster angezeigt.

4. Nehmen Sie die gewünschten Änderungen vor, einschließlich folgender:

   Benutzername

   Definiert den Benutzernamen, unter dem der Agent ausgeführt wird.

   Port

   Legt den Port fest, den der Agent für die Kommunikation mit CA Enterprise Log Manager verwendet.

   Agentengruppe

   Legt die Gruppe fest, der der Agent angehört.

   Maximale Anzahl an Dateien

   Legt die maximale Anzahl von Dateien fest, die in der Ereignisempfang-Dateiwarteschlange erstellt werden können. Der höchste erlaubte Wert sind 1000 Dateien.

   Maximale Größe pro Datei (MB)

   Legt für die einzelnen Dateien in der Ereignisempfang-Dateiwarteschlange die maximale Größe in MB fest. Wenn eine Datei die maximale Größe erreicht, erstellt CA Enterprise Log Manager eine neue Datei. Der höchste erlaubte Wert ist 2048 MB.

Modus zum Senden von Ereignissen

Legt fest, welche der folgenden Übertragungsarten der Agent verwendet:

- Failover - Der Agent sendet Ereignisse an den ersten Server der Liste "Protokollmanager-Server". Falls die Kommunikation unterbrochen wird, versucht er so lange, mit den Servern der Liste zu kommunizieren, bis die Kommunikation wieder hergestellt ist.
- Round-Robin - Der Agent sendet Ereignisse der Reihe nach an die einzelnen Server in der Liste "Protokollmanager-Server" und versucht, nach einer Stunde den nächsten Server in der Liste zu kontaktieren. Dieser Zeitraum ist nicht konfigurierbar.

Aktivieren von Ereignisverschlüsselung

Legt den Agenten so fest, dass er AES128 zur Verschlüsselung der Ereignisse verwendet, die er überträgt. Das Aktivieren der Ereignisverschlüsselung wirkt sich auf die Leistung aus.

Versandplanung aktivieren

Legt den Agenten so fest, dass er Ereignisse nur innerhalb einer bestimmten Zeitspanne sendet. Wenn Sie das Kontrollkästchen "Versandplanung aktivieren" auswählen, werden die Felder "Startzeit" und "Endzeit" angezeigt. Beachten Sie bei der Eingabe der GMT-Zeitwerte, die Sie im 24-Stunden-Format haben möchten, folgende Bedingungen:

- Zwischen den Werten für die Start- und Endzeit muss mindestens eine Stunde liegen.
- Falls der Wert der Startzeit höher ist als der Wert der Endzeit, wird die Endzeit auf den Tag festgelegt, der auf den der Startzeit folgt. Falls Sie die Startzeit beispielsweise auf 23 festlegen und die Endzeit auf 6, läuft die Übertragungszeitspanne von 23:00 Uhr GMT bis 06:00 Uhr GMT des folgenden Tages.

Ersetzen der IP-Adresse mit dem Hostnamen

Legt fest, dass der Agent die IP-Adresse einer Ereignisquelle mit dem Hostnamen der Ereignisquelle ersetzt. Alle Connectors innerhalb des Agenten erben diese Funktion. Falls Sie diese Funktion für alle Agenten Ihrer Umgebung aktivieren möchten, konfigurieren Sie die Agenten jeweils einzeln. Falls Sie diese Funktion aktivieren, ersetzt CA Enterprise Log Manager die IP-Adresse mit dem Hostnamen für folgende CEG-Felder:

- source_hostname
- dest_hostname
- agent_hostname
- event_source_hostname
- receiver_hostname

Protokollmanager-Server

Steuert die CA Enterprise Log Manager-Server, an die der Agent die Ereignisse leitet, sowie die Reihenfolge, in der sie kontaktiert werden. Sie können die Wechselsteuerung verwenden, um verfügbare Server auszuwählen, sowie die Pfeiltasten rechts von den ausgewählten Servern, um die Kommunikationspriorität einzustellen.

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.

5. Klicken Sie auf "Speichern".

Weitere Informationen

Erstellen von Agentengruppen (siehe Seite 701)

Handhabung von manipulierten Dateien

Agenten verwenden bei der Ausführung eine im Speicher gespeicherte Konfigurationsdatei. Wird eine Konfigurationsdatei während der Ausführung eines Agenten manipuliert, verwendet der Agent die manipulierte Datei nicht. Wenn ein Agent vom CA Enterprise Log Manager-Server eine neue Konfiguration erhält, ersetzt er die Datei auf der Festplatte vor dem Neustart durch die erhaltene Datei. Auf diese Weise wird die manipulierte Datei automatisch durch die richtige Datei ersetzt.

Falls die Datei von jemandem manipuliert wird, der den Agenten anschließend von einer externen Quelle neu startet, erkennt der Agent, dass die Datei manipuliert wurde, und wird beendet. Der Agent übernimmt keine Konfigurationsdaten aus der manipulierten Datei, auch nicht aus der CA Enterprise Log Manager-Serverliste.

Im Agenten-Explorer wird angezeigt, dass der Agent nicht antwortet. Setzen Sie die Agentenkonfiguration mit Hilfe der Status- und Befehlstools des CA Enterprise Log Manager-Server zurück. Anschließend funktioniert der Agent wieder ordnungsgemäß.

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

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
   ```

   Hinweis: Beim Aktualisieren der Konfiguration eines Agenten benötigt CA Enterprise Log Manager maximal 5 Minuten, um den aktualisierten Status dieses Agenten mit den anderen Agenten in einer Föderation zu synchronisieren.
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".

Erstellen von Agentengruppen

Sie können eine Agentengruppe erstellen, um ihre Agenten nach Ort, Betriebssystem oder nach einer anderen passenden Kategorie zu sortieren. Für die Erstellung einer Agentengruppe mit dem Agentengruppenassistenten müssen folgende Schritte durchgeführt werden:

1. Öffnen des Assistenten für Agentengruppen
2. Eingeben von Gruppendetails
3. Hinzufügen von Agenten

Weitere Informationen

Öffnen des Assistenten für Agentengruppen (siehe Seite 701)
Hinzufügen von Agentengruppendetails (siehe Seite 702)

Öffnen des Assistenten für Agentengruppen

Um eine Agentengruppe zu erstellen oder eine vorhandene zu bearbeiten, müssen Sie den Assistenten für Agentengruppen öffnen.

So öffnen Sie den Assistenten für Agentengruppen:

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

   Die Ordnerliste "Protokollerfassung" wird angezeigt.

2. Klicken Sie auf den Ordner "Agenten-Explorer".

   Im Detailfenster werden Schaltflächen für die Agentenverwaltung angezeigt.

3. Klicken Sie auf "Neue Agentengruppe": 

   Der Assistent für Agentengruppen wird geöffnet.

   Beachten Sie bei Verwendung des Assistenten Folgendes:

   - Klicken Sie auf "Speichern", um die Datei zu speichern, ohne den Assistenten zu schließen.
   - Klicken Sie auf "Speichern und schließen", um die Datei zu speichern und den Assistenten zu schließen.
   - Klicken Sie auf "Zurücksetzen", um die Ansicht im Assistenten auf die zuletzt gespeicherten Einstellungen zurückzusetzen.

Hinzufügen von Agentengruppendetails

Sie können identifizierende Details zu Ihrer Agentengruppe hinzufügen.

Hinzufügen von Agentengruppendetails

1. Öffnen Sie den Assistenten für Agentengruppen.
2. Geben Sie den Namen der Gruppe und eine optionale Beschreibung zu Referenzzwecken ein.
3. Wählen Sie den Modus zum Senden von Ereignissen aus.
4. (Optional) Geben Sie die ersten Buchstaben des Servers ein, den Sie in das Feld "Namensmuster" eingeben möchten.

   Server, die mit Ihren Suchbegriffen übereinstimmen, werden im Bereich "Verfügbar" angezeigt.
5. Wählen Sie die Server, die Sie über die Wechselsteuerung hinzufügen möchten, aus, und ordnen Sie sie mithilfe der Nach-oben- und Nach-unten-Pfeile in der Reihenfolge an, in der sie in der Agentengruppe angezeigt werden sollen.
6. Gehen Sie weiter zum nächsten Schritt, oder klicken Sie auf "Speichern und schließen".

   Wenn Sie auf "Speichern und Schließen" klicken, wird die Gruppe erstellt. Andernfalls wird der ausgewählte Schritt angezeigt.

Hinzufügen von Agenten zu einer Agentengruppe

Sie können Agenten zu Administrationszwecken zu Ihrer Agentengruppe hinzufügen. Sie können beispielsweise Gruppen nach geografischer Region oder Betriebssystem erstellen.

Hinweis: Die Eigenschaften einer Agentengruppe gelten für alle Agenten dieser Agentengruppe.

So fügen Sie einer Gruppe Agenten hinzu:

1. Öffnen Sie den Assistenten für Agentengruppen, und gehen Sie weiter zum Schritt "Agenten".
2. (Optional) Wählen Sie ein Agentensuchkriterium. Wenn Sie keine Suchbegriffe eingeben, werden alle Agenten angezeigt. Sie können unter den folgenden Kriterien wählen, um die Suche einzugrenzen:
   - 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
   - Agentennamensmuster: Gibt nur die Agenten zurück, die das angegebene Muster enthalten
3. Klicken Sie auf "Suchen".

   Agenten, die mit Ihren Suchbegriffen übereinstimmen, werden im Bereich "Verfügbare Agenten" angezeigt.
4. Wählen Sie die Agenten, die Sie über die Wechselsteuerung hinzufügen möchten, aus, und ordnen Sie sie mithilfe der Nach-oben- und Nach-unten-Pfeile in der Reihenfolge an, in der sie in der Agentengruppe angezeigt werden sollen.

   Hinweis: Sie können Agenten nicht in eine Agentengruppe verschieben, für die keine CA Enterprise Log Manager-Sever konfiguriert wurden.
5. Klicken Sie auf "Speichern und schließen".

   Die Agentengruppe wird in der Liste angezeigt.

Hinweis: Wenn Sie eine vom Benutzer erstellte Agentengruppe löschen, werden die Agenten innerhalb dieser Agentengruppe in die Standard-Agentengruppe verschoben, und die Agenten erben die Eigenschaften der Standard-Agentengruppe.

Konfigurieren der Agentenverwaltung

Sie können Ihre Agenten oder Agentengruppen so konfigurieren, dass sie an verschiedene CA Enterprise Log Manager-Server in Ihrer föderierten Umgebung berichten. Damit können Sie Gruppen oder Agenten so konfigurieren, dass sie Ereignisdaten an die ausgewählten CA Enterprise Log Manager-Server senden.

Die Konfiguration des Agenten-Managements im Assistenten für Protokollmanager-Server umfasst folgende Schritte:

1. Öffnen des Assistenten für Protokollmanager-Server
2. Auswählen der Agenten- oder Agentengruppenziele zur Zuweisung.
3. Auswählen der CA Enterprise Log Manager-Server, die den Agenten oder Gruppen zugewiesen werden sollen

Weitere Informationen

Öffnen des Assistenten für Protokollmanager-Server (siehe Seite 705)
Auswählen von Zielagenten (siehe Seite 706)
Auswählen von Protokoll-Managern (siehe Seite 707)

Öffnen des Assistenten für Protokollmanager-Server

Um Agenten- oder Agentengruppenzuweisungen zu konfigurieren, öffnen Sie den Assistenten für Protokollmanager-Server.

So öffnen Sie den Assistenten für Protokollmanager-Server:

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

   Die Ordnerliste "Protokollerfassung" wird angezeigt. Im Detailfenster werden die Schaltflächen für das Agenten-Management angezeigt.

2. Klicken Sie auf "Protokollmanager-Server" 

   Der Assistenten für die Zuweisung von Protokollmanager-Servern wird angezeigt.

   Beachten Sie bei Verwendung des Assistenten Folgendes:

   - Klicken Sie auf "Speichern", um ihre Daten zu speichern, ohne den Assistenten zu schließen.
   - Klicken Sie auf "Speichern und schließen", um die Zuordnung zu speichern und den Assistenten zu schließen.
   - Klicken Sie auf "Zurücksetzen", um die Ansicht im Assistenten auf die zuletzt gespeicherten Einstellungen zurückzusetzen.

Weitere Informationen

Konfigurieren der Agentenverwaltung (siehe Seite 704)
Auswählen von Zielagenten (siehe Seite 706)
Auswählen von Protokoll-Managern (siehe Seite 707)

Auswählen von Zielagenten

Um Agenten einem Server zur Ereignisannahme und Archivierung von Prozessen zuzuordnen, müssen Sie auswählen, welcher Agent oder welche Gruppe dem jeweiligen CA Enterprise Log Manager-Server zugewiesen werden soll.

So wählen Sie Zielagenten aus:

1. Öffnen Sie den Assistenten für Protokollmanager-Server.
2. Wählen Sie aus, ob die Agenten nach Gruppen oder einzeln zugewiesen werden sollen.
3. Wenn Sie "Gruppen" wählen, sollten Sie zur Zuweisung der zuzuordnenden Gruppen die Wechselsteuerung verwenden. Zur Suche nach Gruppen können Sie im Sucheingabefeld einen Teil des Namens eintippen. Die verfügbaren Gruppen werden beim Eintippen gefiltert.
4. Wenn Sie "Agenten" wählen, sollten Sie zur Zuweisung der zuzuordnenden einzelnen Agenten die Wechselsteuerung verwenden. Zur Suche nach Agenten können Sie die Dropdown-Listen für Agentengruppen und Plattformen sowie das Sucheingabefeld verwenden.
5. Gehen Sie weiter zum Schritt für die Auswahl der Protokoll-Manager.

Weitere Informationen

Konfigurieren der Agentenverwaltung (siehe Seite 704)
Öffnen des Assistenten für Protokollmanager-Server (siehe Seite 705)
Auswählen von Protokoll-Managern (siehe Seite 707)

Auswählen von Protokoll-Managern

Sie müssen wählen, welchem CA Enterprise Log Manager-Server Sie die Agenten oder Agentengruppen zuweisen möchten.

So wählen Sie Protokollmanager-Server:

1. Öffnen Sie den Assistenten für Protokollmanager-Server, wählen Sie Zielagenten aus, und gehen Sie weiter zum Schritt für die Auswahl der Protokoll-Manager.
2. Verwenden Sie zur Auswahl der Server, die Sie den Agenten oder Agentengruppen zuordnen möchten, die Wechselsteuerung. Im Eingabefeld "Namensmuster" können Sie nach der verfügbaren Liste suchen.
3. Klicken Sie auf "Speichern und schließen".

   Die Agenten oder Agentengruppen werden den von Ihnen ausgewählten Servern zugeordnet.

Weitere Informationen

Konfigurieren der Agentenverwaltung (siehe Seite 704)
Öffnen des Assistenten für Protokollmanager-Server (siehe Seite 705)
Auswählen von Zielagenten (siehe Seite 706)

Schutz des Agenten vor Auswirkungen von Server-IP-Adressenänderungen

Wenn Sie einen Agenten installieren, weisen Sie dem Agenten einen primären CA Enterprise Log Manager-Server zu, den dieser als erstes mit den erfassten Ereignissen kontaktiert. Wenn Sie einen Agenten konfigurieren, fügen Sie andere CA Enterprise Log Manager-Server in einer sortierten Liste hinzu. Wenn ein Agent, der zum Versenden erfasster Protokolle an den primären Server bereit ist, diesen nicht erreichen kann, kontaktiert er den sekundären Server in der Liste, bis er einen Server erreicht, der verfügbar ist. Die Konfiguration einer sortierten Liste von Sekundärservern sorgt für eine sichere Protokollzustellung von Agent zu Server. Ein Agent kann Ereignisse nur an jeweils einen CA Enterprise Log Manager senden, damit keine doppelten Ereignisse auftreten.

Wenn den Servern, die Sie zum Verwalten eines Agenten auswählen, neue IP-Adressen zugewiesen werden, kann sich dies auf die Fähigkeit des Agenten zur Weiterleitung erfasster Ereignisse zu einem Server auf der Liste auswirken. Treffen Sie entsprechende Vorsichtsmaßnahmen, um eine hohe Verfügbarkeit der Server für die Agenten sicherzustellen, die diese verwenden, auch wenn diese Server eine manuelle oder dynamische Neuzuordnung ihrer IP-Adressen durchlaufen.

Die IP-Adressen eines installierten CA Enterprise Log Manager könnten sich in folgenden Fällen ändern:

- Dynamische Neuzuordnung durch DHCP

  Der CA Enterprise Log Manager-Server in einem Einzelserversystem wurde so konfiguriert, dass DHCP seine IP-Adresse zuordnet. Kurze Zeit, nachdem dieser Server zur Verwaltung von Agenten ausgewählt wird, weist DHCP ihm eine neue IP-Adresse zu. Dies kann passieren, wenn der CA Enterprise Log Manager so lange offline ist, dass ihm die IP-Adressenüberlassung entgeht. Es ist keine Benutzerbenachrichtigung erforderlich, wenn IP-Adressen dynamisch geändert werden.

- Manuelle Neuzuordnung

  Die CA Enterprise Log Manager-Server werden mit statischen IP-Adressen konfiguriert. Aufgrund eines Site-Prozesses, bei dem IP-Adressen als Teil der Bereitstellung einem neuen Subnet zugewiesen werden, wird den CA Enterprise Log Manager-Servern manuell eine neue IP-Adresse zugewiesen.

Ergreifen Sie geeignete Maßnahmen, um eine hohe Verfügbarkeit der Server für die Agenten sicherzustellen, wenn die IP-Adressen dieser Server Änderungen unterliegen.

Weitere Informationen

Sicherstellen der Verfügbarkeit von Servern mit dynamischen IP-Adressen (siehe Seite 709)
Sicherstellen der Verfügbarkeit von Servern während der Neuzuordnung statischer IP-Adressen (siehe Seite 709)

Sicherstellen der Verfügbarkeit von Servern mit dynamischen IP-Adressen

Wenn Sie DHCP bei der Installation eines Einzelserver-CA Enterprise Log Managers auswählen, geben Sie den Hostnamen (nicht die IP-Adresse) von diesem CA Enterprise Log Manager an, wenn Sie die einzelnen Agenten installieren. Dadurch wird sichergestellt, dass alle DHCP-Neuzuordnungen der IP-Adressen des CA Enterprise Log Manager-Servers keine Auswirkungen auf die Agenten haben, die sie verwenden.

Wenn Sie die IP-Adresse des CA Enterprise Log Manager-Servers bei der Installation der Agenten angeben und sich diese dynamische IP-Adresse ändert, müssen Sie die Agenten erneut installieren, um die Verfügbarkeit des Einzelsystem-CA Enterprise Log Manager-Servers wiederherzustellen. Um dieses potentielle Problem zu vermeiden, empfiehlt sich die Installation eines weiteren CA Enterprise Log Manager-Servers, den Sie dann als sekundären Server für alle Agenten hinzufügen. Dadurch können Sie eine hohe Verfügbarkeit der Server sicherstellen.

Sicherstellen der Verfügbarkeit von Servern während der Neuzuordnung statischer IP-Adressen

Wenn Sie die CA Enterprise Log Manager-Server mit statischen IP-Adressen installieren und später eine Neunumerierung planen, verwenden Sie folgenden Workflow, um eine kontinuierliche hohe Verfügbarkeit der Server auf den sortierten Listen für die Agenten sicherzustellen. Es ist nicht notwendig, den Agenten nach jedem Schritt neu zu starten, da der Agent seine Konfigurationsdaten standardmäßig alle 5 Minuten aktualisiert.

Wichtig! Wenn der Agent nur mit einem CA Enterprise Log Manager-Server in einem Multi-Server-System konfiguriert ist, sollten Sie auf alle Fälle einen zweiten Server zur sortierten Liste hinzufügen, bevor Sie neue IP-Adressen zuweisen. Wenn dies nicht geschieht, kann es sein, dass Sie den Agenten nach der Server-IP-Adressen-Zuordnung neu installieren und konfigurieren müssen, um die Verfügbarkeit des Servers wiederherzustellen.

So stellen Sie sicher, dass Agenten einen CA Enterprise Log Manager-Server auf ihrer sortierten Liste erreichen, während die statischen IP-Adressen den Servern zugeordnet werden:

1. Wenn Sie eine IP-Adressenneuzuordnung zu einem CA Enterprise Log Manager-Server planen, bei der dieser Server der einzige CA Enterprise Log Manager ist, sollten Sie einen temporären CA Enterprise Log Manager installieren, der zu CA EEM auf dem ursprünglichen CA Enterprise Log Manager zeigt.
2. Wenn einer oder mehrere zusätzliche CA Enterprise Log Manager-Server nicht für Agenten in einem Multi-Server-System konfiguriert wurden, sollten Sie mindestens einen zusätzlichen Server der sortierten Liste zuordnen.
   a. Wählen Sie den Agenten-Explorer aus, und klicken Sie auf "Protokollmanager-Server".

      Der Assistent für den Protokollmanager-Server wird mit dem ausgewählten Schritt "Ziele auswählen" geöffnet.

   b. Wählen Sie Agenten oder Gruppen aus, je nach dem, wie Sie Ihre Zuordnungen vornehmen möchten.
   c. Wählen Sie die betreffenden Agenten oder Gruppen als Ziele aus der Liste "Verfügbar" aus, und verschieben Sie sie in die Liste "Ausgewählt".
   d. Klicken Sie auf den Schritt "Protokollmanager-Server auswählen".
   e. Wählen Sie einen CA Enterprise Log Manager aus der Liste "Verfügbar" aus, und verschieben Sie ihn in die Liste "Ausgewählt".
   f. Klicken Sie auf "Speichern und schließen".
3. Entfernen Sie die Hälfte der sortierten Liste der CA Enterprise Log Manager-Server mithilfe des Assistenten für die Zuordnung der Protokollmanager-Server aus der Agenten- oder Agentengruppenkonfiguration.
4. Ordnen Sie den Servern neue statische IP-Adressen zu, die Sie aus der Liste "Ausgewählt" entfernt haben.
5. Fügen Sie die Server mit den neuen IP-Adressen erneut hinzu.
6. Warten Sie, bis der Agent seine Konfigurationsinformationen aktualisiert hat.

   Hinweis: Sie können den Agenten manuell neu starten und die Informationen sofort aktualisieren.
7. Entfernen Sie die andere Hälfte der sortierten Liste.

   Hinweis: Wenn Sie einen temporären Server hinzugefügt haben, können Sie diesen für Failover-Zwecke beibehalten oder ihn deinstallieren und dann löschen.

8. Ordnen Sie diese IP-Adressen neu zu.
9. Fügen Sie diese Server erneut hinzu, um die ursprüngliche sortierte Liste wiederherzustellen.

Weitere Informationen:

Konfigurieren der Agentenverwaltung (siehe Seite 704)
Löschen von Service-Hosts (siehe Seite 155)

Anwenden automatischer Software-Updates

Sie können automatische CA-Software-Updates für Agenten oder Connectors anwenden. Für die Anwendung der automatischen Software-Updates mit dem Assistenten für die Liste der Aktualisierungen müssen folgende Schritte durchgeführt werden:

1. Öffnen des Assistenten für die Liste der Aktualisierungen
2. Auswählen eines der folgenden Aktualisierungstypen und Angeben der Suchkriterien für die verfügbaren Aktualisierungspakete:
   - Agentenaktualisierungen
   - Integrationsaktualisierungen für Connectors

   Hinweis: Wenn Agenten- und Connector-Aktualisierungen vorliegen, müssen Sie zuerst die Agentenaktualisierungen anwenden, damit die Aktualisierung ordnungsgemäß durchgeführt werden kann.
3. Auswählen der Agenten oder Connectors, um sie auf die aktuellste Version zu bringen

Weitere Informationen

Öffnen des Assistenten für die Liste der Aktualisierungen (siehe Seite 712)
Auswählen der Agenten oder Connectors für die Aktualisierung (siehe Seite 713)
Aktualisieren der Agenten- oder Connector-Integrationsversionen (siehe Seite 714)

Öffnen des Assistenten für die Liste der Aktualisierungen

Um Agenten oder Connectors auf die aktuellste Version zu bringen, öffnen Sie den Assistenten für die Liste der Aktualisierungen.

So öffnen Sie den Assistenten für die Liste der Aktualisierungen:

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

   Die Ordnerliste "Protokollerfassung" wird angezeigt.

2. Klicken Sie auf den Ordner "Agenten-Explorer".

   Die Schaltflächen zur Verwaltung von Agenten werden im Detailbereich angezeigt.

3. Klicken Sie auf "Automatisches Software-Update". 

   Der Assistent für die Liste der Aktualisierungen wird geöffnet.

   Beachten Sie bei Verwendung des Assistenten Folgendes:

   - Klicken Sie auf "Speichern", um ihre Daten zu speichern, ohne den Assistenten zu schließen.
   - Klicken Sie auf "Speichern und schließen", um ihren Daten zu speichern und den Assistenten zu schließen.
   - Klicken Sie auf "Zurücksetzen", um die Ansicht im Assistenten auf die zuletzt gespeicherten Einstellungen zurückzusetzen.

Auswählen der Agenten oder Connectors für die Aktualisierung

Sie können nach verfügbaren Aktualisierungen suchen, indem Sie Suchkriterien für die in Frage kommenden Agenten oder Connectors angeben.

So wählen Sie Agenten oder Connectors für die Aktualisierung aus:

1. Öffnen Sie den Assistenten für die Liste der Aktualisierungen.

   Der Assistent für die Liste der Aktualisierungsauswahl wird geöffnet.

2. Wählen Sie "Agentenaktualisierungen" oder "Connector-Aktualisierungen".

   Hinweis: Wenn Agenten- und Connector-Aktualisierungen vorliegen, müssen Sie zuerst die Agentenaktualisierungen anwenden, damit die Aktualisierung ordnungsgemäß durchgeführt werden kann.

3. Geben Sie die Suchkriterien für die Agenten- oder Connector-Aktualisierung ein:

   a. Wählen Sie die Agentengruppe aus der Dropdown-Liste aus.

   b. Wählen Sie die Plattform aus der Dropdown-Liste aus.

   c. Geben Sie das Agentennamensmuster unter Verwendung von Platzhaltern ein.

   d. (Nur für Connector-Integrationsaktualisierungen) Wählen Sie die Integration aus der Dropdown-Liste aus.

4. Klicken Sie auf "Suchen".

   Aktualisierungspakete, die ihren Suchkriterien entsprechen, werden im nächsten Schritt des Assistenten, in der Versionsauswahl, angezeigt. Gehen Sie weiter zum Schritt "Versionsauswahl", um die Daten anzuzeigen und anzuwenden.

Weitere Informationen:

Öffnen des Assistenten für die Liste der Aktualisierungen (siehe Seite 712)
Aktualisieren der Agenten- oder Connector-Integrationsversionen (siehe Seite 714)

Aktualisieren der Agenten- oder Connector-Integrationsversionen

Sie können die Version aller aufgelisteten Agenten oder Connectors mit den heruntergeladenen Aktualisierungsversionen vergleichen, um zu bestimmen, ob eine Aktualisierung erforderlich ist. Dann geben Sie an, ob Sie die aktuelle Version durch eine andere Version ersetzen möchten.

So aktualisieren Sie Agenten oder Connectors:

1. Öffnen Sie den Assistenten für die Liste der Aktualisierungen, und wählen Sie die Agenten oder Connectors aus, die Sie aktualisieren möchten.
2. Gehen Sie weiter zum Schritt "Versionsauswahl".

   Die Liste der Agenten oder Connectors, die Ihren Suchkriterien entspricht, wird angezeigt.

   - Jeder Agent wird in seiner aktuellen Version angezeigt, und in einer Dropdown-Liste wird angezeigt, welche Aktualisierungsversionen verfügbar sind.
   - Jeder Connector wird in seiner aktuellen Integrationsversion angezeigt, und in einer Dropdown-Liste wird angezeigt, welche Aktualisierungsversionen verfügbar sind.
3. (Optional) Wählen Sie "Betriebssystemversion umgehen" aus, um festzustellen, welche Aktualisierungen unabhängig von der Version für ihr ausgewähltes Betriebssystem zur Verfügung stehen.
4. Wählen Sie die Agenten oder Connectors aus, für die Sie Aktualisierungen vornehmen möchten, und klicken Sie auf "Speichern und schließen".

   Der Agent installiert die Aktualisierungen und ersetzt dabei die aktuelle Version durch die ausgewählte Agenten- oder Integrationsaktualisierung.

Hinweis: Sie können prüfen, ob alle Agenten oder Connectors über die aktuellste Version verfügen, indem Sie diese Details anzeigen, nachdem die ausgewählten Aktualisierungen angewendet wurden.

Erstellen einer Agentendiagnosedatei für Support

Sie können die Protokoll- und Konfigurationsdateien eines ausgewählten CA Enterprise Log Manager-Agenten überprüfen. Dieses AgentDiagnostics-Dienstprogramm packt Systeminformationen und Protokolldateien in eine komprimierte .tar-Datei, die an die Support-Mitarbeiter von CA Technologies gesendet werden kann. Sie können diese Datei über FTP oder eine andere Übertragungsmethode senden.

Hinweis: Diese Datei kann vertrauliche Informationen enthalten, z. B. IP-Adressen, Systemkonfigurationen, Hardwareprotokolle und Prozessprotokolle. Verwenden Sie eine sichere Methode, um diese Datei zu speichern und zu übermitteln/transportieren.

So erstellen Sie eine Agentendiagnosedatei

1. Navigieren Sie zum CA Enterprise Log Manager-Agent-bin-Verzeichnis.

   Standardpfad in Windows: C:\Programme\CA\elmagent\bin

   Standardpfad in UNIX/Linux: /opt/CA/ELMagent/bin

2. Führen Sie *einen* der folgenden Schritte durch:

   a. Falls Sie einen Agenten auf einem Windows-System ausführen, führen Sie die Datei "AgentDiagnostics.bat" aus.

   b. Falls Sie einen Agenten auf einem UNIX/Linux-System ausführen, führen Sie die Datei "AgentDiagnostics.sh" aus.

   Eine Agentendiagnosedatei wird mit dem Dateiformat "*Agenthostname_DDMMYYYY_HHMM*.tar.gz" erstellt.

Kapitel 21: Benutzerdefinierte Zertifikate

Dieses Kapitel enthält folgende Themen:

Implementieren von benutzerdefinierten Zertifikaten

Der Installationsprozess generiert zwei Zertifikate und stellt sie in das Verzeichnis "/opt/CA/SharedComponents/iTechnology" des CA Enterprise Log Manager-Servers. Sie können die installierten Zertifikate unverändert verwenden. Diese Zertifikate haben folgende Namen, wobei *ApplicationName* für das CA Enterprise Log Manager-Produkt CAELM ist.

- *ApplicationName*Cert.cer

  Dieses Zertifikat wird von allen CA Enterprise Log Manager-Services zur Kommunikation mit dem Management-Server verwendet. Der Eintrag für dieses Zertifikat ist auch unter der Datei "CALM.cnf" vorhanden.

- *ApplicationName*_AgentCert.cer

  Dieses Zertifikat wird von allen Agenten zur Kommunikation mit dem CA Enterprise Log Manager-Server verwendet.

  Wichtig! Um das CAELM_AgentCert.cer-Zertifikat in einer Umgebung mit aktiven Agenten durch ein benutzerdefiniertes Zertifikat zu ersetzen, müssen diese Agenten neu installiert werden.

Um benutzerdefinierte Zertifikate zu verwenden, müssen Sie zuerst ein Zertifikat des vertrauenswürdigen Roots von einer Root-Zertifizierungsstelle (Certificate Authority = CA) erhalten. Eine Zertifizierungsstelle kann mehrere Zertifikate in Form einer Baumstruktur herausgeben. Alle Zertifikate unter dem Zertifikat des vertrauenswürdigen Roots erben die Vertrauenswürdigkeit des Root-Zertifikats. Dieser Prozess geht davon aus, dass, falls beide Zertifikate ersetzt werden, das Zertifikat benutzerdefinierter Dienste und das Zertifikat benutzerdefinierter Agenten den gleichen vertrauenswürdigen Root haben.

Es werden nur benutzerdefinierte Zertifikate mit .cer-Erweiterungen unterstützt. Nachdem Sie ein Zertifikat des vertrauenswürdigen Roots erhalten haben, lautet die übliche Reihenfolge von Aktionen zur Implementierung benutzerdefinierter Zertifikate wie folgt:

1. Fügen Sie das Zertifikat des vertrauenswürdigen Roots zu iAuthority.conf auf dem CA Enterprise Log Manager-Verwaltungsserver oder Standalone-CA EEM hinzu.
2. Wenn Sie CAELM_AgentCert.cer ersetzen, fügen Sie das Zertifikat des vertrauenswürdigen Roots zu iControl.conf auf dem CA Enterprise Log Manager-Verwaltungsserver hinzu und wiederholen Sie dann diese Hinzufügung auf jedem anderen CA Enterprise Log Manager.
3. Wenn Sie CAELMCert.cer ersetzen, fügen Sie den allgemeinen Namen dieses benutzerdefinierten Zertifikats zur Richtlinie "AdministerObjects" auf dem CA Enterprise Log Manager-Verwaltungsserver oder Standalone-CA EEM hinzu.
4. Fügen Sie die benutzerdefinierten Zertifikate zum Ordner "iTechnology" jedes CA Enterprise Log Manager-Servers und den Namen und das Kennwort für jedes Zertifikat in separaten Konfigurationsdateien hinzu.

Fügen Sie das Zertifikat des vertrauenswürdigen Roots zum CA Enterprise Log Manager-Verwaltungsserver hinzu.

Zuerst erhalten Sie ein Zertifikat des vertrauenswürdigen Roots in PEM-Format von der Zertifizierungsstelle (Certificate Authority = CA). Danach fügen Sie dieses Zertifikat des vertrauenswürdigen Roots in die Benutzeroberfläche der SPIN-Seite von iTechnology des Verwaltungsservers oder Standalone-CA EEM hinzu.

So fügen Sie das Zertifikat des vertrauenswürdigen Roots zum CA Enterprise Log Manager-Verwaltungsserver hinzu

1. Wechseln Sie zur Benutzeroberfläche der SPIN-Seite von CA-iTechnology des Verwaltungsservers oder Standalone-CA EEM.

   `https://<management_ELM_hostname>:5250/spin`

   `https://<EEM_hostname>5250/spin`

   Die SPIN-Seite von CA iTechnology wird angezeigt.

2. Wählen Sie den iTech-Administrator aus der Dropdown-Liste aus, und klicken Sie auf "Los".

   Die iTechnology-Administratorseite wird mit einem Anmeldungslink angezeigt.

3. Klicken Sie auf "Anmelden".

   Das CA iTechnology-Anmeldedialogfeld wird angezeigt.

4. Geben Sie die EiamAdmin-Anmeldeinformationen ein, wählen Sie iAuthority und klicken Sie auf "Anmelden".

5. Wählen Sie die Registerkarte "iAuthority" aus und fügen Sie wie folgt den vertrauenswürdigen Root zu iAuthority.conf hinzu:

   a. Geben Sie eine Beschriftung für das Zertifikat ein. Geben Sie als Beschriftung nicht "myself" ein.

   b. Durchsuchen Sie die Verzeichnisse und wählen Sie die ".cer"-Datei aus.

   c. Klicken Sie auf "Vertrauenswürdigen Root hinzufügen".

   Die Bestätigungsmeldung zeigt an, dass der vertrauenswürdige Root zu iAuthority.conf hinzugefügt wurde, einer Datei, die nur auf dem Verwaltungsserver oder auf dem Standalone-CA EEM existiert.

6. Wenn Sie einen Standalone-CA EEM verwenden, fahren Sie mit dem letzten Schritt fort.

7. Wenn Sie das CAELM_AgentCert.cer-Zertifikat durch ein benutzerdefiniertes Zertifikat ersetzen, fügen Sie den vertrauenswürdigen Root wie folgt zu iControl.conf hinzu:

   a. Wählen Sie die Registerkarte "Konfigurieren" aus.

   b. Geben Sie für das Zertifikat die gleiche Beschriftung ein, die Sie im vorherigen Schritt eingegeben haben.

   c. Klicken Sie auf "Durchsuchen" und wählen Sie die gleiche Root-PEM-Datei (.cer) aus, die Sie in einem vorherigen Schritt ausgewählt haben.

   d. Klicken Sie auf "Vertrauenswürdigen Root hinzufügen".

   Die Bestätigungsmeldung zeigt an, dass der vertrauenswürdige Root des benutzerdefinierten Zertifikats zur iControl.conf-Datei im iTechnology-Verzeichnis des CA Enterprise Log Manager-Verwaltungsservers hinzugefügt wurde.

8. Klicken Sie auf "Abmelden", und schließen Sie die SPIN-Seite von iTechnology.

Fügen Sie das Zertifikat des vertrauenswürdigen Roots zu allen anderen CA Enterprise Log Manager-Servern hinzu.

Wenn Sie das CAELM_AgentCert.cer-Zertifikat durch ein benutzerdefiniertes Zertifikat ersetzen, müssen Sie das Zertifikat des vertrauenswürdigen Roots zur Benutzeroberfläche der SPIN-Seite von iTechnology jedes zusätzlichen CA Enterprise Log Manager-Servers hinzufügen. Fügen Sie bei dieser Prozedur das Zertifikat des vertrauenswürdigen Roots zu CA iControl hinzu. Diese Prozedur wird nicht benötigt, wenn Sie nur das CAELMCert.cer-Zertifikat ersetzen.

So fügen Sie das Zertifikat des vertrauenswürdigen Roots zu CA iControl jedes CA Enterprise Log Manager-Nicht-Verwaltungsservers hinzu

1. Melden Sie sich an der SPIN-Benutzeroberfläche in dem iGateway an, auf dem ein Nicht-Verwaltungsserver ausgeführt wird. Verwenden Sie folgende URL:

   `https://<ELM_hostname>:5250/spin/`

   Die SPIN-Seite von CA iTechnology wird angezeigt.

2. Wählen Sie den iTech-Administrator aus der Dropdown-Liste aus, und klicken Sie auf "Los".

   Die iTechnology-Administratorseite wird mit einem Anmeldungslink angezeigt.

3. Klicken Sie auf "Anmelden".

   Das CA iTechnology-Anmeldedialogfeld wird angezeigt.

4. Geben Sie die EiamAdmin-Anmeldeinformationen ein, wählen Sie iAuthority und klicken Sie auf "Anmelden".

5. Wählen Sie die Registerkarte "Konfigurieren" und fügen Sie den vertrauenswürdigen Root wie folgt hinzu:

   a. Geben Sie für das Zertifikat die gleiche Beschriftung ein, die Sie im vorherigen Schritt eingegeben haben.

   b. Durchsuchen Sie die Verzeichnisse und wählen Sie die ".cer"-Datei aus.

   c. Klicken Sie auf "Vertrauenswürdigen Root hinzufügen".

   Der vertrauenswürdige Root des benutzerdefinierten Zertifikats wird der iControl.conf-Datei im iTechnology-Verzeichnis hinzugefügt. Eine Bestätigungsmeldung wird angezeigt.

6. Klicken Sie auf "Abmelden", und schließen Sie die SPIN-Seite von iTechnology.

Hinzufügen eines allgemeinen Zertifikatsnamens zu einer Zugriffsrichtlinie

Das CAELMCert.cer-Zertifikat wird von allen CA Enterprise Log Manager-Services zur Kommunikation mit dem CA Enterprise Log Manager-Verwaltungsserver verwendet. Wenn Sie CAELMCert.cer durch ein benutzerdefiniertes Zertifikat ersetzen, müssen Sie den allgemeinen Namen (common name = cn) dieses benutzerdefinierten Zertifikats zur Richtlinie "AdministerObjects" auf dem Verwaltungsserver oder dem CA EEM-Standalone-Server hinzufügen.

Hinweis: Es ist nicht erforderlich, die [Benutzer] CERT_CAELM-Identität, den allgemeinen Namen des Standardzertifikats, von dieser Richtlinie zu löschen.

So fügen Sie den benutzerdefinierten allgemeinen Namen des Zertifikats zur Richtlinie "AdministerObjects" hinzu:

1. Wechseln Sie durch die Eingabe der entsprechenden URL zum CA Enterprise Log Manager-Verwaltungsserver oder dem CA EEM-Standalone-Server.

   `https://<management_server_hostname>:5250/spin/calm`

   `https://<EEM_server_hostname>:5250/spin/eiam`

2. Melden Sie sich mit Administratorrechten beim CA Enterprise Log Manager-Verwaltungsserver an. Wenn Sie auf einen CA EEM-Standalone-Server zugreifen, melden Sie sich als "EiamAdmin"-Benutzer an.

3. Klicken Sie auf die Registerkarte "Verwaltung", auf die Unterregisterkarte "Benutzer- und Zugriffsverwaltung" und greifen Sie auf den Link der Zugriffsrichtlinie im linken Fensterbereich zu. Wenn Sie bei einem CA EEM-Standalone-Server angemeldet sind, klicken Sie auf die Registerkarte "Zugriffsrichtlinien verwalten".

4. Klicken Sie auf den Link "Richtlinien zur Bereichsdefinierung".

   Im Hauptbereich wird die Richtlinientabelle der Bereichsdefinierungsrichtlinien angezeigt.

5. Blättern Sie zur Richtlinie "AdministerObjects" und wählen Sie den Link "AdministerObjects" aus.

   Die Richtlinie "AdministerObjects" wird im Bearbeitungsmodus geöffnet.

6. Fügen Sie den allgemeinen Namen (common name = cn) des benutzerdefinierten Zertifikats wie folgt hinzu:
   a. Geben Sie den allgemeinen Namen des benutzerdefinierten Zertifikats in das Feld "Identität" ein.
   b. Klicken Sie auf den Pfeil, um Ihren Eintrag zu verschieben.

      In der Liste "Ausgewählte Identitäten" wird Folgendes angezeigt: [User}<*custom certificate cn*>
7. Klicken Sie auf "Speichern".

   Dir Richtlinie "AdministerObjects" wird mit dem Zusatz des allgemeinen Namens des benutzerdefinierten Zertifikats als Identität gespeichert, die Lese- und Schreibzugriff auf die in dieser Richtlinie gelisteten Ressourcen gewährt.
8. Klicken Sie auf "Schließen", und melden Sie sich von der Benutzeroberfläche CA Enterprise Log Manager ab.

Bereitstellen neuer Zertifikate

CA Enterprise Log Manager verwendet zwei Zertifikate. Sie können eines oder beide der vordefinierten Zertifikate durch benutzerdefinierte Zertifikate ersetzen. Um neue Zertifikate bereitzustellen, melden Sie sich bei der Soft-Appliance an, stoppen Sie iGateway, fügen Sie die neuen Zertifikate hinzu, ändern Sie die entsprechenden Konfigurationsdateien und starten iGateway anschließend neu.

Bevor Sie neue Zertifikate bereitstellen, überprüfen Sie:

- Ob das vertrauenswürdige Root-Zertifikat zur iTechnology iAuthority des von Ihren CA Enterprise Log Manager-Servern verwendeten Verwaltungsservers oder CA EEM-Standalone-Servers hinzugefügt wurde.
- Ob, falls Sie CAELM_AgentCert.cer durch ein benutzerdefiniertes Zertifikat ersetzen, das Zertifikat des vertrauenswürdigen Roots zu iTechnology iControl jedes CA Enterprise Log Manager-Servers hinzugefügt wurde.
- Ob der benutzerdefinierte allgemeine Name des Zertifikats zur Richtlinie "AdministerObjects" hinzugefügt wurde. Dies bezieht sich auf das benutzerdefinierte Zertifikat, das CAELMCert.cer ersetzen soll.

So stellen Sie neue Zertifikate bereit:

1. Greifen Sie auf den Host zu, auf dem der CA Enterprise Log Manager-Server installiert ist.
2. Melden Sie sich mit den **caelmadmin**-Anmeldeinformationen beim CA Enterprise Log Manager-Server an.
3. Lassen Sie die Benutzer an der Eingabeaufforderung folgendermaßen zum Root-Verzeichnis wechseln:

   ```
   su - root
   ```

4. Wechseln Sie mit dem folgenden Befehl zum Verzeichnis "/opt/CA/SharedComponents/iTechnology":

   ```
   cd $IGW_LOC
   ```

5. Stoppen Sie iGateway.

   ```
   ./S99igateway stop
   ```

6. So ersetzen Sie CAELMCert.cer:

   a. Kopieren Sie das benutzerdefinierte *ApplicationName*Cert.cer-Zertifikat und die *ApplicationName*Cert.key-Schlüsseldatei in das iTechnology-Verzeichnis.

   b. Öffnen Sie die Datei "CALM.cnf". Ersetzen Sie den Zertifikatnamen durch den neuen Namen.

   c. Ersetzen Sie den vorhandenen Schlüsseldateinamen durch den neuen Schlüsseldateinamen.

7. So ersetzen Sie CAELM_AgentCert.cer:

   a. Kopieren Sie das benutzerdefinierte *ApplicationName*_AgentCert.cer-Zertifikat und die *ApplicationName*_AgentCert.key-Schlüsseldatei in das iTechnology-Verzeichnis.

   b. Öffnen Sie die Datei "AgentManager.conf". Ersetzen Sie den Zertifikatnamen durch den neuen Namen.

   c. Ersetzen Sie den vorhandenen Schlüsseldateinamen durch den neuen Schlüsseldateinamen.

8. Starten Sie iGateway.

   ```
   ./S99igateway start
   ```

   Alle nach dieser Bereitstellung installierten Agenten verwenden automatisch das benutzerdefinierte Zertifikat, falls CAELM_AgentCert.cer ersetzt wurde.

Anhang A: Zugänglichkeitsfunktionen

CA möchte sicherstellen, dass alle Kunden unabhängig von ihren Fähigkeiten die Produkte und die unterstützende Dokumentation erfolgreich einsetzen können, um damit zentrale Geschäftsaufgaben durchführen zu können. Dieser Abschnitt beschreibt die Eingabehilfen, die Teil von CA Enterprise Log Manager sind.

Eingabehilfenmodus

Sie können CA Enterprise Log Manager so einrichten, dass ein Eingabehilfenmodus verwendet wird, der alle Grafikfenster in Abfragen und Berichten als Tabellen anzeigt. Um den Eingabehilfenmodus aufzurufen, aktivieren Sie das Kontrollkästchen "Eingabehilfen aktivieren" im Anmeldebildschirm.

Eingabehilfensteuerung

Sie können mithilfe der Tastatursteuerung durch CA Enterprise Log Manager navigieren, wie in folgender Tabelle erläutert:

Aufgaben	Tastatursteuerung
Wechsel zwischen geöffneten Anwendungen	STRG-TAB
Auswählen einer Datei in einem geöffneten Fenster	STRG-TAB
Hilfe	F1
Klicken auf Schaltfläche	Leertaste oder Eingabetaste
Aktivieren von Kontrollkästchen	Leertaste oder Eingabetaste
Menü "Öffnen", Kombinationsfeld	STRG + Nach-unten-Pfeil
Listennavigation	STRG + Nach-unten-Pfeil zur Fokuseinstellung Nach-oben/Nach-unten-Pfeile zur Navigation Leertaste oder Eingabetaste zur Elementauswahl

Aufgaben	Tastatursteuerung
Optionsfeldgruppe	STRG + Nach-unten-Pfeil zur Fokuseinstellung Nach-oben/Nach-unten-Pfeile zur Navigation Leertaste oder Eingabetaste zur Elementauswahl
Schließen des aktiven Fensters	ALT F4
Doppelklicken	STRG + D

Sprachanzeigeeinstellungen für CA Enterprise Log Manager

Sie können die CA Enterprise Log Manager-Benutzeroberfläche auf Englisch und in folgenden Sprachen anzeigen:

- Französisch
- Italienisch
- Deutsch
- Spanisch
- Japanisch

Ändern Sie die Spracheinstellungen im Browserfenster. Wenn Sie beispielsweise Microsoft Internet Explorer verwenden, öffnen Sie das Dialogfeld "Internetoptionen", und fügen Sie die Hauptsprache hinzu, die angezeigt werden soll, oder wählen Sie diese aus.

Wenn Sie eine der fünf unterstützten Sprachen auswählen und dann die CA Enterprise Log Manager-Benutzeroberfläche öffnen, wird diese in der entsprechenden Sprache angezeigt. Die Beschriftungen und Registerkarten an der Benutzeroberfläche sind übersetzt, bestimmte andere Elemente bleiben jedoch unübersetzt: Titel von Kennungen und Datenzeichenfolgen in Berichtsergebnissen bleiben zum Beispiel auf Englisch.

Hinweis: Wenn Sie CA Enterprise Log Manager beim Ändern der Sprache anzeigen, wird das Browserfenster aktualisiert, so dass die Oberfläche in der neuen Sprache angezeigt wird. Falls Sie dabei angemeldet sind, kehren Sie zum Anmeldebildschirm zurück, der dann in der neuen Sprache angezeigt wird.

Manuelle Lokalisierung für CA Enterprise Log Manager

Sie können CA Enterprise Log Manager manuell lokalisieren, indem Sie eigene Sprachdateien erstellen. Auf diese Weise können Sie die CA Enterprise Log Manager-Benutzeroberfläche nicht nur in den bereits unterstützten Sprachen, sondern auch in anderen Sprachen anzeigen. Sie können hierzu vorhandene Dateien kopieren, die Sie als Vorlagen verwenden möchten.

So lokalisieren Sie CA Enterprise Log Manager manuell:

1. Melden Sie sich beim Host des CA Enterprise Log Manager-Servers an, navigieren Sie zu "opt/CA/LogManager/local", und wählen Sie die Dateien aus, die Sie als Vorlagen verwenden möchten. Für jede Sprache gibt es zwei Dateien:

   - "content.properties": Enthält Text, der verschiedene Inhalte beschreibt, beispielsweise Berichts- und Abfragenamen sowie Beschreibungen.
   - "ui.properties": Enthält Textzeichenfolgen für die Titel von Benutzeroberflächenfunktionen, beispielsweise Bezeichnungen für Registerkarten und Kopfzeilen.

   Den Namen sämtlicher Dateien ist ein Standardpräfix für die Sprache vorangestellt. Die deutsche Inhaltsdatei hat beispielsweise den Namen "de_content.properties". Die englische Benutzeroberflächendatei hat den Namen "en_ui.properties".

2. Kopieren Sie jeweils eine Datei beider Dateitypen, und benennen Sie diese mit dem Standardpräfix um. Wenn Sie beispielsweise eine Lokalisierungsdatei für Portugiesisch erstellen möchten, kopieren Sie die Dateien und benennen Sie in "pt_content.properties" und "pt_ui.properties" um.

   Hinweis: Sie finden die Standardsprachpräfixe im Browser in der Liste der unterstützten Sprachen.

3. Öffnen Sie die Dateien, und übersetzen Sie die in der Originalsprache vorliegenden Zeichenfolgen in die gewünschte Sprache. Wenn Sie zum Beispiel die englischen Dateien kopiert haben, ersetzen Sie alle englischen Textzeichenfolgen durch die gewünschte Sprache.

4. Speichern Sie die manuell übersetzten Dateien an dem im ersten Schritt festgelegten Speicherort auf jedem CA Enterprise Log Manager-Server, auf dem sie verfügbar sein sollen.

5. Stellen Sie den Browser auf die Zielsprache ein, und melden Sie sich bei CA Enterprise Log Manager an.

Weitere Informationen:

Sprachanzeigeeinstellungen für CA Enterprise Log Manager (siehe Seite 726)

Anhang B: Zugreifen auf erfasste Ereignisse mit ODBC und JDBC

Dieses Kapitel enthält folgende Themen:

Wissenswertes zum ODBC-/JDBC-Zugriff in CA Enterprise Log Manager

CA Enterprise Log Manager ermöglicht einen schreibgeschützten ODBC- und JDBC-Zugriff auf den Ereignisprotokollspeicher, so dass Sie folgende Aufgaben durchführen können:

- Konfigurieren benutzerdefinierter Berichte mit einem externen Hilfsprogramm für die Berichterstellung wie z. B. Crystal Reports von BusinessObjects
- Abrufen ausgewählter Protokollinformationen mit Hilfe externer Anwendungen

Diese Funktionen ermöglichen Ihnen die Erstellung und Formatierung Ihrer eigenen benutzerdefinierten Berichte unter Verwendung von Protokollinformationen, die bereits von CA Enterprise Log Manager abgerufen wurden. Darüber hinaus können Sie Daten abrufen, um sie mit bereits vorhandenen Correlation-Engines, Malware-Erkennungsprogrammen und anderen Funktionen zu verarbeiten.

Konfigurieren Sie nach der Installation des von CA bereitgestellten Clients auf dem System, das für den Zugriff auf den Ereignisprotokollspeicher verwendet werden soll, eine Verbindung zur Datenquelle, und beginnen Sie dann mit dem Abrufen der Daten. Die serverseitigen Komponenten werden vom Service für automatische Software-Updates installiert.

Erstellen von ODBC- und JDBC-Abfragen für die Verwendung in CA Enterprise Log Manager

Die ODBC- und JDBC-Unterstützung in CA Enterprise Log Manager ist auf schreibgeschützte Abfragen beschränkt, die SELECT-Anweisungen für folgende Tabellen verwenden:

- VIEW_EVENT - enthält Ereignisse aus der Ereignisdatenbank
- VIEW_INCIDENT - enthält Incidents aus der Incident-Datenbank
- VIEW_INCIDENTEVENT_BYID - enthält Incident-Komponentenereignisse aus der Incident-Ereignisdatenbank

Erstellen Sie Ihre SELECT-Anweisungen unter Verwendung der ANSI SQL-Formate und -Regeln. Die serverseitigen Komponenten beinhalten ein SQL-Analysemodul. Der Parser implementiert einen großen Teil der SQL-Eingabeebene gemäß X3.135-1992-Spezifikation "Database Language SQL". Der Parser unterstützt ebenfalls SQL-Funktionen von ANSI SQL99 und kommerziellen Datenbanken wie Microsoft SQL Server und Oracle. Außerdem ist der Parser mit der ODBC-Spezifikation der Minimal-Grammatik kompatibel.

Die ELM-Schemadefinition dient als Schema für diese Tabelle. Nähere Informationen zum Schema finden Sie im *Referenzhandbuch zur ELM-Schemadefinition (CEG)*.

Einschränkungen der SQL-Unterstützung

CA Enterprise Log Manager unterstützt keine Aufrufe gespeicherter Prozeduren, DCL-Befehle (Datensteuerungssprache) oder DDL-Befehle (Datendefinitionssprache).

Die folgenden Operationen und Schlüsselwörter der Datenbearbeitungssprache (DML) werden von CA Enterprise Log Manager ebenfalls nicht unterstützt:

- UNION
- JOIN
- Geschachteltes SELECT
- INSERT
- UPDATE
- DELETE
- Operatoren zur Transaktionssteuerung wie COMMIT, ROLLBACK usw.

Unterstützte SQL-Funktionen

Die folgenden SQL-Funktionen werden bei der Erstellung von SELECT-Anweisungen unterstützt:

- ABS(*numerischer_Ausdr*)
- ROUND(*numerischer_Ausdr, ganzzahliger_Ausdr*)
- LCASE(*Zeichenfolgeausdruck*)
- LOWER(*Zeichenfolgeausdruck*)
- LENGTH(*Zeichenfolgeausdruck*)
- LTRIM(*Zeichenfolgeausdruck*)
- RTRIM(*Zeichenfolgeausdruck*)
- SUBSTRING(*Zeichenfolgeausdruck, Start, Länge*)
- UCASE(*Zeichenfolgeausdruck*)
- UPPER(*Zeichenfolgeausdruck*)
- IFNULL (*Ausdr, Standardwert*)
- ISNULL (*Ausdr, Standardwert*)

- NVL (*Ausdr, Standardwert*)
- CONVERT (*Wertausdruck, Datentyp*)
- CURDATE()
- CURTIME()
- CURTIMESTAMP()
- DATEADD(*Datumsteil, Zahl, Datum*)
- TIMESTAMPADD(*Datumsteil, Zahl, Datum*)
- DATEDIFF(*Datumsteil, Startdatum, Enddatum*) Für den Datumsteil sind die Werte "Jahr", "Tag" und "Sekunde" zulässig.
- TIMESTAMPDIFF(*Datumsteil, Startdatum, Enddatum*) Für den Datumsteil sind die Werte "Jahr", "Tag" und "Sekunde" zulässig.
- DAYOFMONTH(*Datumsausdruck*)
- DAYOFWEEK(*Datumsausdruck*)
- DAYOFYEAR(*Datumsausdruck*)
- HOUR(*Uhrzeitausdruck*)
- MINUTE(*Uhrzeitausdruck*)
- MONTH(*Datumsausdruck*)
- NOW( )
- SECOND(*Uhrzeitausdruck*)
- WEEK(*Datumsausdruck*)
- YEAR(*Datumsausdruck*)
- AVG([ALL | DISTINCT]*Ausdruck*)
- SUM([ALL | DISTINCT]*Ausdruck*)
- COUNT({[ALL | DISTINCT]*Ausdruck*] | *})
- MAX([ALL | DISTINCT]*Ausdruck*)
- MIN([ALL | DISTINCT]*Ausdruck*)

Verarbeitung von Abfragen

CA Enterprise Log Manager verarbeitet eine vom Client initiierte ODBC- bzw. JDBC-Abfrage auf folgende Weise:

1. Eine Client-Anwendung sendet eine SELECT-Anweisung über eine ODBC-Verbindung an den CA Enterprise Log Manager-Server.
2. Der CA Enterprise Log Manager-Server validiert die SELECT-Anweisung. Bei erfolgreicher Validierung erstellt der CA Enterprise Log Manager-Server eine der Abfrage entsprechende Datenstruktur.

   Alle aufgetretenen Fehler werden direkt an den Client-Treiber zurückgegeben.
3. Der CA Enterprise Log Manager-Server konvertiert die SQL-Elemente in eine Abfrage, die er verarbeiten kann. Bei erfolgreicher Konvertierung wird die Abfrage vom CA Enterprise Log Manager-Server ausgeführt.

   Alle aufgetretenen Fehler werden an den Client-Treiber zurückgegeben.
4. Der CA Enterprise Log Manager-Server verwaltet für jede Abfrage Statusinformationen, einschließlich eines Timers für die Ablaufzeit, so dass eine Abfrage abgebrochen werden kann, falls die Sitzung geschlossen wird oder die Abfrage abläuft.
5. Der CA Enterprise Log Manager-Server übersetzt die Abfrageergebnisse und sendet sie zurück an den ODBC-Client-Treiber. Anschließend erhält die Client-Anwendung die Daten.

Ergebnisspalten-Aliase

Im Rahmen der Verwaltung des Abfragestatus werden von CA Enterprise Log Manager-Aliasnamen für Ergebnisspalten unterstützt. Sie können daher in Ihren benutzerdefinierten Berichten CEG-Felder mit eigenen Bezeichnungen und Überschriften verwenden.

Die Aliasnamen werden beibehalten und für die ordnungsgemäße Zuordnung der Daten verwendet, wenn der CA Enterprise Log Manager-Server ein Ergebnis an den Client-Treiber zurücksendet.

Ergebnisbeschränkungen

Aus Gründen der Speicherplatzverwaltung sorgt CA Enterprise Log Manager dafür, dass die Anzahl der Ergebniszeilen beschränkt wird. CA Enterprise Log Manager verwendet nur einen Teil des Transact-SQL TOP-Schlüsselworts mit einem festen Wert. Die Prozentsatz-Variante des Schlüsselworts wird nicht unterstützt.

Der in CA Enterprise Log Manager standardmäßig verwendete TOP-Wert sind 5000 Zeilen, mit höchstens 50.000 Zeilen.

CA Enterprise Log Manager-spezifische Fehlercodes

Im Folgenden sind die ODBC- und JDBC-Fehlercodes von Fehlern aufgeführt, die beim Zugriff auf den CA Enterprise Log Manager-Ereignisprotokoll-Speicher auftreten können. Mit jeder Fehlermeldung werden spezifische Fehlerdetails angegeben.

- 88 – do not support (Nicht unterstützt)

  Die zugehörige Fehlermeldung enthält Details zur nicht unterstützen Funktionalität.

- 300 – generic error (Allgemeiner Fehler)

  Die zugehörige Fehlermeldung enthält Details.

- 301 – error to convert multibyte character parameters (Fehler beim Konvertieren von Multibyte-Zeichenparametern)
- 302 – authentication error (Authentifizierungsfehler)
- 304 – invalid expression (column) in OrderBy or GroupBy clause (Ungültiger Ausdruck (Spalte) in OrderBy- oder GroupBy-Klausel)

Bei folgenden Fehlern handelt es sich um Ausführungsfehler bei SQL-Anweisungen:

- 305 – error to start query (Fehler beim Starten der Abfrage)
- 306 – error to get query status (Fehler beim Abrufen des Abfragestatus)
- 307 – error to parse query results XML (Fehler beim Analysieren der XML-Datei mit den Abfrageergebnissen)

- 308 – query execution error (Abfrageausführungsfehler)
- 309 – query executed with errors (Abfrage wurde mit Fehlern ausgeführt)
- 310 – error to fetch query results (Fehler beim Abrufen der Abfrageergebnisse)
- 311 – query timeout (Zeitüberschreitung bei Abfrage)

Beispiel: Verwenden eines Zugriffsfilters zum Beschränken von ODBC-Ergebnissen

Sie können einen Zugriffsfilter erstellen, um die für eine ODBC-Zugriffsanforderung zurückgegebenen Daten einzuschränken. Wenn Mitglieder der angegebenen Anwendungsgruppe unter Verwendung des ODBC-Clients auf CA Enterprise Log Manager-Ereignisdaten zugreifen, werden nur die vom Filter zugelassenen Informationen angezeigt.

Bei diesem Beispiel wird davon ausgegangen, dass eine Anwendungsgruppe mit dem Namen "UNIX-Analysten" vorhanden ist und für alle Mitglieder dieser Gruppe nur UNIX-Ereignisse aus dem Ereignisprotokollspeicher angezeigt werden sollen. Der in diesem Beispiel erstellte Filter beschränkt die Anzeige der Ereignisdaten sowohl innerhalb der CA Enterprise Log Manager-Benutzeroberfläche als auch bei externen Anforderungen über ODBC.

Weitere Informationen zu Zugriffsfiltern finden Sie in der Online-Hilfe.

So erstellen Sie einen Zugriffsfilter:

1. Melden Sie sich als Administrator bei CA Enterprise Log Manager an.
2. Klicken Sie auf die Registerkarte "Verwaltung" und anschließend auf die Unterregisterkarte "Benutzer- und Zugriffsverwaltung".
3. Klicken Sie auf "Neuer Zugriffsfilter"  . Der Assistent für das Zugriffsfilterdesign wird gestartet.

4. Geben Sie im Feld "Name" die Bezeichnung "UNIX-Analysten" sowie im Feld "Beschreibung" den Ausdruck "Zugriffsfilter für UNIX-Analysten" ein, und klicken Sie dann oben im Dialogfeld auf Schritt 2, "Identitäten".
5. Ändern Sie den Typ in "Anwendungsgruppe", geben Sie im Feld "Name" die Bezeichnung "UNIX" ein, und klicken Sie dann auf "Identitäten suchen".

   Eine Liste der mit Ihren Suchkriterien übereinstimmenden Identitäten wird in einer Wechselsteuerung angezeigt, so dass Sie die gewünschten Identitäten auswählen können.
6. Wählen Sie in der Liste "Verfügbare Identitäten" die Anwendungsgruppe "UNIX-Analysten" aus, und klicken Sie auf den nach rechts weisenden Pfeil der Wechselsteuerung, um die Auswahl in die Liste "Ausgewählte Identitäten" zu verschieben.
7. Klicken Sie oben im Dialogfeld auf Schritt 3, "Zugriffsfilter".
8. Klicken Sie auf "Neuer Ereignisfilter"  , um eine Zeile hinzuzufügen, und klicken Sie dann in den Feldbereich unter "Spalte".
9. Wählen Sie aus der Dropdown-Liste den Eintrag "event_logname" aus, und klicken Sie dann in den Feldbereich unter "Wert".
10. Wählen Sie aus der Dropdown-Liste die Option "Unix" aus. Das Dialogfeld entspricht nun in etwa der folgenden Abbildung:

11. Klicken Sie auf "Speichern und schließen".

Beispiel: Vorbereitung für die Verwendung von ODBC- und JDBC-Clients mit Crystal Reports

Die Vorbereitung für die Verwendung des ODBC- oder JDBC-Clientzugriffs auf CA Enterprise Log Manager-Ereignisse mit BusinessObjects Crystal Reports umfasst folgende Schritte:

1. Erstellen Sie einen CA Enterprise Log Manager-Benutzer, um den Zugriff auf die Datenbank zuzulassen.
2. Überprüfen Sie, ob der ODBC-Service SSL-Verschlüsselung und Port 17002 verwendet.
3. Installieren Sie den ODBC-Client, oder kopieren Sie die JDBC-Dateien auf den Server, auf dem sich Crystal Reports befindet.

   Informationen zu diesen Installationen finden Sie im *Implementierungshandbuch*.
4. Konfigurieren Sie die Betriebssystemkomponenten:
   a. Erstellen und testen Sie in der Windows-Systemsteuerung eine ODBC-Datenquelle.
   b. Bearbeiten Sie die Crystal Reports-Konfigurationsdatei so, dass der JDBC-Client verwendet wird.
5. Erstellen Sie Ereignisse, die von CA Enterprise Log Manager erfasst werden sollen.

   Falls Sie nicht sicher sind, ob der Ereignisprotokoll-Speicher bereits Ereignisse des abgefragten Typs enthält, können Sie diesen Schritt überspringen.

Hinweis: Bei diesem Prozess und dem zugehörigen Beispiel wird vorausgesetzt, dass Sie mit dem Erstellen grundlegender SQL-Anweisungen und dem Umgang mit Crystal Reports vertraut sind. Weitere Informationen zur Verwendung von Crystal Reports finden Sie in der BusinessObjects-Online-Hilfe.

Erstellen eines CA Enterprise Log Manager-Benutzers für den ODBC- oder JDBC-Zugriff

Gehen Sie wie unten beschrieben vor, um ein Benutzerkonto mit dem Namen "ELM_Zugriff" zu erstellen, das Sie mit den JDBC- und ODBC-Clients verwenden können.

CA Enterprise Log Manager-Benutzer mit Datenzugriffsberechtigung können mit Hilfe von ODBC oder JDBC auf Ereignisdaten zugreifen. Alle mit CA Enterprise Log Manager bereitgestellten Standardrollen verfügen über diese Berechtigung. Für dieses Beispiel können Sie einen Benutzer mit einer beliebigen CA Enterprise Log Manager-Standardrolle erstellen: Administrator, Analyst oder Auditor.

So erstellen Sie den neuen Benutzer:

1. Melden Sie sich als Administrator beim CA Enterprise Log Manager-Server an.
2. Klicken Sie auf die Registerkarte "Verwaltung" und auf die Unterregisterkarte "Benutzer- und Zugriffsverwaltung".
3. Klicken Sie auf die Schaltfläche "Benutzer", um die eingebettete CA EEM-Benutzeroberfläche anzuzeigen.
4. Klicken Sie auf "Neuer Benutzer". Das Dialogfeld "Neuer Benutzer" wird geöffnet.
5. Klicken Sie auf "Anwendungsbenutzerdetails hinzufügen", und weisen Sie dem Administratorkonto Anwendungsberechtigungen zu.

   Hinweis: In einer Produktionsumgebung würden Sie einem Benutzer die geringstmöglichen Berechtigungen für den Zugriff auf Daten zuweisen. Sie können den Zugriff auf vielerlei Arten beschränken, unter anderem durch Benutzerrollen, Zugriffsrichtlinien und Zugriffsfilter. Weitere Informationen finden Sie in der *Online-Hilfe*.
6. Stellen Sie den Benutzerdatensatz nach Bedarf fertig, und weisen Sie ein Kennwort zu. Notieren Sie sich dieses, damit Sie es später in diesem Beispiel zur Hand haben.
7. Speichern Sie den Benutzer, und schließen Sie das Fenster "Benutzer".

Konfigurieren der ODBC-Service-Einstellungen

Gehen Sie wie unten beschrieben vor, um die ODBC- und JDBC-Serviceeinstellungen für CA Enterprise Log Manager zu konfigurieren.

Hinweis: Änderungen in diesem Bereich führen zu einem Neustart der serverseitigen Prozesse, die ODBC- und JDBC-Kommunikation ermöglichen.

So konfigurieren Sie den ODBC-Service:

1. Melden Sie sich als Administrator beim CA Enterprise Log Manager-Server an.
2. Klicken Sie auf die Registerkarte "Verwaltung" und auf die Unterregisterkarte "Services".
3. Klicken Sie auf den Knoten "ODBC-Service".
4. Übernehmen Sie die Standardeinstellungen:
   - "Dienste aktivieren": wahr (ermöglicht ODBC- und JDBC-Verbindungen auf dem CA Enterprise Log Manager-Server)
   - Port: 17002
   - "Verschlüsselt (SSL)": aktiviert
   - Sitzungszeitlimit: 15 Minuten
   - "Protokollierungsstufe": Standardwert NICHT FESTGELEGT übernehmen
5. Klicken Sie auf "Speichern".

Erstellen einer ODBC-Datenquelle "elm"

Gehen Sie wie unten beschrieben vor, um eine Datenquelle mit dem Namen "CA-ELM" zu erstellen.

Hinweis: Sie können die Datenquelle erst nach der Installation des ODBC-Clients konfigurieren.

So erstellen Sie eine Datenquelle:

1. Öffnen Sie die Windows-Systemsteuerung.
2. Öffnen Sie den Ordner "Verwaltung", und starten Sie das Hilfsprogramm "Datenquellen (ODBC)".
3. Klicken Sie auf "Hinzufügen", um das Dialogfeld "Neue Datenquelle erstellen" anzuzeigen.

4. Wählen Sie den Eintrag "DataDirect OpenAccess SDK 6.0" aus, und klicken Sie auf "Fertig stellen".

   Das Hilfsprogramm DataDirect OpenAccess SDK ODBC Driver Setup zeigt einen Konfigurationsbildschirm an.

5. Klicken Sie in das Feld "Datenquellenname", und geben Sie eine Textbeschreibung ein.

6. Geben Sie im Feld "Service-Host" den Namen des CA Enterprise Log Manager-Servers ein. In diesem Beispiel wird "ca-elm" verwendet.

7. Geben Sie im Feld "Service-Port" den Wert 17002 ein.

8. Aktivieren Sie das Kontrollkästchen "Verschlüsselt (SSL)".

9. Geben Sie folgende benutzerdefinierte Eigenschaften ein:

   ```
   querytimeout=600
   (seconds);queryfederated=true;queryfetchrows=1000;offsetmins=0;suppressNoncri
   ticalErrors=false
   ```

10. Klicken Sie auf "Anwenden" und anschließend auf "OK".

    Wenn die Verbindungsparameter korrekt sind, wird eine Meldung über eine erfolgreiche Verbindung angezeigt.

11. Klicken Sie auf "OK", um zum Dialogfeld "ODBC-Datenquellen-Administrator" anzuzeigen, und klicken Sie dann erneut auf "OK", um das Hilfsprogramm zu beenden.

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
```

Bearbeiten der Crystal Reports-Konfigurationsdatei

Erst nachdem Sie vorab einige Konfigurationseinstellungen bereitgestellt haben, können Sie Crystal Reports mit dem JDBC-Client von CA Enterprise Log Manager verwenden. Nach der Konfiguration der Crystal Reports-XML-Konfigurationsdatei können Sie ANSI-SQL-Standardabfragen vorbereiten und an den Ereignisprotokoll-Speicher von CA Enterprise Log Manager senden.

So konfigurieren Sie Crystal Reports-Einstellungen für JDBC:

1. Stellen Sie sicher, dass Sie vor dem Bearbeiten der Konfigurationsdatei die JAR-Dateien des JDBC-Clients auf den Crystal Reports-Server kopieren.

   Weitere Informationen finden Sie im *Implementierungshandbuch*.

2. Greifen Sie auf den Server zu, auf dem sich Crystal Reports befindet.
3. Suchen Sie die Datei "CRConfig.xml", und öffnen Sie sie zum Bearbeiten.

4. Suchen Sie die <DataDriverCommon>-Kennung und den darunter befindlichen <Classpath>-Kennungsabschnitt.
5. Fügen Sie dem Klassenpfad den Speicherort der JDBC-JAR-Dateien für den JDBC-Client hinzu.
6. Ändern Sie den Wert in den JDBC-URL-Kennungen wie folgt:

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

   Im Abschnitt mit den Hinweisen zur JDBC-URL finden Sie weitere Erläuterungen zu diesen Parametern.

   In der Dokumentation zu Crystal Reports finden Sie weitere Informationen zum Festlegen der Verbindungsparameter in diesem Produkt.
7. Ändern Sie den Wert in den JDBC-Kennungen für Klassennamen wie folgt:

   ```
   com.ca.jdbc.openaccess.OpenAccessDriver
   ```
8. Speichern Sie die Datei, und beenden Sie den Vorgang.

Weitere Informationen:

Hinweise zur JDBC-URL (siehe Seite 743)

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 740)

Erstellen von Ereignissen für das Beispiel zu ODBC

Erstellen Sie für die anzuzeigende Beispielabfrage einige relevante Ereignisse. Führen Sie dazu fehlgeschlagene Aktivitäten wie die folgenden herbei:

- Melden Sie sich beim CA Enterprise Log Manager-Server mehrmals falsch an.
- Melden Sie sich bei einem Agentenhost, dessen Ereignisse an einen bestimmten CA Enterprise Log Manager-Server gesendet werden, falsch an.
- Greifen Sie mit falschen Anmeldeinformationen auf eine Netzwerk- oder Systemressource zu.

Verwenden von Crystal Reports für den Zugriff auf den Ereignisprotokollspeicher mit ODBC

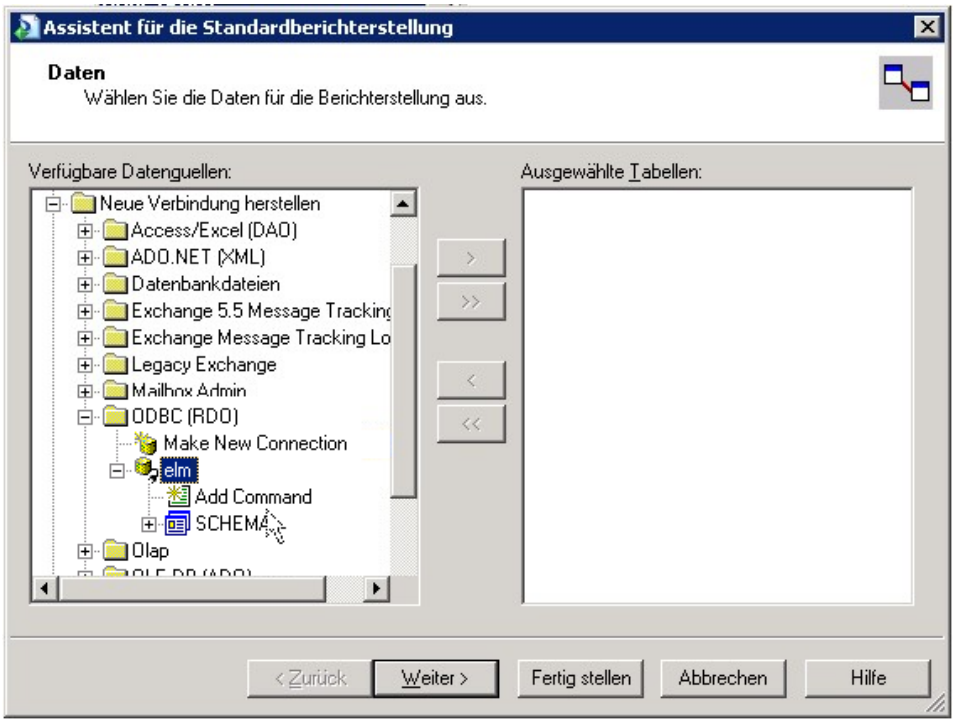
Mit Hilfe der Funktion für den ODBC-Zugriff können Sie CA Enterprise Log Manager-Ereignisdaten von einem Drittanbieter-Berichtstool, wie z. B. BusinessObjects Crystal Reports, abfragen. Nachdem die erforderliche Installation und Konfiguration durchgeführt wurde, haben Sie die Möglichkeit, ANSI SQL-Standardabfragen an den CA Enterprise Log Manager-Ereignisprotokollspeicher einzurichten und zu senden.

Das Datenbankschema für den Ereignisprotokollspeicher ist die ELM-Schemadefinition (CEG, Common Event Grammar). Die Online-Hilfe von CA Enterprise Log Manager enthält eine CEG-Referenz, die Sie bei der Erstellung von Abfragen unterstützt. Sie können auch die zugrunde liegenden SQL-Anweisungen der vordefinierten Abfragen überprüfen. Verwenden Sie jedoch ANSI SQL, um außerhalb von CA Enterprise Log Manager auf die Datenbank zuzugreifen.

So greifen Sie aus Crystal Reports auf Ereignisdaten zu:

1. Führen Sie die erforderliche Installation und Konfiguration durch.
2. Starten Sie Crystal Reports, und rufen Sie den Assistenten für Standardberichte auf.

3. Stellen Sie im Dialogfeld "Daten" eine ODBC-Verbindung her, und wählen Sie die in der Windows-Systemsteuerung erstellte ODBC-Datenquelle aus.



4. Erstellen Sie mit Hilfe der Funktion zum Hinzufügen von Befehlen eine Abfrage im SQL-Eingabebereich.

   Beispielsweise können Sie die folgende Abfrage erstellen:

   ```
   SELECT source_username as source_username , SUM(event_count) AS
   FUNC_SUM_event_count FROM view_event WHERE event_result = 'F' GROUP BY
   source_username ORDER BY FUNC_SUM_event_count DESC;
   ```

5. Klicken Sie auf "OK", um die Eingabe der Abfrage abzuschließen.

   Es wird eine Berichtsvorlage angezeigt, in die die von der Abfrage zurückgegebenen Datenspalten eingefügt werden müssen.

6. Übernehmen Sie die Felder per Drag & Drop aus dem Feldexplorer (obere rechte Ecke) als Spalten in die Berichtsvorlage.

   Beim Ausführen der Abfrage werden die den Feldern zugewiesenen Werte angezeigt. Sie können die jeweils gewünschte Visualisierung oder Anpassung mit Hilfe von Crystal Reports vornehmen.

7. (Optional) Vergleichen Sie die Berichtsergebnisse mit denen des vordefinierten Berichts "Fehlgeschlagene Aktivitäten nach Benutzer".

Zugreifen auf Ereignisse aus Crystal Reports mit JDBC

Über die folgenden Aufgaben können Sie mit JDBC auf den Ereignisprotokoll-Speicher zugreifen:

1. Kopieren Sie die JDBC-JAR-Dateien für den Client auf den Server, auf dem sich Crystal Reports befindet.
2. Bearbeiten Sie die Crystal Reports-Konfigurationsdatei.
3. Senden Sie mit Hilfe von Crystal Reports eine Abfrage.

Hinweis: Bei diesem Prozess und dem zugehörigen Beispiel wird vorausgesetzt, dass Sie mit dem Erstellen grundlegender SQL-Anweisungen und dem Umgang mit Crystal Reports vertraut sind. Weitere Informationen zur Verwendung von Crystal Reports finden Sie in der BusinessObjects-Online-Hilfe.

Kopieren der JAR-Dateien für den JDBC-Treiber

Sie können mit dem JDBC-Treiber von einem CA Enterprise Log Manager-Server erst auf Ereignisse zugreifen, nachdem Sie die zugehörigen JAR-Dateien auf den Server kopiert haben, den Sie für den Zugriff verwenden möchten.

So kopieren Sie die Dateien:

1. Öffnen Sie das ISO-Image, oder greifen Sie auf die Installations-DVD für die Anwendung zu.
2. Navigieren Sie zu dem Verzeichnis "\CA\ELM\JDBC".
3. Kopieren Sie die JAR-Dateien auf den Server, auf dem sich Crystal Reports befindet.

   Das Berichtspaket, das Sie verwenden, erfordert einen spezifischen Speicherort für diese Dateien. Sehen Sie in der Dokumentation nach, die im Lieferumfang Ihrer Anwendung enthalten ist.
4. Notieren Sie sich für den Referenzpfad bei der Konfiguration von Verbindungen den Namen des Verzeichnisses, in dem Sie diese Dateien ablegen.

Verwenden von Crystal Reports für den Zugriff auf den Ereignisprotokoll-Speicher mit Hilfe von JDBC

Mit der JDBC-Zugriffsfunktion können Sie in einem Berichterstellungstool eines anderen Herstellers wie BusinessObjects Crystal Reports auf CA Enterprise Log Manager-Ereignisdaten zugreifen.

Das Datenbankschema für den Ereignisprotokollspeicher ist die ELM-Schemadefinition (CEG, Common Event Grammar). Die Online-Hilfe von CA Enterprise Log Manager enthält eine CEG-Referenz, die Sie bei der Erstellung von Abfragen unterstützt. Sie können auch die zugrunde liegenden SQL-Anweisungen der vordefinierten Abfragen überprüfen. Verwenden Sie jedoch ANSI SQL, um außerhalb von CA Enterprise Log Manager auf die Datenbank zuzugreifen.

So greifen Sie aus Crystal Reports auf Ereignisdaten zu:

1. Starten Sie Crystal Reports, und rufen Sie den Assistenten für Standardberichte auf.
2. Erstellen Sie im Dialogfeld "Data" (Daten) eine JDBC-Verbindung.

   Hinweis: Wenn das Dialogfeld "Connection Information" (Verbindungsinformationen) angezeigt wird, verwenden Sie für den Datenbanknamen den Wert "*Default*" (Standard).
3. Erstellen Sie mit Hilfe der Funktion "Add Command" (Befehl hinzufügen) im SQL-Eingabebereich die folgende Abfrage, und führen Sie sie aus:

   ```
   SELECT source_username as source_username , SUM(event_count) AS
   FUNC_SUM_event_count FROM view_event WHERE event_result = 'F' GROUP BY
   source_username ORDER BY FUNC_SUM_event_count DESC;
   ```
4. Ziehen Sie die Felder rechts aus dem Feld-Explorer als Spalten in die Berichtsvorlage.

   Beim Ausführen der Abfrage werden die den Feldern zugewiesenen Werte angezeigt. Mit den Crystal Reports-Tools können Sie jede benötigte Visualisierung oder Anpassung erstellen.
5. (Optional) Vergleichen Sie die Berichtsergebnisse mit denen des vordefinierten Berichts "Fehlgeschlagene Aktivitäten nach Benutzer".

Entfernen des ODBC-Clients unter Windows

Auf allen Windows-Plattformen werden mit der Option "Entfernen" des Client-Installationspakets die Produktdateien und die Einträge in den Systeminformationen gelöscht.

Wichtig! Wenn Sie im Installationsverzeichnis des lokalen ODBC-Clients IP-Quelldateien erstellt hatten, sichern Sie diese Dateien an einem anderen Speicherort, bevor Sie den ODBC-Client von einem Windows-System entfernen.

Wenn der lokale ODBC-Client installiert ist und Sie ihn an einem anderen Speicherort installieren möchten, verwenden Sie die Option "Entfernen". Entfernen Sie den installierten lokalen ODBC-Client, und installieren Sie ihn dann erneut am neuen Speicherort.

So entfernen Sie den ODBC-Client:

1. Öffnen Sie in der Windows-Systemsteuerung die Option "Software".
2. Suchen Sie den Eintrag "CA Enterprise Log Manager-ODBC-Treiber", und wählen Sie ihn aus.
3. Klicken Sie auf "Entfernen".

Entfernen des JDBC-Clients

Wenn Sie den JDBC-Client deinstallieren möchten, entfernen Sie das Installationsverzeichnis.

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

A

B

C

D

E

F

S

U

V

Z