CA Enterprise Log Manager

Versionshinweise

r12.1 SP1

CA-Produktreferenzen

Dieses Dokument bezieht sich auf die folgenden Produkte von CA:

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

Technischer Support – Kontaktinformationen

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

Änderungen in der Dokumentation

Seit der letzten Version dieser Dokumentation wurden folgende Aktualisierungen vorgenommen:

- Upgrade durch automatische Software-Updates – Diesem bereits vorhandenen Abschnitt wurden Informationen zu CA Enterprise Log Manager r12.1 SP1 hinzugefügt. Verwenden Sie automatische Software-Updates, um dieses Service Pack zu erhalten und somit ein Upgrade der FIPS-Unterstützung für CA Enterprise Log Manager durchzuführen.
- Neue und veränderte Funktionen in r12.1SP1 – Dieses Kapitel beschreibt die FIPS-Kompatibilität in CA Enterprise Log Manager, die verwendete Verschlüsselung, Beschränkungen und die nötigen Konfigurationsänderungen, um die Benutzeroberfläche sowohl über Microsoft Internet Explorer als auch über Mozilla Firefox anzeigen zu können. Enthält auch Anweisungen zur Verwendung des ISO-Images bei neuen Bereitstellungen sowie zum Hinzufügen eines neuen CA Enterprise Log Manager-Servers zu einer bereits vorhandenen Bereitstellung.
- Änderungen in "Zertifikatkonflikt durch Ändern der Systemzeit des CA EEM-Servers" – Dieses bereits vorhandene Thema enthält nun die neue Dateinamenerweiterung des Zertifikats (.cer).
- Erforderliche Energieeinstellungen für bestimmte HP- und IBM-Computer – Dieses neue Thema beschreibt erforderliche Änderungen an den standardmäßigen Energieeinstellungen auf Servern der Serie HP Proliant DL 380G5 und IBM X3650.
- Die nachfolgenden bekannten Probleme wurden beseitigt, da sie entweder gelöst wurden oder für diese Aktualisierung nicht mehr gelten:
  - Fehler bei Agenten mit benutzerdefinierten Zertifikaten
  - Sekundäre Syslog-Dispatcher versagt bei hoher Belastung
  - Ereignisse vom selben Host können mit verschiedenen Zielhostnamen angezeigt werden
  - Einschränkung bei den Spezifikationen von PDF-Berichten
  - Nach einer Aktualisierung ist das Anmelden bei CA Enterprise Log Manager nicht möglich
  - Direkte Aktualisierung auf r12.1 M10 verursacht inkorrekte Anzeige der Sensorversion
  - Nicht korrekter Fehler "Audit-Richtlinienmanager ist nicht installiert"
  - Upgrade auf CA Audit erforderlich für die Interaktion mit CA Enterprise Log Manager

Weitere Informationen:

Inhalt

Anhang A: Vereinbarung gegenüber Drittparteien 89

Kapitel 1: Willkommen

Willkommen bei CA Enterprise Log Manager. Dieses Dokument enthält Informationen zur Betriebssystemunterstützung, zu Verbesserungen und zu bekannten Problemen sowie Informationen darüber, wie der technische Support von CA kontaktiert werden kann.

Aktualisieren mit automatischen Software-Updates

Aktualisieren Sie CA Enterprise Log Manager auf die neueste Version oder den neuesten Service Pack, indem Sie alle Module, die zum Download verfügbar sind, herunterladen.

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. Mit dieser Vorgehensweise lassen sich die neuen Server korrekt registrieren.

Befolgen Sie diese Richtlinien:

1. Überprüfen Sie die Konfiguration für automatische Software-Updates, um sicherzustellen, dass die Basiskonfiguration vollständig ist.
   a. Klicken Sie auf die Unterregisterkarte "Services" in der Registerkarte "Verwaltung", und wählen Sie das Modul "Automatisches Software-Update" aus.
   b. Wählen Sie für "Automatischer Neustart nach Aktualisierung des Betriebssystems" die Option "Nein" aus.
   c. Ziehen Sie das Protokollmanagermodul in die ausgewählte Liste, wenn nicht bereits ausgewählt.
   d. Überprüfen Sie, dass alle erforderlichen Werte auf globaler Ebene konfiguriert sind.
   e. Überprüfen Sie, dass für jeden CA Enterprise Log Manager-Server alle erforderlichen Werte konfiguriert sind.

   Hinweis: Aktualisieren Sie, in föderierten Umgebungen, übergeordnete vor untergeordneten Elementen.

   Ein selbstüberwachendes Ereignis, das angibt, dass automatische Software-Updates installiert wurden, weist auf den Abschluss des Vorgangs hin.

2. Überprüfen Sie die Konfiguration für automatische Software-Updates, um sicherzustellen, dass die Basiskonfiguration vollständig ist.

   a. Klicken Sie auf die Unterregisterkarte "Services" in der Registerkarte "Verwaltung", und wählen Sie das Modul "Automatisches Software-Update" aus.

   b. Wählen Sie für "Automatischer Neustart nach Aktualisierung des Betriebssystems" die Option "Nein" aus.

   c. Ziehen Sie alle übrigen Module, die heruntergeladen werden sollen, in die ausgewählten Liste.

   Hinweis: Aktualisieren Sie, in föderierten Umgebungen, übergeordnete vor untergeordneten Elementen.

3. Wenn der Prozess des automatischen Software-Updates abgeschlossen ist, starten Sie jeden CA Enterprise Log Manager-Server neu.

   Ein selbstüberwachendes Ereignis, das angibt, dass automatische Software-Updates installiert wurden, weist auf den Abschluss des Vorgangs hin.

4. Aktualisieren Sie Agenten und Connectors wie folgt:

   a. Klicken Sie auf die Registerkarte "Verwaltung" und dann auf die Unterregisterkarte "Protokollerfassung", und wählen Sie "Agenten-Explorer" aus.

   b. Bestimmen Sie, ob automatische Software-Updates auf Agenten-Explorer-Ebene, auf Agentengruppen-Ebene oder Agenten-Ebene angewendet werden sollen.

   c. Wählen Sie die gewünschte Ebene aus, und klicken Sie auf die Schaltfläche "Automatisches Software-Update".

   d. Wenden Sie die Updates auf Agenten an, wenn Agenten zu den heruntergeladenen Modulen gehören.

   e. Klicken Sie erneut auf die Schaltfläche "Automatisches Software-Update".

   f. Wenden Sie, wenn verfügbar, Aktualisierungen auf Connectors an.

5. 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: Überprüfen Sie die Versionshinweise auf bekannte Probleme im Zusammenhang mit automatischen Software-Updates.

Weitere Informationen:

Automatischer Neustart nach Aktualisierung des Betriebssystems während SP-Upgrade (siehe Seite 66)
Ein aktualisierter Syslog-Protokollsensor unter r12.1 SP1 macht eine Aktualisierung zu Integrationen auf Windows-Agenten erforderlich (siehe Seite 74)

Kapitel 2: Betriebsumgebung

Dieses Kapitel enthält folgende Themen:

Hardware- und Softwarevoraussetzungen

CA Enterprise Log Manager installiert beim anfänglichen Setup das Betriebssystem Red Hat Enterprise Linux.

Im CA Enterprise Log Manager Certification Matrix Index werden die Verknüfungen zu allen CA Enterprise Log Manager-Zertifizierungsmatrizen aufgelistet. Dies umfasst folgende Matrizen:

- Serverhardware und -software

  Serverhardware und -software-Zertifizierungsmatrix für CA Enterprise Log Manager

- Agentenhardware und -software

  Agentenhardware und -software-Zertifizierungsmatrix für CA Enterprise Log Manager

- Protokollsensoren und die entsprechende Betriebssystemunterstützung

  Protokollsensor-Zertifizierungsmatrix für CA Enterprise Log Manager

- Produktintegrationen

  Produktintegrationsmatrix für CA Enterprise Log Manager

- Zertifizierung mit CA Audit iRecorders

  Audit iRecorder-Zertifizierungsmatrix für CA Enterprise Log Manager

Sie können mit den folgenden Browsern und dem Adobe Flash Player 9 oder 10 auf CA Enterprise Log Manager zugreifen:

- Internet Explorer 6 SP2 (nur Nicht-FIPS-Modus)
- Internet Explorer 7 oder 8 (FIPS-Modus oder Nicht-FIPS-Modus)
- Mozilla Firefox 2.0.x und 3.0.x (nur Nicht-FIPS-Modus)
- Mozilla Firefox 3.5.8 oder später (FIPS-Modus oder Nicht-FIPS-Modus)

Hinweis: Dateiexporte funktionieren nicht, wenn Sie mit einem Mozilla Firefox-Browser auf CA Enterprise Log Manager zugreifen.

Erforderliche Energieeinstellungen für bestimmte HP- und IBM-Computer

Wenn für Installationen von CA Enterprise Log Manager auf Servern der Serie HP Proliant DL 380G5 oder IBM X3650t die standardmäßigen Energieeinstellungen verwendet werden, können Probleme mit iGateway den Betrieb verlangsamen bzw. andere Schnittstellenprobleme einen manuellen Dienstneustart erforderlich machen.

Ändern Sie die Einstellungen, bevor Sie CA Enterprise Log Manager installieren, um diese potenziellen Probleme zu vermeiden.

Hinweis: Wenn Sie CA Enterprise Log Manager bereits installiert haben, können Sie die Anwendung beenden, die Einstellungen wie beschrieben ändern und den Computer neu starten.

So ändern Sie die Energieeinstellungen auf HP Proliant DL 380G5:

1. Greifen Sie auf das Menü "BIOS-Einstellungen" zu.
2. Navigieren Sie zu den Energieverwendungs-Einstellungen.
3. Wählen Sie aus den verfügbaren Optionen "OS Control Mode" aus.

   Hinweis: Die Standardeinstellung ist "HP Dynamic Power Settings Mode".

So ändern Sie die Energieeinstellungen auf IBM X3650:

1. Greifen Sie auf das Menü "BIOS-Einstellungen" zu.
2. Navigieren Sie zu den Energieverwendungs-Einstellungen.
3. Deaktivieren Sie folgende Parameter:
   - Active Energy Manager
   - Enhanced C1 Power State

Bildschirmauflösung

Es ist eine Bildschirmauflösung von mindestens 1024 x 768 Pixel erforderlich. Für optimale Anzeigeergebnisse wird eine Bildschirmauflösung von1280 x 1024 empfohlen.

CA EEM-Serverreferenzen

Informationen zu den bei einem bestehenden CA EEM-Server unterstützten Betriebssystemen finden Sie im *CA Embedded Entitlements Manager-Handbuch "Erste Schritte"*. Dieses Handbuch ist im CA Enterprise Log Manager-Bookshelf enthalten.

Sie können diesen Bookshelf auch beim technischen Support herunterladen. Wenn Sie Hilfe benötigen, wenden Sie sich an den Technischen Support unter http://ca.com/support.

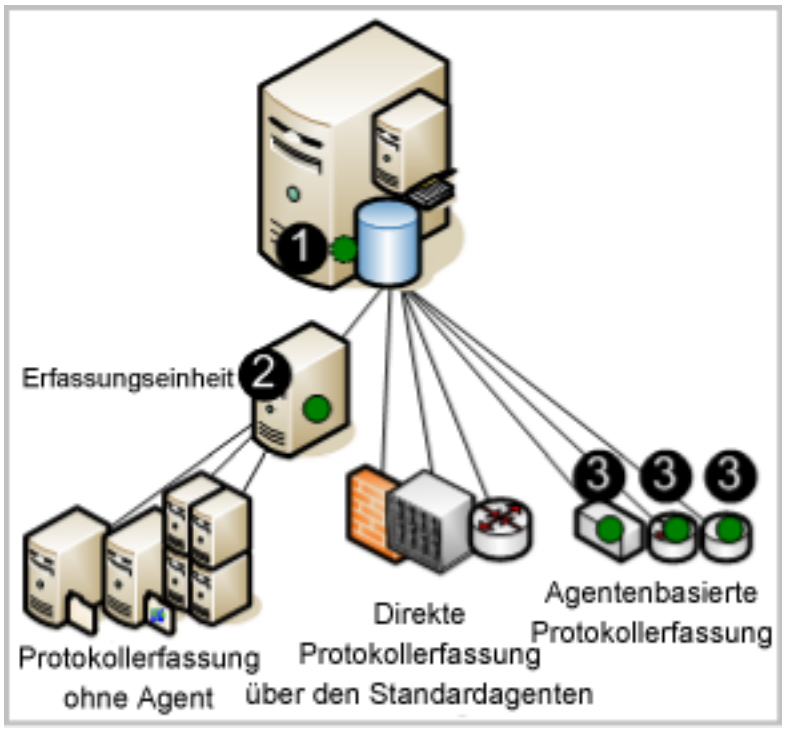
Kapitel 3: Leistungsmerkmale

Dieses Kapitel enthält folgende Themen:

Protokollerfassung

Der CA Enterprise Log Manager-Server kann so eingerichtet werden, dass er Protokolle mit einer oder mehreren unterstützten Techniken erfasst. Die Techniken unterscheiden sich durch Typ und Speicherort der Komponente, die die Protokolle abhört und erfasst. Diese Komponenten werden auf Agents konfiguriert.

Die folgende Abbildung zeigt ein Single-Server-System, auf dem der Ort der Agents mit einem dunklen (grünen) Kreis dargestellt wird.



Die Nummern in den Abbildungen beziehen sich auf folgende Schritte:

1. Konfigurieren Sie den Standardagent auf CA Enterprise Log Manager, um Ereignisse direkt von den angegebenen Syslog-Quellen abzurufen.
2. Konfigurieren Sie den Agent, der auf einem Windows-Sammelpunkt installiert wurde, um Ereignisse von angegebenen Windows-Servern zu erfassen und an CA Enterprise Log Manager zu senden.
3. Konfigurieren Sie Agents, die auf Hosts installiert wurden, auf denen Ereignisquellen ausgeführt werden, um den konfigurierten Ereignistyp zu erfassen und eine Unterdrückung durchzuführen.

Hinweis: Datenverkehr vom Agent zum Ziel-CA Enterprise Log Manager-Server wird immer verschlüsselt.

Die einzelnen Protokollerfassungstechniken haben folgende Vorteile:

- Direkte Protokollerfassung

  Bei der direkten Protokollerfassung konfigurieren Sie den Syslog-Listener auf dem Standardagent, so dass dieser Ereignisse von den von Ihnen angegebenen vertrauenswürdigen Quellen empfängt. Sie können andere Connectors auch so konfigurieren, dass sie Ereignisse von allen Ereignisquellen erfassen, die mit der Soft-Appliance-Plattform kompatibel sind.

  Vorteil: Sie müssen keinen Agents installieren, um Protokolle von Ereignisquellen zu erfassen, die sich in unmittelbarer Nähe des CA Enterprise Log Manager-Servers befinden.

- Erfassung ohne Agent

  Bei der Erfassung ohne Agent gibt es keinen lokalen Agent an den Ereignisquellen. Stattdessen wird an einem bestimmten Sammelpunkt ein Agent installiert. Für jede Zielereignisquelle wird auf diesem Agent ein Connector konfiguriert.

  Vorteil: Sie können Protokolle von Ereignisquellen erfassen, die auf Servern ausgeführt werden, auf denen keine Agenten installiert werden können, beispielsweise auf Servern, auf denen die Installation von Agenten aufgrund von betriebsinternen Richtlinien nicht zugelassen ist. Die Übermittlung ist garantiert, wenn beispielsweise die ODBC-Protokollerfassung korrekt konfiguriert wurde.

- Agentbasierte Erfassung

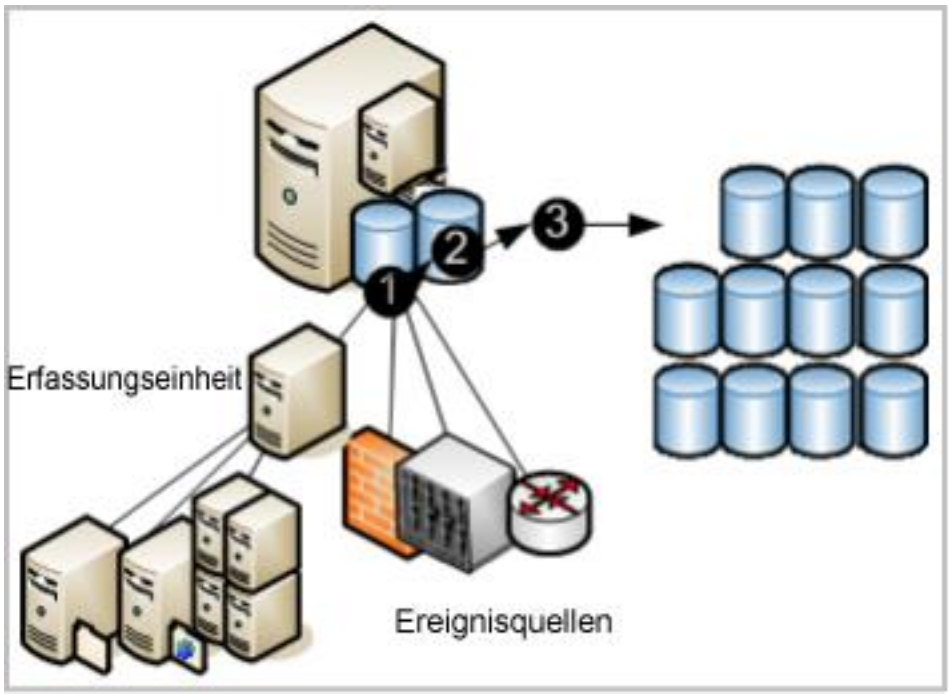
  Bei der agentbasierten Erfassung wird ein Agent überall dort installiert, wo ein oder mehrere Ereignisquellen ausgeführt werden und ein Connector für jede Ereignisquelle konfiguriert wurde.

  Vorteil: Sie können Protokolle von Quellen erfassen, auch wenn die Bandbreite zwischen Quelle und CA Enterprise Log Manager nicht ausreicht, um eine direkte Protokollerfassung zu unterstützen. Sie können mit dem Agenten die Ereignisse filtern und so den Datenverkehr im Netzwerk reduzieren. Die Ereignisübermittlung ist garantiert.

Hinweis: Weitere Informationen zur Konfiguration von Agents finden Sie im *Verwaltungshandbuch*.

Protokollspeicherung

CA Enterprise Log Manager bietet die Möglichkeit der verwalteten eingebetteten Protokollspeicherung für kürzlich archivierte Datenbanken. Ereignisse, die durch Agenten von Ereignisquellen erfasst worden sind, durchlaufen den im folgenden Diagramm dargestellten Speicherlebenszyklus.



Die Nummern in den Abbildungen beziehen sich auf folgende Schritte:

1. Neue Ereignisse werden unabhängig von der verwendeten Technik an CA Enterprise Log Manager gesendet. Der Status der eingehenden Ereignisse hängt von der verwendeten Erfassungstechnik ab. Eingehende Ereignisse müssen verfeinert werden, bevor sie in die Datenbank eingefügt werden können.
2. Wenn die Datenbank mit den verfeinerten Datensätzen die konfigurierte Größe erreicht hat, werden alle Datensätze in einer Datenbank komprimiert und unter einem eindeutigen Namen gespeichert. Durch das Komprimieren der Protokolldaten werden die Kosten für das Verschieben und Speichern der Daten reduziert. Die komprimierte Datenbank kann entweder basierend auf einer Auto-Archivierungskonfiguration automatisch verschoben werden, oder sie kann manuell gesichert und verschoben werden, bevor sie das konfigurierte Löschalter erreicht. (Automatisch archivierte Datenbanken werden sofort nach dem Verschieben aus der Quelle gelöscht.)
3. Wenn Sie komprimierte Datenbanken täglich per Auto-Archivierung auf einen Remote-Server verschieben, können Sie diese Sicherungen, falls gewünscht, in einen langfristigen Off-Site-Protokollspeicher verschieben. Mit Hilfe von beibehaltenen Protokollsicherungen können Sie die Konformität mit Gesetzen und Bestimmungen aufrechterhalten, die besagen, dass Protokolle sicher erfasst, über eine bestimmte Anzahl von Jahren zentral gespeichert und für Überprüfungen verfügbar gemacht werden müssen. (Sie können Protokolle aus einem langfristigen Speicher jederzeit wiederherstellen.)

Hinweis: Weitere Informationen zum Konfigurieren des Ereignisprotokollspeichers einschließlich der Einrichtung der Auto-Archivierung finden Sie im *Implementierungshandbuch*. Weitere Informationen zum Wiederherstellen der Sicherungen für Untersuchungen und Berichte finden Sie im *Verwaltungshandbuch*.

Standarddarstellung von Protokollen

Protokolle, die von Anwendungen, Betriebssystemen und Geräten erstellt werden, verwenden eigene Formate. CA Enterprise Log Manager verfeinert die erfassten Protokolle, um die Datenberichte zu standardisieren. Dieses Standardformat erleichtert Auditoren und leitenden Managern den Vergleich von Daten, die in verschiedenen Quellen erfasst wurden. Technisch vereinfacht die ELM-Schemadefinition (Common Event Grammar, CEG) von CA die Implementierung der Ereignisnormalisierung und -klassifizierung.

Die ELM-Schemadefinition verwendet für die Normalisierung unterschiedlicher Ereignisaspekte verschiedene Felder. Dazu zählen folgende Felder:

- Idealmodell (Technologieklasse, z. B. Antivirus, DBMS und Firewall)
- Kategorie (z. B. Identitätsverwaltung und Netzwerksicherheit)
- Klasse (z. B. Kontenverwaltung und Gruppenverwaltung)
- Aktion (z. B. Kontenerstellung und Gruppenerstellung)
- Ergebnisse (z. B. Erfolgreich und Fehler)

Hinweis: Weitere Informationen zu den Regeln und Dateien für die Ereignisverfeinerung finden Sie im *CA Enterprise Log Manager-Verwaltungshandbuch*. Details zum Normalisieren und Kategorisieren von Ereignissen finden Sie in der Online-Hilfe im Abschnitt zur ELM-Schemadefinition.

Konformitätsberichte

Mit CA Enterprise Log Manager können Sie sicherheitsrelevante Daten erfassen und verarbeiten und in Berichte für interne oder externe Auditoren umwandeln. Sie können mit Fragen und Berichten für Untersuchungen interagieren. Sie können die Berichterstellung durch die Planung von Berichtsaufträgen automatisieren.

Das System stellt Folgendes zur Verfügung:

- Leicht zu verwendende Abfragefunktion mit Kennungen
- Echtzeitnahe Berichte
- Zentral durchsuchbare, verteilte Archive kritischer Protokolle

Der Fokus liegt auf Konformitätsberichten und weniger auf der Echtzeitzuordnung von Ereignissen und Alarmen. Gesetze und Bestimmungen erfordern Berichte, mit denen die Einhaltung von branchenspezifischen Regelungen nachgewiesen werden kann. CA Enterprise Log Manager bietet Berichte mit folgenden Kennungen für eine einfache Identifizierung:

- Basel II
- COBIT
- COSO
- EU-Datenschutzrichtlinie
- FISMA
- GLBA
- HIPAA
- ISO\IEC 27001\2
- JPIPA
- JSOX
- NERC
- NISPOM
- PCI
- SAS 70
- SOX

Sie können vordefinierte Protokollberichte überprüfen oder auf Grundlage von selbst definierten Kriterien Suchläufe durchführen. Neue Berichte erhalten Sie mit den automatischen Software-Updates.

Protokollanzeigefunktionen werden wie folgt unterstützt:

- Bedarfsbasierte Abfragefunktion mit vordefinierten oder benutzerdefinierten Abfragen, deren Ergebnisse bis zu 5000 Datensätze umfassen können
- Schnelle Suche über Eingabeaufforderungen nach bestimmten Hostnamen, IP-Adressen, Portnummern oder Benutzernamen
- Geplante und bedarfsbasierte Berichterstattung mit standardisiertem Berichtsinhalt
- Geplante Abfragen und Alarme
- Basisberichte mit Trendinformationen
- Interaktive grafische Ereignisanzeige
- Automatische Berichterstattung mit E-Mail-Anhang
- Richtlinien zur automatischen Berichtsaufbewahrung

Hinweis: Weitere Informationen zu vordefinierten Abfragen und Berichten oder zur eigenen Erstellung finden Sie im *CA Enterprise Log Manager-Verwaltungshandbuch*.

Alarm bei Verletzung von Richtlinien

Mit CA Enterprise Log Manager können Sie bei Ereignissen, die ein zeitnahes Eingreifen erfordern, das Versenden von Alarmen automatisieren. Sie können Aktionsalarme auch jederzeit über CA Enterprise Log Manager überwachen, indem Sie ein Intervall festlegen, das einen beliebigen Zeitraum von "die letzten fünf Minuten" bis "die letzten dreißig Tage" umfassen kann. Alarme werden auch automatisch an ein RSS-Feed gesendet, auf das über einen Webbrowser zugegriffen werden kann. Optional können Sie auch andere Ziele angeben, u. a. E-Mail-Adressen, einen CA IT PAM-Prozess, der beispielsweise Help-Desk-Tickets erstellt, oder eine oder mehrere SNMP-Trap-IP-Zieladressen.

Um Ihnen den Einstieg zu erleichtern, sind verschiedene vordefinierte Abfragen für die Planung von Aktionsalarmen verfügbar. Beispiele:

- Übermäßige Benutzeraktivität
- Hohe durchschnittliche CPU-Auslastung
- Geringer freier Speicherplatz
- Sicherheitsereignisprotokoll in den letzten 24 Stunden gelöscht
- Windows-Überwachungsrichtlinie in den letzten 24 Stunden geändert

Einige Abfragen verwenden Schlüssellisten, bei denen Sie die in der Abfrage verwendeten Werte verfügbar machen. Einige Schlüssellisten umfassen vordefinierte Werte, die Sie ergänzen können. Dazu gehören beispielsweise Standardkonten und berechtigte Gruppen. Andere Schlüssellisten, beispielsweise die Liste für unternehmenskritische Ressourcen, verwenden keine Standardwerte. Nach deren Konfiguration können Warnungen für vordefinierte Abfragen geplant werden, z. B.:

- Hinzufügen oder Entfernen von Gruppenmitgliedern durch berechtigte Gruppen
- Erfolgreiche Anmeldung durch Standardkonto
- Keine Ereignisse von unternehmenskritischen Quellen erhalten

Schlüssellisten können manuell, durch Import einer Datei oder durch Ausführen eines CA IT PAM-Prozesses mit dynamischen Werten aktualisiert werden.

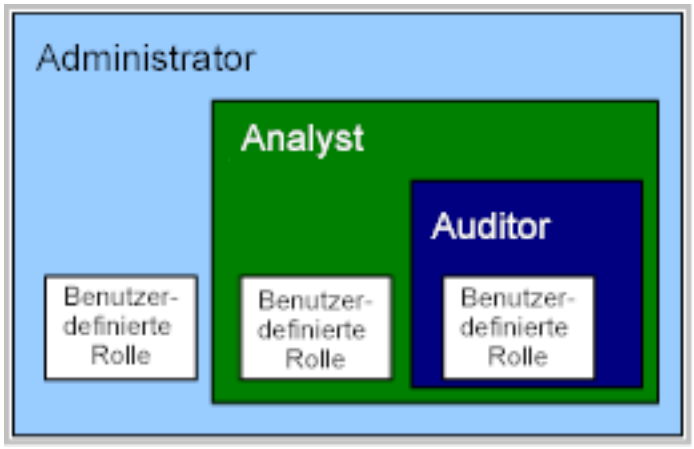
Hinweis: Einzelheiten zu Aktionsalarmen finden Sie im *CA Enterprise Log Manager-Administrationshandbuch*.

Rollenbasierter Zugriff

CA Enterprise Log Manager bietet drei vordefinierte Anwendungsgruppen oder Rollen. Administratoren weisen Benutzern folgende Rollen zu, um Zugriffsrechte für CA Enterprise Log Manager-Funktionen zu definieren:

- Administrator
- Analyst
- Auditor

Der Auditor hat Zugriff auf alle Funktionen. Der Analyst hat über die Auditor-Funktionen hinaus Zugriff auf weitere Funktionen. Der Administrator hat Zugriff auf alle Funktionen. Sie können benutzerdefinierte Rollen mit entsprechenden Richtlinien erstellen, die den Benutzerzugriff auf Ressourcen so einschränken, wie es für Ihre betriebsinternen Anforderungen erforderlich ist.



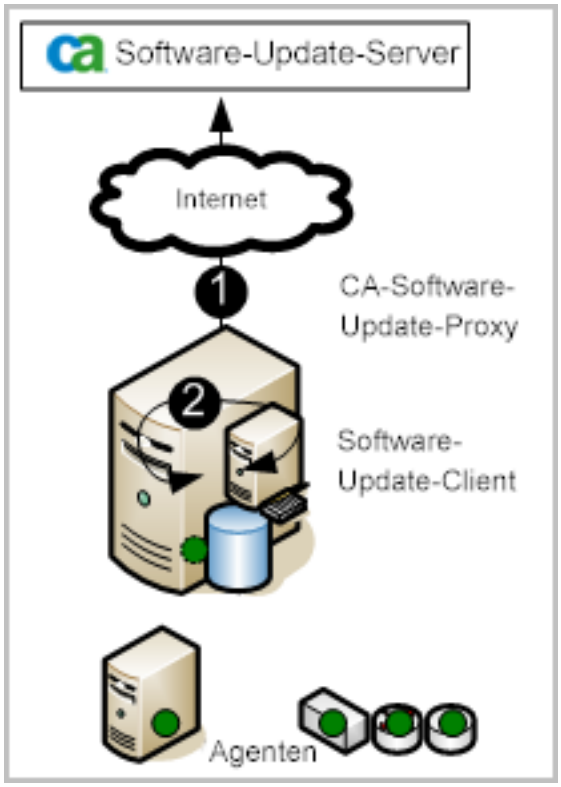
Administratoren können den Zugriff auf jede Ressource anpassen, indem sie eine benutzerdefinierte Anwendungsgruppe mit entsprechenden Richtlinien erstellen und diese Anwendungsgruppe oder Rolle bestimmten Benutzerkonten zuweisen.

Hinweis: Weitere Informationen zur Planung oder Erstellung von Rollen, benutzerdefinierten Richtlinien und Zugriffsfiltern finden Sie im *CA Enterprise Log Manager-Verwaltungshandbuch*.

Verwalten Von Automatischen-Software-aktualisieren

Das-Modul-Für-Automatische-Software-aktualisieren ist ein Dienst, bei dem Sie automatische-Software-aktualisieren-Über-Höhlen-CA-Software-Update-Server-Nach Einem Festgelegten-Plan-Automatisch Herunterladen Und ein CA Enterprise Log Manager-Server-Verteilen-Können. Wenn-Ein-Automatisches-Software-Aktualisierungs-auch das Modul für-Agenten-Betrifft, wird als Bereitstellung dieser aktualisieren sterben ein Agenten-Durch als Benutzer initiiert sterben. *Automatische Software-Updates* sind Aktualisierungen für CA Enterprise Log Manager-Softwarekomponenten und das Betriebssystem, Patch sowie Inhaltsaktualisierungen, wie z. B. Berichte.

Sterben Sie als folgende Abbildung zeigt ein Szenario mit der einfachsten direkten Internetverbindung aus:



Sterben Sie als Nummern in Höhle Abbildungen beziehen sich auf folgende Schritte:

1. Der-CA Enterprise Log Manager-Server-kontaktiert als Standardserver für das-Software-Aktualisierungs-Höhlen-CA-Software-Update-Server-Und Lädt Alle Verfügbaren Neuen-aktualisieren-Herunter. Der CA Enterprise Log Manager-Server erstellt eine Sicherung und verschiebt dann als Inhaltsaktualisierungen zur eingebetteten Komponente des Verwaltungsservers sterben, der als Inhaltsaktualisierungen für alle anderen CA Enterprise Log Managers speichert sterben.
2. Der-CA Enterprise Log Manager-Server-Installiert-Als-Client-Für-Automatische-Software-aktualisieren das Produkt und als benötigten-Betriebssystem-Aktualisierungs-Selbständig sterben.

Hinweis: Weitere Informationen Zum Planen-und Konfigurieren von automatischen-Software-aktualisieren finden Sie im *Implementierungshandbuch*. Weitere Informationen Zum Verfeinern-und Bearbeiten der Konfiguration für automatische-Software-aktualisieren und für das Anwenden von aktualisieren auf Agenten finden Sie im *Verwaltungshandbuch*.

Unterstützung für IPv6-IP-Adressen

Zuvor war die Angabe von IP-Adressen auf die für IPv4 übliche punktierte Dezimalschreibweise beschränkt gewesen. Bei der aktuellen Version können Sie nun in jedem IP-Adressfeld IPv6-Adressen angeben. IPv6 nutzt anstelle der von IPv4 verwendeten 32-Bit-Adressen 128-Bit-Adressen. Alle auf der IP-Adressenversion basierenden Richtlinien unterstützen sowohl IPv6 als auch IPv4.

Sie können IPv4-zugeordnete IPv6-Adressen oder das traditionelle IPv6-Format nutzen. Das IPv4-zugeordnete IPv6-Adressformat ermöglicht die Darstellung einer IPv4-Adresse eines IPv4-Knotens als IPv6-Adresse.

- Die bevorzugte IPv6-Form wird in acht Gruppen von vier Hexadezimalzahlen dargestellt (x:x:x:x:x:x:x:x). Jedes x steht für eine bis vier Hexadezimalzahlen von acht 16-Bit-Teilen der Adresse.
- Die IPv4-zugeordnete IPv6-Adresse, vorteilhaft in einer gemischten Umgebung mit IPv4- und IPv6-Knoten, hat das Format 0:0:0:0:0:FFFF:d.d.d.d, wobei jedes "d" einen Dezimalwert der Adresse darstellt (für IPv4 übliche punktierte Dezimalschreibweise).

  Wichtig! IPv4-kompatible IPv6-Adressen im Format 0:0:0:0:0:0:d.d.d.d sind gemäß RFC 4291 mittlerweile veraltet, da der aktuelle IPv6-Übergangsmechanismus diese Adressen nicht mehr verwendet.

Die folgende Adresse ist eine gültige IPv6-Adresse im traditionellen Format.

2001:0db8:85a3:08d3:1319:8a2e:0370:7334

Wenn eine oder mehrere der vierstelligen Gruppen 0000 lauten, können die Nullen ausgelassen werden und durch zwei Doppelpunkte (::) ersetzt werden. Führende Nullen in einer Gruppe können ebenfalls ausgelassen werden. Die folgenden beispielhaften IP-Adressen sind gleichwertig:

- 2001:0db8:0000:0000:0000:0000:1428:57ab
- 2001:0db8::1428:57ab
- 2001:db8:0:0:0:0:1428:57ab
- 2001:db8::1428:57ab

Wenn Sie IPv4-Adressen mit IPv4-zugeordneten Adressen ersetzen, orientieren Sie sich an folgenden Beispielen:

- 0:0:0:0:0:FFFF:192.168.2.128
- 0:0:0:0:0:FFFF:172.16.2.128

Alternativ können Sie das folgende komprimierte Format verwenden:

- ::FFFF:192.168.2.128
- ::FFFF:172.16.2.128

Kapitel 4: Neue und geänderte Funktionen in r12.1

Dieses Kapitel enthält folgende Themen:

Offener API-Zugriff

CA Enterprise Log Manager ermöglicht es Ihnen, mit Hilfe von API-Aufrufen und unter Verwendung des Abfrage- und Berichtsmechanismus auf Daten im Ereignis-Repository zuzugreifen und sie einem Web-Browser anzuzeigen. Sie können die API auch verwenden, um CA Enterprise Log Manager-Abfragen oder -Berichte in eine CA-Benutzeroberfläche oder die Benutzeroberfläche eines Drittanbieters einzubetten.

Zu den CA Enterprise Log Manager API-Funktionen zählen:

- Authentifizierte, sichere APIs
- Produktregistrierung für Single Sign-On (SSO)
- Abruf von nach Kennungen gefilterten Abfrage- oder Berichtslisten
- Anzeige einer Abfrage oder eines Berichts in der interaktiven CA Enterprise Log Manager-Benutzeroberfläche, die das Filtern und Einbetten in eine Benutzerschnittstelle zulässt

Weitere Informationen zur API finden Sie im *AP-Programmierungshandbuch* und in der Online-Hilfe.

Ausführbare Alarme: CA IT PAM-Integration

Mit Hilfe geplanter Alarme, die Inhalte von Protokolldatensätzen abfragen, ermittelt CA Enterprise Log Manager potenzielle Kontrollverletzungen und verdächtige IT-Aktivitäten. CA Enterprise Log Manager benachrichtigt die IT-Sicherheitsverantwortlichen, die alle Alarme überprüfen und entscheiden, ob eine Abhilfemaßnahme erforderlich ist. Die typischen Prüfmaßnahmen sind meist Routine und gut zur Automatisierung geeignet. Mit Hilfe einer engen Integration von CA Enterprise Log Manager und CA IT PAM können diese Routineantwortaktionen automatisch durchgeführt werden. So müssen IT-Sicherheitsverantwortliche keine sich wiederholenden Aufgaben durchführen und sich nur mit den wichtigsten Problemen befassen.

CA IT PAM-Integration erlaubt es Ihnen, Anforderungen in CA Service Desk zu erstellen, indem Sie einen vordefinierten CA IT PAM Ereignis-/Alarmausgabeprozess von Alarmen ausführen. Sie können außerdem benutzerdefinierte IT PAM Ereignis-/Alarmausgabeprozesse von CA Enterprise Log Manager aus ausführen, mit denen andere Antworten auf verdächtige Ereignisse automatisiert werden können.

Details finden Sie im Abschnitt "Arbeiten mit CA IT PAM Ereignis-/Alarmausgabeprozessen" im Kapitel "Aktionsalarme" des CA Enterprise Log Manager-*Administrationshandbuchs*.

Ausführbare Alarme: SNMP-Integration mit NSM-Produkten

Alarme werden generiert, wenn durch geplante Abfragen Ereignisse abgerufen werden, die auf verdächtige Aktivitäten hinweisen. Sie können das Senden solcher Alarme als SNMP-Traps an Netzwerksicherheits-Überwachungsprodukte (network security monitoring, NSM) wie z. B. CA Spectrum oder CA NSM automatisieren. Bereiten Sie die Zielprodukte so vor, dass sie SNMP-Traps von CA Enterprise Log Manager empfangen und interpretieren, konfigurieren Sie die Zielorte, und geben Sie dann die Ereignisinformationen an, die gesendet werden sollen.

Details finden Sie im Abschnitt "Arbeiten mit SNMP-Traps" im Kapitel "Aktionsalarme" des CA Enterprise Log Manager-*Administrationshandbuch*.

ODBC- und JDBC-Zugriff

CA Enterprise Log Manager gewährt mit ODBC und JDBC schreibgeschützten Zugriff auf erfasste Ereignisprotokollinformationen. Diese Zugriffsart können Sie folgendermaßen nutzen:

- Erstellen von benutzerdefinierten Berichten mit Hilfe von Tools wie "BusinessObjects Crystal Reports"

- Abrufen ausgewählter Protokollinformationen zur Verwendung mit einem Korrelationsmodul
- Überprüfen von Protokollen auf Angriffe oder zum Aufspüren von Malware

Bei der ODBC- und JDBC-Zugriffsfunktion wird ein Client verwendet, den Sie auf einem geeigneten Server in Ihrem Netzwerk installieren. Der CA Enterprise Log Manager-Server installiert seine serverseitigen Komponenten während der Installation des automatischen Software-Updates automatisch.

Information zur Installation finden Sie im *Implementierungshandbuch*. Information zur Konfiguration und Beispiele finden Sie im *Administrationshandbuch*.

Relevanz von Identität und Asset: CA IT PAM-Integration

CA IT PAM-Integration erlaubt es Ihnen, aktualisierte Werte für einen bestimmten Schlüssel beizubehalten, indem ein "CA IT PAM-Prozess für dynamische Werte " ausgeführt wird. Ein Prozess mit dynamischen Werten ruft die aktuellen Werte aus Repositorys ab, in denen aktuelle Daten gespeichert sind. Wenn Sie einen Prozess erstellen, der Werte für kritische Assets aus der Asset-Datei oder -Datenbank abruft, können Sie den Schlüssel "Kritische_Assets" in vordefinierten Berichten und Abfragen durch Anklicken einer Schaltfläche aktualisieren.

Details finden Sie im Abschnitt "Arbeiten mit SNMP-Traps" im Kapitel "Aktionsalarme" des CA Enterprise Log Manager-*Administrationshandbuch*.

Erweiterte direkte Protokollerfassung durch den Standardagenten

Bei der Installation von CA Enterprise Log Manager wird der Syslog-Listener mit der Bezeichnung "Syslog_Connector" auf dem Standardagenten bereitgestellt, um die Erfassung von Syslog-Ereignissen zu ermöglichen. Die Linux_localsyslog-Integration mit dem zugehörigen Connector, Linux_localsyslog_Connector, steht ebenfalls zur Erfassung von Syslog-Ereignissen zur Verfügung.

Der Agent kann nun außer Syslog-Ereignissen auch andere Ereignisse direkt erfassen. Mit dem WinRm-Connector kann der Standardagent Ereignisse von Produkten erfassen, die auf Microsoft Windows-Plattformen ausgeführt werden, wie z. B. Active Directory Certificate Services und Microsoft Office Communication Server. Mit dem ODBC-Connector kann der Standardagent Ereignisse von mehren Datenbanken erfassen, wie z. B. Oracle9i und SQL Server 2005, sowie von Datenbanken, deren Ereignisse in diesen Datenbanken gespeichert werden.

Zeitplan für automatische Updates für Clients für automatische Software-Updates

Wenn Sie den CA Enterprise Log Manager-Server zum ersten Mal installieren, konfigurieren Sie globale Einstellungen für alle Services. Hierzu zählen auch automatische Software-Updates. Für automatische Software-Updates fungiert der erste installierte Server als Standard-Proxy für automatische Software-Updates. Sie konfigurieren die Startzeit für die Aktualisierung und die Häufigkeit, mit der dieser Proxy auf dem CA-Server für automatische Software-Updates nach Aktualisierungen sucht. Bei der Installation weiterer Server werden diese standardmäßig als Clients für automatische Software-Updates installiert. Zusätzliche Server konfigurieren Sie auf der lokalen Ebene. Zur Konfiguration auf der lokalen Ebene wählen Sie den Namen des zu konfigurierenden Servers aus und setzen anschließend ausgewählte globale Konfigurationen außer Kraft.

Die Startzeit der Aktualisierung von Clients für automatische Software-Updates wird standardmäßig von der globalen Einstellung geerbt. Wenn die geerbte Einstellung nicht manuell außer Kraft gesetzt wird, um eine Verzögerung zu erzwingen, kommt es zu Problemen. Zur Vermeidung solcher Probleme wird der Aktualisierungszeitplan für Clients jetzt mit einer Verzögerung von 15 Minuten automatisiert. Der Aktualisierungszeitplan für Clients für automatische Software-Updates muss daher nicht mehr manuell konfiguriert werden.

Kapitel 5: Neue und geänderte Funktionen in r12.1 SP1

Dieses Kapitel enthält folgende Themen:

FIPS 140-2-Kompatibilität - Übersicht

Die FIPS-Veröffentlichung (Federal Information Processing Standards) 140-2 ist ein Sicherheitsstandard für die kryptographischen Bibliotheken und Algorithmen, die ein Produkt für die Verschlüsselung verwenden sollte. Die FIPS 140-2-Verschlüsselung wirkt sich auf die Übermittlung aller sensiblen Daten zwischen verschiedenen CA-Produktkomponenten sowie zwischen CA-Produkten und Produkten von Drittanbietern aus. In der FIPS-Veröffentlichung 140-2 sind die Anforderungen festgelegt, die erfüllt werden müssen, um innerhalb eines Sicherheitssystems zum Schutz von sensiblen, nicht klassifizierten Daten kryptographische Algorithmen zu verwenden.

Durch die Verwendung von FIPS-konformen Algorithmen im FIPS-Modus kann der Ereignisdatenverkehr in CA Enterprise Log Manager gesichert und FIPS-kompatibel stattfinden. Gleichzeitig läuft CA Enterprise Log Manager standardmäßig im Nicht-FIPS-Modus, in dem der Ereignisdatenverkehr *nicht* durch FIPS-kompatible Algorithmen gesichert wird. Bei CA Enterprise Log Manager-Servern in föderierten Netzwerken können diese beiden Betriebsarten nicht kombiniert werden. Dies bedeutet, dass ein Server, der im Nicht-FIPS-Modus betrieben wird, Abfrage- und Berichtsdaten nicht mit Servern im FIPS-Modus gemeinsam benutzen kann.

Informationen zum Aktivieren und Deaktivieren des FIPS-Modus finden Sie im Abschnitt "Installieren von CA Enterprise Log Manager" des *Implementierungshandbuchs* und in der Onlinehilfe für den Systemstatus-Service.

Weitere Informationen:

Betriebsarten (siehe Seite 38)
Verschlüsselungsbibliotheken (siehe Seite 38)
Verwendete Algorithmen (siehe Seite 39)
Info zu Zertifikaten und Schlüsseldateien (siehe Seite 40)
Beschränkungen in der Unterstützung von FIPS (siehe Seite 41)
Konfigurieren von Microsoft Internet Explorer, um in FIPS-Modus auf CA Enterprise Log Manager zuzugreifen (siehe Seite 43)
Konfigurieren von Mozilla Firefox, um in FIPS-Modus auf CA Enterprise Log Manager zuzugreifen (siehe Seite 43)

Betriebsarten

CA Enterprise Log Manager kann in zwei Modi betrieben werden: FIPS-Modus oder Nicht-FIPS-Modus. Die Verschlüsselungsgrenzen sind in beiden Modi die selben, doch die Algorithmen sind unterschiedlich. Standardmäßig werden CA Enterprise Log Manager-Server im Nicht-FIPS-Modus betrieben. Benutzer mit der Administratorrolle können den Betrieb im FIPS-Modus aktivieren.

Nicht-FIPS-Modus

Dieser Modus verwendet für die Ereignisübertragung und andere Arten der Kommunikation zwischen dem CA Enterprise Log Manager- und dem CA EEM-Server eine bestimmte Kombination von Verschlüsselungsalgorithmen, die unter Umständen nicht den FIPS 140-2-Standards entsprechen.

FIPS-Modus

Dieser Modus verwendet für die Ereignisübertragung und andere Arten der Kommunikation zwischen dem CA Enterprise Log Manager- und dem CA EEM-Server FIPS-zertifizierte Verschlüsselungsalgorithmen.

Benutzer auf Administratorebene können die Betriebsarten von Agenten über den Agenten-Explorer-Knoten auf der Unterregisterkarte "Protokollerfassung" der Registerkarte "Verwaltung" überprüfen.

Weitere Informationen zum Wechseln zwischen FIPS- und Nicht-FIPS-Modus finden Sie in der Onlinehilfe für Systemstatusaufgaben oder im Abschnitt zur Servicekonfiguration des *Implementierungshandbuchs*.

Verschlüsselungsbibliotheken

In der FIPS 140-2-Veröffentlichung (Federal Information Processing Standards) sind die Anforderungen festgelegt, die erfüllt werden müssen, um innerhalb eines Sicherheitssystems zum Schutz von sensiblen, nicht klassifizierten Daten kryptographische Algorithmen zu verwenden.

In CA Enterprise Log Manager ist auch die Verschlüsselungsbibliothek Crypto-C Micro Edition (ME) v2.1.0.2 von RSA eingebettet, die offiziell anerkannt den FIPS 140-2-*Sicherheitsanforderungen für an kryptographische Module* entspricht. Die Nummer des Gültigkeitserklärungszertifikats für dieses Modul ist 865.

Verwendete Algorithmen

Computerprodukte, die FIPS 140-2-zertifizierte kryptographische Module verwenden, können nur FIPS-genehmigte Sicherheitsfunktionen verwenden. Diese umfassen AES (Advanced Encryption Algorithm), SHA-1 (Secure Hash Algorithm) und Protokolle auf höherer Ebene wie TLS v1.0, die in den FIPS 140-2-Handbüchern ausdrücklich erlaubt sind.

Im Nicht-FIPS-Modus verwendet CA Enterprise Log Manager die folgenden Algorithmen:

- AES 128
- Triple DES (3DES)
- SHA-1
- MD5
- SSL v3

Im FIPS-Modus verwendet CA Enterprise Log Manager die folgenden Algorithmen:

- AES 128
- Triple DES (3DES)
- SHA-1
- TLS v1

CA Enterprise Log Manager verwendet SHA-1 als standardmäßigen Digest Algorithm, um Kennwörter zu verschlüsseln und Serveranfragen zu signieren.

CA Enterprise Log Manager verwendet TLS v1.0 zur Kommunikation mit LDAP-Verzeichnissen, wenn die LDAP-Verbindung TLS verwendet, zur Kommunikation zwischen iTechnology-Komponenten, zur Kommunikation mit dem iGateway-Dienst im FIPS-Modus und für den Ereigniskanal zischen dem Agenten und dem logDepot-Dienst.

Info zu Zertifikaten und Schlüsseldateien

Das Upgrade auf CA Enterprise Log Manager r12.1 SP1 konvertiert das Format vorhandener P12-Zertifikate zum PEM-Format, um FIPS 140-2 zu unterstützen. Diese Konvertierung hat die Generierung der folgenden Dateien zur Folge:

- Zertifikatsdatei mit der Erweiterung ".cer"
- Schlüsseldatei mit der Erweiterung ".key"

Schlüsseldateien werden nicht verschlüsselt, und es liegt beim Benutzer, sie sowohl Server- als auch Agenthosts vor unbefugtem Zugriff zu schützen. Zum Schutz von Schlüsseln und Zertifikaten, die im Dateissystem gespeichert sind, verwendet die CA Enterprise Log Manager-Software-Appliance verschiedene Betriebssystem-Härtungsverfahren. CA Enterprise Log Manager unterstützt die Verwendung von externen Schlüsselspeichergeräten nicht.

CA Enterprise Log Manager verwendet die folgenden Zertifikate und Schlüsseldateien:

Zertifikats/Schlüsseldatei name	Verzeichnis	Beschreibung
CAELMCert	/opt/CA/SharedComponents/iTechnology (Sie können sich auf mit dem kürzeren, variablen Namen, "$IGW_LOC" auf dieses Verzeichnis beziehen.)	Dieses Zertifikat wird von allen CA Enterprise Log Manager-Diensten für die Kommunikation zwischen CA Enterprise Log Manager-Servern sowie zwischen CA Enterprise Log Manager-Servern und dem CA EEM-Server verwendet. In der Hauptkonfigurationsdatei "CALM.cnf" befindet sich ein Eintrag für dieses Zertifikat und die dazugehörige Schlüsseldatei. Die Tag-Paare beginnen jeweils mit < anCertificate> und <KeyFile>.
CAELM_AgentCert	$IGW_LOC auf dem Server des Agentenhosts	Agenten verwenden dieses Zertifikat, um mit einem beliebigen CA Enterprise Log Manager-Server zu kommunizieren. Der CA Enterprise Log Manager-Verwaltungsserver gibt dieses Zertifikat an den Agenten weiter. Das Zertifikat gilt für sämtliche CA Enterprise Log Manager-Server innerhalb einer bestimmten Instanz der Anwendung.

Zertifikats/Schlüsseldatei name	Verzeichnis	Beschreibung
itpamcert	IT PAM-Server	Dieses Zertifikat wird für die Kommunikation mit IT PAM verwendet. Weitere Informationen finden Sie in der Dokumentation zu CA IT PAM.
rootcert	$IGW_LOC	Dieses Zertifikat ist ein selbstsigniertes Stammzertifikat, das während der Installation durch iGateway signiert wird.
iPozDsa	$IGW_LOC	Der CA EEM-Server verwendet dieses Zertifikat sowohl als lokaler als auch als Remote-Server. Hinweis: Weitere Informationen finden Sie in der CA EEM-Dokumentation.
iPozRouterDsa	$IGW_LOC	Der CA EEM-Server verwendet dieses Zertifikat sowohl als lokaler als auch als Remote-Server. Hinweis: Weitere Informationen finden Sie in der CA EEM-Dokumentation.
iTechPoz-trusted	/opt/CA/Directory/dxserver/config/ssld	CA Directory verwendet dieses Zertifikat.
iTechPoz-<hostname>-Router	/opt/CA/Directory/dxserver/config/ssld	CA Directory verwendet dieses Zertifikat.

Beschränkungen in der Unterstützung von FIPS

Die folgenden CA Enterprise Log Manager-Funktionen und -Produktinteraktionen unterstützen keine Vorgänge im FIPS-Modus:

ODBC- und JDBC-Zugriff auf den Ereignisprotokollspeicher.

ODBC und JDBC hängen in CA Enterprise Log Manager von einen zu Grunde liegenden SDK ab, der der Vorgänge im FIPS-Modus nicht unterstützt. Administratoren von föderierten Netzwerken, die FIPS-Vorgänge benötigen, müssen den ODBC-Dienst manuell auf allen CA Enterprise Log Manager-Servern deaktivieren. Im *Implementierungshandbuch* finden Sie einen Abschnitt zum Deaktivieren des ODBC- und JDBC-Zugriffs auf den Ereignisprotokollspeicher.

Einen CA EEM-Server gemeinsam benutzen

CA Enterprise Log Manager r12.1 SP1 verwendet den FIPS-kompatiblen CA EEM r8.4 SP3. Das Aktivieren des FIPS-Modus auf dem CA Enterprise Log Manager-Server deaktiviert die Kommunikation zwischen dem gemeinsam benutzen CA EEM und sämtlichen Produkten, die CA EEM r8.4 SP3 nicht unterstützen.

PAM CA IT ist z. B. nicht FIPS-kompatibel. Wenn Sie für Ihren CA Enterprise Log Manager-Server den FIPS-Modus festlegen, schlägt die Integration mit CA IT PAM fehl.

Sie können einen CA EEM-Server für CA Enterprise Log Manager r12.1 SP1 und PAM CA IT r2.1 SP2 und r2.1 SP3 nur in Nicht-FIPS-Modus verwenden.

Wenn Ihre CA IT PAM -Installation den CA EEM-Server nicht freigibt, kann CA Enterprise Log Manager r12.1 SP1 in FIPS-Modus ausgeführt werden und mit CA IT PAM kommunizieren. Diese Kommunikationswege sind jedoch nicht FIPS-kompatibel.

LDAP Bind erfordert übereinstimmende Betriebsmodi

Der Erfolg der Kommunikation mit einem externen Benutzerspeicher hängt von folgenden Faktoren ab:

- Die CA Enterprise Log Manager-Server und ihr CA EEM-Verwaltungsserver müssen sich im selben FIPS-Modus befinden, und
- Der CA EEM-Server muss sich im selben FIPS-Modus wie ein FIPS-aktivierter externer Benutzerspeicher befinden, wenn für die Verbindung TLS v1.0 verwendet wird.

  Hinweis: Es ist keine FIPS-Kompatibilität verfügbar, wenn zwischen dem CA EEM-Server und dem externen Benutzerspeicher eine unverschlüsselte Kommunikation stattfindet, oder wenn sich der CA EEM-Server und der Benutzerspeicher in unterschiedlichen FIPS-Modi befinden.

SNMP-Traps

Sie können SNMP-Ereignisse mithilfe von SNMP V2 oder SNMP V3 senden. Beide werden im Nicht-FIPS-Modus unterstützt.

Wenn der SNMP-Trap-Zielserver FIPS-aktiviert ist, müssen Sie V3-Sicherheit wählen. Wählen Sie dann SHA als Authentifizierungsprotokoll und AES als Verschlüsselungsprotokoll. Diese Optionen werden auf der auf der Seite "Ziel" des Assistenten zum Planen von Aktionsalarmen ausgewählt.

Konfigurieren von Microsoft Internet Explorer, um in FIPS-Modus auf CA Enterprise Log Manager zuzugreifen

Möglicherweise sind zusätzliche Browserkonfigurationseinstellungen erforderlich, damit die Benutzeroberfläche des CA Enterprise Log Manager-Servers im FIPS-Modus angezeigt werden kann. Durch den folgenden Vorgang können Sie die erforderlichen Optionen einstellen, um mit Microsoft Internet Explorer 7 oder 8 auf CA Enterprise Log Manager zuzugreifen.

Hinweis: Mit Microsoft Internet Explorer 6 können Sie nicht im FIPS-Modus auf CA Enterprise Log Manager-Server zugreifen.

Konfigurieren von Microsoft Internet Explorer 7 oder 8

1. Öffnen Sie den Browser auf, und gehen Sie zu "Extras", "Internetoptionen".
2. Wählen Sie die Registerkarte "Erweitert", und führen Sie einen Bildlauf zum Bereich "Sicherheit" durch.
3. Wählen alle folgenden Optionen aus:
   - SSL 2.0 verwenden
   - SSL 3.0 verwenden
   - TLS 1.0 verwenden
4. Klicken Sie auf OK.

Konfigurieren von Mozilla Firefox, um in FIPS-Modus auf CA Enterprise Log Manager zuzugreifen

Möglicherweise sind zusätzliche Browserkonfigurationseinstellungen erforderlich, damit die Benutzeroberfläche des CA Enterprise Log Manager-Servers im FIPS-Modus angezeigt werden kann. Durch den folgenden Vorgang können Sie die erforderlichen Optionen einstellen, um mit Mozilla Firefox 3.5.8 oder später auf CA Enterprise Log Manager zuzugreifen.

Hinweis: Um auf CA Enterprise Log Manager zuzugreifen, das Mozilla Firefox-Plug-In für Adobe Flash 9 oder 10 installiert sein.

Konfigurieren von Mozilla Firefox

1. Öffnen Sie den Browser auf, und gehen Sie zu "Extras", "Einstellungen".
2. Klicken Sie auf die Registerkarte "Erweitert" und dann auf die Unterregisterkarte "Verschlüsselung".
3. Wählen die beiden folgenden Optionen aus:
   - SSL 3.0 verwenden
   - TLS 1.0 verwenden
4. Wählen Sie die Unterregisterkarte "Sicherheit" aus, und wählen Sie die Option zum Verwenden eines Master-Kennworts.
5. Klicken Sie auf "Master-Passwort ändern...", geben Sie im angezeigten Fenster ein geeignetes Kennwort ein, und klicken Sie auf "OK".
6. Wählen Sie die Registerkarte "Erweitert" aus.
7. Klicken Sie auf "Sicherheitsgeräte".

   Das Fenster "Gerätemanager" wird angezeigt.
8. Wählen Sie das NSS Internal PKCS #11-Modul im linken Bereich aus.

   Durch diese Aktion wird der rechte Bereich aufgefüllt.
9. Wählen Sie die Zeile "Module NSS Internal FIPS PKCS #11 Module" aus, und klicken Sie auf "FIPS aktivieren".
10. Wenn Sie dazu aufgefordert werden, geben Sie das Master-Kennwort ein, das Sie in einem früheren Schritt erstellt haben, und klicken Sie auf "OK".
11. Klicken Sie im Fenster "Gerätemanager" auf "OK".
12. Klicken Sie im Fenster "Optionen" auf "OK".
13. Starten Sie den Browser neu.

Weitere Informationen:

Aktualisieren mit automatischen Software-Updates (siehe Seite 11)

ISO-Image für Neuinstallationen

Um Ihnen zu helfen, CA Enterprise Log Manager schnellstmöglich bereitzustellen oder zu einer vorhandenen Bereitstellung einen neuen CA Enterprise Log Manager Server hinzuzufügen, stellen wir für das Service Pack ein ISO-Image zur Verfügung. Das ISO-Image kann vom Download-Bereich von Support Connect heruntergeladen werden.

Es wird empfohlen, in den folgenden Fällen jeweils das neueste ISO-Image zu verwenden:

- Bereitstellung von CA Enterprise Log Manager. Bei einer Installation vom neuesten ISO-Image bleibt die Anzahl der erforderlichen automatischen Software-Updates, die Sie anwenden müssen, relativ gering, und Ihre Bereitstellung wird beschleunigt.
- Beim Hinzufügen eines neuen CA Enterprise Log Manager-Servers nach einem Upgrade der Server in Ihrer bestehenden Bereitstellung. Stellen Sie zuerst sicher, dass das Upgrade der Server und Agents in Ihrer aktuellen Bereitstellung erfolgreich abgeschlossen wurde, und dass Server und Agents Ereignisse empfangen. Installieren Sie dann die neuen Server mithilfe des ISO-Images, um die Kapazität zu erhöhen und die Anzahl der anzuwendenden automatischen Software-Updates so gering wie möglich zu halten.

Hinweis: Das Installationsverfahren hat sich geändert. Eine neue Eingabeaufforderung fragt, ob die Installation mit aktiviertem FIPS-Modus erfolgen soll. Beim Hinzufügen eines neuen CA Enterprise Log Manager-Servers zu einer vorhandenen FIPS-Bereitstellung (d. h. der CA Enterprise Log Manager-Verwaltungsserver oder der Remote-CA EEM-Server befinden sich im FIPS-Modus) aktivieren Sie den FIPS-Modus während der Installation. Anderenfalls wird der neue Server nicht registriert und muss neu installiert werden. Weitere Informationen über den FIPS-Modus finden Sie im *Implementierungshandbuch* .

Kapitel 6: Bekannte Probleme

Dieses Kapitel enthält folgende Themen:

Agenten und CA-Adapter

Im Folgenden werden die bekannten Probleme in Verbindung mit Agenten und CA-Adaptern aufgeführt.

Abhängigkeiten bei der Agenteninstallation auf Red Hat Linux 4

Symptom:

Wenn Sie den CA Enterprise Log Manager-Agenten auf Red Hat Enterprise Linux 4-Systemen installieren, tritt bei der Installation ein Fehler auf, und es wird eine Fehlermeldung über erforderliche Abhängigkeiten angezeigt.

Lösung:

Unter Red Hat Enterprise Linux 4 benötigt der CA Enterprise Log Manager-Agent das Legacy Software Development-Paket. Installieren Sie das Legacy Software Development-Paket, bevor Sie den Agenten installieren.

Die Genauigkeit der Statuszeit des Agenten ist von der NTP-Server-Konfiguration abhängig

Symptom:

Wenn auf verschiedenen CA Enterprise Log Manager-Servern, die Erfassungen ausführen, manuell eine andere Uhrzeit eingestellt ist, können Diskrepanzen in der Berichtszeit für Agentenaktivitäten auftreten.

Lösung:

Wenn Sie die einzelnen CA Enterprise Log Manager in Ihrem Netzwerk installieren, geben Sie einen NTP-Server an. Durch die Konfiguration eines NTP-Servers für jeden Server wird die Berichtszeit für Agenten, die von unterschiedlichen Servern verwaltet werden, synchronisiert.

Einräumen von Zeit für die Aktualisierung nach der Massenbereitstellung von Connectors

Symptom:

Neue Connectors werden nach einer Massenbereitstellung von Connectors nicht sofort im Agenten-Explorer angezeigt.

Lösung:

Je nach Anzahl der Connectors und der Agenten, auf denen Sie diese bereitstellen, müssen Sie einige Minuten warten, bis alle Connectors im Agenten-Explorer aktualisiert wurden.

Massenbereitstellung von Connectors mit IPv6-Adresse funktioniert nicht richtig

Symptom:

Die Bereitstellung von Connectors mit Hilfe des Assistenten zur Massenbereitstellung von Connectors unter Angabe der Server-Adresse im IPV6-Format funktioniert nicht wie erwartet. Nach einiger Zeit wird der Connector-Status "Wird ausgeführt" angezeigt. Wenn Sie den Connector bearbeiten, sehen Sie, dass nur die ersten vier Ziffern des Servernamens in der IPV6-Adresse angezeigt werden. Die Felder für den Benutzernamen, das Kennwort und die Domäne sind leer.

Lösung:

In der CA Enterprise Log Manager-Benutzeroberfläche wird der Inhalt der Quelldatei derzeit mit zwei Doppelpunkten (::) als Trennzeichen zur Trennung der einzelnen Quellen gesendet. Da die IPv6-Adresse den zweifachen Doppelpunkt enthält, wird dieser als Trennzeichen verarbeitet. Der Connector-Datensatz wird daher nicht richtig gespeichert.

Verwenden Sie die IPv6-Adresse nicht für die Massenbereitstellung von Connectors. Sie *können* Connectors mit Hilfe von Hostnamen für die Massenbereitstellung konfigurieren. Darüber hinaus können Sie einen IPv6-Connector anhand der normalen Anweisungen im Assistenten "Erstellung eines neuen Connectors" konfigurieren.

Keine Leerzeichen bei Name für DVD-Einbindung zulässig

Symptom:

Beim manuellen Installieren eines Agenten von dem DVD-ROM-Medium des Produkts auf einem Computer mit dem Linux-Betriebssystem wird eine Fehlermeldung zur Verweigerung des Zugriffs angezeigt und die Installation wird abgebrochen.

Lösung:

Zum Installieren eines Agenten von DVD-Medien müssen Sie zuerst das DVD-Laufwerk mit einem Befehl einbinden, der etwa folgenden Wortlaut hat:

```
$ mount /dev/cdrom <local path>
```

Die DVD-ROM kann nicht in einen lokalen Pfadnamen (Verzeichnis) eingebunden werden, der Leerzeichen enthält. Binden Sie die DVD-ROM in einen Verzeichnisnamen ein, der keine Leerzeichen enthält, und installieren Sie dann den Agenten.

Ereignisquellenkonfiguration auf Domänenebene schlägt fehl

Symptom:

Wenn Sie einen Connector für den Zugriff auf eine Windows-Ereignisquelle und das Lesen der zugehörigen Protokolle konfigurieren, erstellen Sie im Rahmen dieses Vorgangs auch ein Benutzerkonto mit eingeschränkten Berechtigungen und weisen diesem die erforderlichen Berechtigungen zu. Handelt es sich bei einer der Ereignisquellen um einen Windows Server 2003-Host (SP1), legen Sie in einem der Schritte eine lokale Sicherheitsrichtlinie *Wechseln der Identität eines Clients nach der Authentifizierung* fest. Wenn diese Benutzerberechtigung lokal eingestellt wird, treten keine Probleme auf. Wird diese Einstellung jedoch als Domänenrichtlinie auf alle Server angewendet, bewirkt diese globale Anwendung, dass die bestehenden lokalen Zuweisungen für andere Benutzer entfernt werden, und zwar für "Administratoren" und "SERVICE".

In einem Support-Artikel von Microsoft ist angegeben, dass Probleme auftreten, wenn eine Gruppenrichtlinien-Einstellung, die ein Benutzerrecht "Annehmen der Clientidentität nach Authentifizierung" definiert, mit der Domäne verknüpft ist. Dieses Benutzerrecht sollte nur mit einem Standort oder einer Organisationseinheit verknüpft werden.

Lösung:

Der Microsoft Knowledge Base-Artikel mit der ID 930220 enthält die Empfehlung, die vollständige ungesicherte TPC/IP-Konnektivität wiederherzustellen und dazu die IPSec-Services zu deaktivieren und den Computer neu zu starten. Ferner sind in diesem Artikel die Schritte angegeben, anhand derer sich die Gruppen "Administratoren" und "SERVICE" wieder als Gruppenrichtlinien-Einstellung hinzufügen lassen. Rufen Sie folgenden Link auf:

http://support.microsoft.com/kb/930220

Darüber hinaus empfiehlt Microsoft die folgenden Methoden zum Beheben von Problemen, die durch die Anwendung der Einstellung "Annehmen der Clientidentität nach Authentifizierung" als Gruppenrichtlinie hervorgerufen werden:

- Methode 1: Ändern von Gruppenrichtlinien-Einstellungen
- Methode 2: Ändern der Registrierung

Die Schritte zur Implementierung beider empfohlener Lösungen finden Sie im Microsoft Knowledge Base-Artikel mit der ID 911801. Rufen Sie folgenden Link auf:

http://support.microsoft.com/kb/911801

Das Aktivieren von SSL-Kommunikation verursacht ODBC-/JDBC-Verzögerungen

Symptom:

Wenn die Kommunikation von CA Enterprise Log Manager-Agentenservern im Nicht-FIPS-Modus stattfindet, kommt es zu einer kurzen Unterbrechung in der ODBC-/JDBC-Kommunikation, wenn die SSL-Kommunikation aktiviert wird.

Lösung:

Wenn Sie ODBC oder JDBC verwenden, kann die CA Enterprise Log Manager-Serverkommunikation unmittelbar nach der Aktivierung von SSL fehlschlagen. Warten Sie etwa fünf Minuten, damit die Kommunikation wiederhergestellt wird.

Integrationen mit Dateiprotokollsensoren 4.0.0.0 unterstützen SUSE Linux nicht

Symptom:

Nach einem direkten Upgrade von CA Enterprise Log Manager 12.1 auf 12.1 SP1 Upgrade wird im Integrationsassistenten eine unrichtige Meldung zum Plattformstatus angezeigt. Wenn Sie im ersten Schritt des Assistenten die Version 4.0.0.0 des Dateiprotokollsensors auswählen, wird in der Liste der vefügbaren Plattformen "Linux_X86_32 SLES11" angezeigt.

Lösung:

Diese Information ist falsch. SUSE Linux wird für die Version 4.0.0.0 des Dateiprotokollsensors nicht unterstützt Ignorieren Sie diese Meldung. Sie können keine benutzerdefinierte Integration mit diesem Protokollsensor erstelln.

Einschränkung bei der Konfiguration von Ports

Symptom:

Wenn der Syslog-Listener mit dem Standard-UDP-Port auf einem Agenten, der als Nicht-Root-Benutzer auf einem Linux-Host ausgeführt wird, konfiguriert ist, wird der UDP-Port 514 (Standard für Syslog) nicht geöffnet, und an diesem Port werden keine Syslog-Ereignisse erfasst.

Lösung:

Wenn der Agent als Nicht-Root-Benutzer auf einem UNIX-System ausgeführt wird, müssen Sie entweder die Ports des Syslog-Listeners zu Portnummern über 1024 ändern oder diesen Service so ändern, dass er als Root ausgeführt wird.

Mögliche Leistungsbeeinträchtigungen, wenn zu viele Integrationen ausgewählt sind

Symptom:

Die Leistung des Standardagenten sinkt, wenn Sie zu viele Syslog-Standardintegrationen für einen Connector angeben. In diesem Fall bezieht sich der Begriff "Leistung" auf die Anzahl der pro Sekunde verarbeiteten Ereignisse (EPS).

Lösung:

CA Enterprise Log Manager lädt für jede Integration Nachrichtenanalysedateien (XMP-Dateien) und Datenzuordnungsdateien (DM-Dateien). Während einzelner Vorgänge überprüft CA Enterprise Log Manager eingehende Ereignisse anhand der Listen mit regulären Ausdrücken. Bei einer größeren Anzahl von Dateien verlängert sich die Verarbeitungszeit.

Sie können ein Absinken der Leistung vermeiden, indem Sie nicht benötigte Integrationen beim Erstellen eines Syslog-Connectors entfernen. Überprüfen Sie nach der Installation die für den Standard-Syslog-Connector konfigurierten Integrationen, und entfernen Sie alle, die Sie nicht benötigen.

Kein Löschen des Standardagenten bei Entfernen des Servers aus einem Verbund

Symptom:

Beim Entfernen eines CA Enterprise Log Manager-Servers aus einer Gruppe von Verbundservern wird der Standardagent des gelöschten Servers nicht aus der entsprechenden Agentengruppe gelöscht.

Lösung:

Löschen Sie den Agenten in der Unterregisterkarte "Agenten-Explorer" manuell aus seiner Gruppe.

Berichte mit Daten, die vom CA SAPI Collector erfasst wurden, zeigen Ereignisse nicht ordnungsgemäß an

Symptom:

Bei Ereignissen, die mit dem CA Audit SAPI Collector erfasst werden, sind nicht alle Felder ordnungsgemäß ausgefüllt. Dies führt dazu, dass die Daten in den meisten Berichte nicht wie erwartet angezeigt werden.

Lösung:

Verwenden Sie den CA Audit SAPI Router, um Ereignisse von Ihrer bestehenden CA Audit-Infrastruktur zu erfassen.

Weitere Informationen zum Konfigurieren des SAPI-Routers finden Sie im *Implementierungshandbuch* im Abschnitt "Überlegungen für CA Audit-Benutzer".

Keine Garantie für Syslog-Übermittlung über UDP

Symptom:

Die garantierte Übermittlung kann bei der direkten Erfassung von Syslogs über das UDP-Protokoll des Syslog-Listeners ein Problem darstellen.

Lösung:

Ziehen Sie als Lösung für die möglichen Probleme bezüglich einer garantierten Übermittlung einen Mechanismus zur lokalen Syslog-Erfassung in Betracht. Dabei konfigurieren Sie einen Syslog-Listener auf einem Agenten, der mit der Syslog-Ereignisquelle installiert ist.

Hinweis: Wählen Sie den bekannten Port für Syslog, Port 514, nur dann, wenn der Agent als Root ausgeführt wird. Weisen Sie einen privaten Port zu, wenn der Agent wie empfohlen als Benutzer mit geringeren Berechtigungen ausgeführt wird. Zu den privaten Ports zählen Ports von 49152 bis 65535.

Syslog-Services bei UNIX-Konflikt

Symptom:

Bei folgendem Szenario empfängt CA Enterprise Log Manager keine Syslog-Ereignisse:

Computer 1

Ein CA Enterprise Log Manager-Server wartet auf Syslog-Ereignisse von Computer 2.

Computer 2

Ein RHEL 4.0-Computer mit einem lokalen Agenten, der einen Syslog-Connector enthält, sendet seine Ereignisse mit dem Syslog-Listener zu Computer 1.

Computer 3

Ein UNIX-Computer sendet Ereignisse zu Computer 2 mit dem dort installierten Connector.

In diesem Fall kann der Agentencomputer die Ereignisse von Computer 3 nicht erfassen, da der Syslog-Service und der Syslog-Connector des Betriebssystems auf dem gleichen System ausgeführt werden.

Lösung:

Beenden Sie den Syslog-Service auf Computer 2, damit Sie Ereignisse von Computer 3 (dem UNIX-Computer) empfangen können. Sie können auch die Umgebung neu konfigurieren, so dass Syslog-Services auf dem gleichen Computer nicht miteinander in Konflikt geraten.

WMI-Protokollsensor generiert mehrere Benutzerberechtigungsereignisse

Symptom:

Wenn Sie einen Connector mit dem WMI-Protokollsensor zum Erfassen von Ereignissen verwenden, stoßen Sie möglicherweise auf mehrere Ereignisse im Zusammenhang mit Berechtigungen.

Lösung:

Diese Ereignisse werden angezeigt, wenn die Windows-Überwachungsrichtlinie, durch die erfolgreiche Aktionen zur Verwendung von Berechtigungen erfasst werden, auf dem Zielsystem aktiviert ist. Sie sind ein Nebenprodukt der Ereigniserfassung und deuten auf kein Problem hin. Wenn diese Ereignisse nicht mehr angezeigt werden sollen, können Sie eine Unterdrückungsregel erstellen, damit CA Enterprise Log Manager sie nicht mehr erhält.

Der auf einem Solaris-Agentensystem ausgeführte Textdatei-Protokollsensor beendet den Empfang von Ereignissen

Symptom:

Der auf einem Solaris-Agentensystem ausgeführte Textdatei-Protokollsensor beendet den Empfang von Ereignissen.

Die Protokolldatei für den Connector enthält eine Fehlermeldung, die anzeigt, dass die Bibliotheksdatei "libssl.so.0.9.7" nicht geöffnet werden konnte:

```
[4] 07/20/10 18:55:50 ERROR :: [ProcessingThread::DllLoad] :Error is: ld.so.1:
caelmconnector: fatal: libssl.so.0.9.7: open failed: No such file or directory
[4] 07/20/10 18:55:50 ERROR :: [ProcessingThread::run] Dll Load and Initialize
failed, stopping the connector ...
[3] 07/20/10 18:55:50 NOTIFY :: [CommandThread::run] Cmd_Buff received is START
```

Lösung:

Identifizieren Sie den Speicherort der Bibliothek, um den Agenten für den Empfang von Ereignissen zu aktivieren.

So beheben Sie den Fehler auf dem Solaris-Agentensystem:

1. Navigieren Sie zum Ordner "/etc". Beispiel:

   ```
   cd /etc.
   ```

2. Öffnen Sie im Ordner "etc" die Datei "profile". Beispiel:

   ```
   vi /etc/profile
   ```

3. Fügen Sie am Ende der Datei die zwei folgenden Zeilen ein:

   ```
   LD_LIBRARY_PATH=/usr/sfw/lib:$LD_LIBRARY_PATH
   ```

   ```
   export LD_LIBRARY_PATH
   ```

4. Schließen Sie die aktuelle Sitzung des Solaris-Agentensystems.
5. Öffnen Sie eine neue Sitzung des Solaris-Agentensystems.
6. Beenden Sie den CA Enterprise Log Manager-Agenten auf dem Solaris-System. Beispiel:

   ```
   /opt/CA/ELMAgent/bin/S99elmagent stop
   ```

7. Starten Sie den CA Enterprise Log Manager-Agenten auf dem Solaris-System. Beispiel:

   ```
   /opt/CA/ELMAgent/bin/S99elmagent start
   ```

   Der Textdatei-Protokollsensor beginnt, Ereignisse zu empfangen, und der Fehler wird nicht mehr in der Protokolldatei angezeigt.

Sehr hoher Ereignisstrom führt dazu, dass der Agent nicht reagiert

Symptom:

Ein CA Enterprise Log Manager-Agent hört auf, zu reagieren und Ereignisse zu akzeptieren. Die folgende Fehlermeldung wird in der Datei "caelmdispatcher.log" angezeigt:

```
[275] 07/12/10 14:32:05 ERROR :: FileQueue::PutEvents Unable to write to new event file
[275] 07/12/10 14:32:05 ERROR :: WriterThread::run Unable to push events to FileQueue, Retrying
[275] 07/12/10 14:32:10 NOTIFY :: FileQueue::UpdateCurrentWriterFile Reached Max files configured limit=10, Not creating any new files for now
```

Lösung:

Dadurch wir angezeigt, dass für die Hardware in der Umgebung eine sehr hohe Anzahl an Ereignissen eingeht. Sie können diesem Problem entgegenwirken, indem Sie den Agenten durch die folgende Vorgehensweise neu konfigurieren:

1. Klicken Sie in "Verwaltung" auf die Unterregisterkarte "Protokollerfassung", und erweitern Sie den Ordner "Agenten-Explorer".
2. Wählen Sie den Agenten aus, den Sie neu konfigurieren möchten, klicken Sie auf "Bearbeiten", und passen Sie folgenden Parameter an:

   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. Die Standardeinstellung ist 10.

   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. Die Standardeinstellung ist 100 MB.

   Sie können diese Parameter nach oben hin erweitern, um den Erfordernissen Ihrer Umgebung und der Rate der pro Sekunde empfangenen Ereignisse zu entsprechen.

Anwendung (nicht Benutzeroberfläche)

Im Folgenden werden die bekannten Probleme in Verbindung mit der Softwareanwendung (nicht mit der CA Enterprise Log Manager-Benutzeroberfläche) aufgeführt.

Anmeldung beim CA Enterprise Log Manager Server mit EiamAdmin-Benutzernamen nicht möglich

Symptom:

Der EiamAdmin-Benutzername und das Kennwort werden bei Ihrem Versuch, sich beim CA Enterprise Log Manager-Server anzumelden (nicht über die Benutzeroberfläche), nicht erkannt.

Lösung:

Um wartungsbezogene Aufgaben, wie die Konfigurierung der Archivierung durchzuführen, erstellt die Installation einen anderen Benutzernamen (caelmadmin) und weist diesem das gleiche Kennwort zu, das der Installer für EiamAdmin bereitgestellt hat. Verwenden Sie den "caelmadmin"-Benutzernamen und das entsprechende Kennwort, um sich beim CA Enterprise Log Manager-Server anzumelden.

Weiter Informationen finden Sie unter den Standardbenutzerkonten im *Implementierungshandbuch*.

Übermäßige Anzahl von ELMAdapter-Protokolldateien

Symptom:

Auf dem CA Enterprise Log Manager-Server kann sich eine große Anzahl von Adapter-Protokolldateien ansammeln. Dies ist insofern atypisch, als dass Protokollmeldungen normalerweise am Ende einer einzigen Protokolldatei angehängt werden. Das Problem kann durch die Aktivierung der Ablaufverfolgung verursacht werden.

So ermitteln Sie, ob dieses Problem besteht:

1. Planen Sie Berichte und Alarme, und führen Sie ODBC-Abfragen wie die folgende aus:

   ```
   select event_logname,count(*) from view_event where event_time_gmt >=
   timestampadd(hh,-1,now()) AND event_time_gmt <= now() group by event_logname;
   ```

2. Melden Sie sich unter Verwendung von SSH beim CA Enterprise Log Manager-Server an, und geben Sie den Caelmadmin-Benutzernamen und das Kennwort an.
3. su zu root, und geben Sie das Root-Kennwort an.
4. Navigieren Sie zum Ordner "iTechnology":

   ```
   cd /opt/CA/SharedComponents/iTechnology
   ```

5. Stellen Sie fest, ob aufgrund von Abfragen durch ODBC-Treiber eine übermäßige Anzahl von Protokolldateien erstellt wurde. Diese Dateien sind wie folgt benannt: "ELMAdapter_<oaserverpid>_-IP.log".

Lösung:

Falls dieses Problem besteht, stellen Sie folgendermaßen sicher, dass die Fehlerverfolgung deaktiviert ist:

1. Melden Sie sich unter Verwendung von SSH beim CA Enterprise Log Manager-Verwaltungsserver an, und geben Sie den "caelmadmin"-Benutzernamen und das Kennwort an.
2. su zu root, und geben Sie das Root-Kennwort an.
3. Navigieren Sie zum Ordner "iTechnology":

   ```
   cd /opt/CA/SharedComponents/iTechnology
   ```

4. Öffnen Sie die Datei "oaserver-dm.ini" zum Bearbeiten.
5. Blättern Sie zu "[Service_0]", und stellen Sie sicher, dass die Ablaufverfolgung deaktiviert ist. Andernfalls ändern Sie sie so, dass sie mit folgendem Beispiel übereinstimmt:

   ```
   ServiceDebugLogLevel=0
   ServiceIPLogOption=Disable All Tracing
   ```

6. Starten Sie den ODBC-Service wie folgt neu:

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

b. Klicken Sie auf "ODBC-Server".

c. Führen Sie einen der folgenden Schritte aus:

   - Falls das Kontrollkästchen "Dienste aktivieren" nicht aktiviert ist, aktivieren Sie es, und klicken Sie dann auf "Speichern".
   - Falls das Kontrollkästchen "Dienste aktivieren" aktiviert ist, deaktivieren Sie es, klicken Sie auf "Speichern", aktivieren Sie das Kontrollkästchen "Dienste aktivieren" wieder, und klicken Sie erneut auf "Speichern".

Manueller Import von Analysedateien macht eventuell eine Änderung des Zeitlimitwertes erforderlich

Wenn während der CA Enterprise Log Manager-Installation Analysedateien (XMP-Dateien) importiert werden, kommt es gelegentlich zu einem Problem. Dieses Problem tritt am häufigsten bei der Installation von CA Enterprise Log Manager auf Servern, die die Mindestanforderungen an die Hardware nicht erfüllen, oder in langsamen Netzwerken auf.

Symptom:

Während der Installation tritt beim Import von Analysedateien ein Fehler auf. Sie können dieses Problem nach Abschluss der Installation beheben. Führen Sie das mitgelieferte Skript *EEM/content/ImportCALMXMP.sh* aus, um die Dateien manuell zu importieren. (Weitere Informationen zu diesem Skript finden Sie im *Implementierungshandbuch*.) Durch diese Aktion wird der Fehler in der Regel behoben.

In manchen Fällen kann die XMP-Datei des Cisco-Routers jedoch nicht erfolgreich importiert werden, während das Skript für den manuellen Import ausgeführt wird. Die Installation des CA Enterprise Log Manager-Servers ist erfolgreich verlaufen. Der Fehler beim Import der XMP-Dateien führt jedoch dazu, dass die Standard-Connectors nicht ordnungsgemäß auf dem lokalen Agenten installiert werden. Sie können die Connectors erst bereitstellen, nachdem Sie die XMP-Dateien erfolgreich manuell importiert haben.

Lösung:

Ein überschrittener Standardzeitlimitwert im Skript *EEMImportUtility.sh* verursacht das Problem beim Import der Cisco-XMP-Datei. Das Skript *ImportCALMXMP.sh* ruft das Skript *EEMImportUtility.sh* auf. Der Standardwert für das Zeitlimit beträgt 4 Minuten. Stellen Sie das Standardzeitlimit auf 6 Minuten ein, um genügend Zeit für einen manuellen Import auf langsameren Servern einzuräumen.

So ändern Sie den Standardwert für das Zeitlimit:

1. Navigieren Sie zu dem Verzeichnis "EEM/content".
2. Bearbeiten Sie die Datei "ImportCALMXMP.sh".
3. Suchen Sie die folgende Zeile, und ändern Sie den Zeitlimitwert wie dargestellt:

   ```
   ./EEMImportUtility.sh -h simdemo01 -u EiamAdmin -m FgAMCQQJAllf -a CAELM -type xmp -l XMP" to "./EEMImportUtility.sh -timeout 360000 -h simdemo01 -u EiamAdmin -m FgAMCQQJAllf -a CAELM -type xmp -l XMP
   ```

   Hinweis: Der Wert für das Zeitlimit wird in Millisekunden ausgedrückt.
4. Speichern und schließen Sie die Datei.
5. Führen Sie das Skript erneut aus.
6. Stellen Sie manuell Connectors für "syslog" und "Linux_LocalSyslog" auf dem Standardagenten bereit.

Ereignisverfeinerung

Im Folgenden werden die bekannten Probleme in Verbindung mit der Ereignisverfeinerung aufgeführt.

Verschiedene Operatoren für Blockzuordnungen für Zeichenfolgenwerte und numerische Werte erforderlich

Symptom:

Beim Verwenden des Zuordnungsassistenten reagieren Blockzuordnungswerte für numerische oder Zeichenfolgenspalten nicht wie erwartet.

Lösung:

Beim Erstellen von Blockzuordnungen kann der Operator "Equal" (Gleich) nur mit numerischen Spalten verwendet werden. Verwenden Sie den "Übereinstimmungs-Operator" für alle Zeichenfolgenspalten.

Die benutzerdefinierte Datenzuordnung kann keine epSIM-Ereignisse (iTech) zuordnen

Symptom:

Eine benutzerdefinierte Datenzuordnung, die für epSIM-Ereignisse (iTechnology) erstellt wurde, kann die Ereignisse nicht zuordnen, nachdem Sie im Protokollerfassungs-Explorer unter CA Adapter auf das iTechnology Event-Plugin angewendet wurde.

Wenn Sie die Abfrage "Alle Ereignisse des Systems" überprüfen, um festzustellen, ob iTech-Ereignisse entsprechend der benutzerdefinierten Datenzuordnung zugeordnet werden, stellen Sie fest, dass iTech-Ereignisse nicht zugeordnet werden. Infolgedessen werden keine Abfrageergebnisse zurückgegeben. Die Meldung "Es wurden keine Ereignisse zugeordnet. Ereignisse können nicht zugeordnet werden." wird angezeigt.

Lösung:

Öffnen Sie die benutzerdefinierte Datenzuordnungsdatei, und ersetzen Sie "$EventLog" durch "$Log". Dies bedeutet:

Ändern Sie dien Ziele: <DM_Field name="event_logname" type="string" value="$EventLog" mapping="direct"/>

In: <DM_Field name="event_logname" type="string" value="$Log" mapping="direct"/>

Diese Änderung stellt sicher, dass Ereignisse zugeordnet werden. Ignorieren während Zuordnungsanalyse die Nachricht , die aussagt: "Es wurden keine Ereignisse zugeordnet.".

Abfragen und Berichte

Im Folgenden werden die bekannten Probleme in Verbindung mit Abfragen und Berichten aufgeführt.

Abfrageergebnisse von Aktionsalarmen können unvollständig sein

Symptom:

Wenn ein Aktionsalarm generiert wird, können Sie in CA Enterprise Log Manager sofort das Abfrageergebnis anzeigen. Um die Ergebnisse in CA Enterprise Log Manager anzuzeigen, klicken Sie auf die Registerkarte "Alarmverwaltung", dann auf die Unterregisterkarte "Aktionsalarme", und wählen Sie den Namen des Alarms aus. Die Ergebnisse werden in einer Diagrammansicht angezeigt. Wenn durch den Aktionsalarm ein CA IT PAM-Ereignis-/Alarmausgabeprozess aufgerufen wird, durch den in CA Service Desk ein Help Desk-Ticket geöffnet wird, enthält die Help Desk-Ausgabe eine URL. Wenn Sie zu dieser URL navigieren und sich anmelden, werden die Abfrageergebnisse für den Alarm auf einer einzelnen Seite angezeigt. Bei einem Vergleich dieser Ergebnisse mit den auf der Unterregisterkarte "Aktionsalarme" angezeigten Ergebnissen werden Sie eventuell Unterschiede in den Abfrageergebnissen feststellen. Wenn beispielsweise Ergebnisse für "Anzahl" angezeigt werden, sind die Zahlen in der URL-Ansicht möglicherweise größer als die Zahlen, die in CA Enterprise Log Manager angezeigt werden. Dieses Problem kann auf stark ausgelasteten Systemen auftreten, wenn die unter "Ergebnisbedingungen" festgelegte dynamische Endzeit im Alarm unzureichend ist. Eine Einstellung ist unzureichend, wenn vor dem Einlesen der Datenbank nicht genügend Zeit für die Datenbankaktualisierung eingeräumt wird. Die Wahrscheinlichkeit, dass dieses Problem auftritt, wurde verringert, indem der Standardwert für die dynamische Endzeit für den vordefinierten Bereich "Letzte 5 Minuten" auf 'jetzt', '-2 Minuten' eingestellt wurde.

Lösung:

Ändern Sie die dynamische Endzeit im Schritt "Ergebnisbedingungen" des Aktionsalarms von 'jetzt', '-2 Minuten' in einen Wert, durch den mehr Zeit eingeräumt wird, beispielsweise in 'jetzt', '-10 Minuten'.

Einschränkung von Abfragen bei mehreren Suchbegriffen

Symptom:

Bei der Abfrage in einer einzelnen Suchspalte wird wie erwartet eine Suche durchgeführt, bei der die Groß- und Kleinschreibung nicht berücksichtigt wird. Bei einer Abfrage in mehreren Suchspalten wird jedoch eine von der Groß- und Kleinschreibung abhängige Suche durchgeführt, wobei Sternchen (*), die als Platzhalter interpretiert werden sollten, zeichengetreu interpretiert werden. Dieses Problem tritt auf, wenn der intern generierte SQL-Code in der WHERE-Klausel den OR-Operator enthält.

Lösung:

Beschränken Sie Ihre Abfragen bei der Verwendung von Eingabeaufforderungen auf die Suche in jeweils einer Spalte. Wenn Sie Ihre eigene Abfrage mit mehreren Ausdrücken erstellen, verbinden Sie mehrere LIKE-Platzhalterausdrücke mit dem logischen AND-Operator.

Fehler beim einfachen Filter von Abfrageassistenten bei Sonderzeichen

Symptom:

Wenn Sie in einem Abfrageassistenten in ein Feld für einen einfachen Filter eine Zeichenfolge eingeben, die Sonderzeichen enthält, treten Fehler auf. Sie können die Abfrage mit folgenden Sonderzeichen speichern und ausführen:

```
( ) & * > < ? : } {
```

Die Abfrage wird jedoch ohne dieses Feld als Filter ausgeführt, und es werden auch dann Daten angezeigt, wenn die Übereinstimmungsbedingung nicht erfüllt wird.

Lösung:

Verwenden Sie die aufgeführten Sonderzeichen nicht in Feldwerten für einfache Filter.

Keine Statusanzeige des geplanten Jobs nach Upgrade

Symptom:

Auf der Unterregisterkarte "Berichtsplanung" der Registerkarte "Geplante Berichte" können Sie alle geplanten Jobs und deren Status anzeigen. In der Statusspalte wird während des Prozesses der Berichterstellung "Wird erstellt" und wenn der Job geplant ist, "Geplant" angezeigt. Nach einem Upgrade von der Basisversion r12.0 GA wird der Inhalt der Statusspalte für Berichte unabhängig vom Status gelöscht. Wenn ein geplanter Bericht erneut generiert wird, wird dessen Status erneut angezeigt.

Lösung:

Das Fehlen eines Werts in der Statusspalte für einen geplanten Job ist nur ein vorübergehendes Anzeigeproblem. Keine Maßnahme ergreifen. Der korrekte Status wir das nächste Mal angezeigt, wenn der Bericht generiert wird.

Gewisse Aktionsalarmjobs schlagen fehl, wenn Sie zu häufig geplant werden

Symptom:

Wenn ein Aktionsalarm, der von Abfrageereignissen für ein bestimmtes Zeitintervall generiert wurde, häufiger geplant wurde, als der Dauer dieses Zeitintervalls entspricht, können jene Jobs, die sich überschneiden, fehlschlagen. Die folgende Meldung wird anzeigt: "Failed to generate the alert as the previous query is in progress". Wenn Sie z. B. eine Abfrage nach bestimmten Ereignissen durchführen möchten, die während der letzten drei Stunden generiert wurden, Sie die Abfrage jedoch so festgelegt haben, dass sie stündlich durchgeführt werden soll, kann der erste Job nicht abgeschlossen werden, bevor der zweite startet. CA Enterprise Log Manager fährt in diesem Fall mit der Ausführung des ersten Jobs fort und sendet Fehlermeldungen für die zwei nächsten geplanten Jobs. Sobald das dreistündige Intervall abgelaufen ist, wird ein Alarm gesendet, falls Ereignisse eingetreten sind, die die Kriterien erfüllen, und die nächste Ausführung dieses Alarms startet.

Lösung:

Wenn Sie im Schritt "Ergebnisbedingungen" nur einen Datumsbereich ausgewählt haben, wählen Sie ein Wiederholungsintervall aus, dass dem Intervall in "Auswahl des Datumsbereichs" *entspricht*. Wenn Sie z. B. eine Abfrage nach bestimmten Ereignissen durchführen möchten, die während der letzten drei Stunden generiert wurden und bestimmte Kriterien erfüllen, legen Sie im Schritt "Ergebnisbedingungen" in "Auswahl des Datumsbereichs" Folgendes fest:

Dynamische Endzeit: "Jetzt" - "2 Minuten"

Dynamische Startzeit: "Jetzt" - "182 Minuten"

Wenn Sie den Ablaufplan festlegen, sollten das Wiederholungsintervall im Schritt "Jobs planen" auf die folgende Weise auf einen Wert festlegen, der 3 Stunden (180 Minuten) entspricht:

Wiederholungsintervall: 3 Stunden

Indem Sie dieselben Intervalle für Abfrage und Wiederholung festlegen. stellen Sie sicher, dass jedes Ereignis, das die Kriterien erfüllt, durch die Erstellung eines Alarms festgehalten wird. Diese Empfehlung gilt nicht, wenn Sie ein Zeitintervall für gruppierte Ereignisse angeben.

Kennungen, die Sonderzeichen enthalten, können nicht gelöscht werden

Symptom:

Der Versuch, eine Abfrage- oder Berichtskennung zu löschen, die eines der Sonderzeichen ~ ! @ # $ % ^ & * ( ) _ + { } | : " < > ? enthält, schlägt fehl.

Lösung:

Verwenden Sie beim Erstellen von Abfrage- oder Berichtskennungen nicht die aufgeführten Sonderzeichen.

Automatisches Software-Update

Im Folgenden werden die bekannten Probleme in Verbindung mit automatischen Software-Updates aufgeführt.

Automatischer Neustart nach Aktualisierung des Betriebssystems während SP-Upgrade

Symptom:

Wenn die Aktualisierungsoption "Automatischer Neustart nach Aktualisierung des Betriebssystems" auf "Ja" eingestellt ist, wenn Sie das Service-Pack-Update anwenden, wird das Betriebssystem neu gestartet, bevor das binäre CA Enterprise Log Manager-Update abgeschlossen ist. Zu den nicht abgeschlossenen Updates zählt auch das Update der iGateway-Skripts zum Herunterfahren. Dieses Update muss angewendet werden, damit iGateway beim Neustart des Betriebssystems ordnungsgemäß heruntergefahren werden kann.

Lösung:

Stellen Sie die Aktualisierungsoption "Automatischer Neustart nach Aktualisierung des Betriebssystems" auf "Nein", bevor Sie das Update des Protokollmanagermoduls des Service Pack anwenden.

Fehler wegen ungenügenden Speicherplatzes bei Rechnern mit geringer Speicherkapazität

Symptom:

Das Herunterladen eines automatischen Software-Updates auf einen Computer, der über weniger als die empfohlenen 8 GB Speicherkapazität verfügt, kann aufgrund eines Java-Fehlers wegen ungenügenden Speicherplatzes fehlschlagen. Große Pakete werden mit iGateway heruntergeladen, wenn die Heapgröße für Java Virtual Machine (JVM) nicht eingestellt ist.

<so

Ändern Sie die Einstellung der JVM-Heapgröße, wenn Sie CA Enterprise Log Manager auf Hardware mit einer Speicherkapazität von weniger als den empfohlenen 8 GB installieren. Dazu müssen Sie die Datei "caelm-java.group" bearbeiten.

So ändern Sie die Einstellung der JVM-Heapgröße:

1. Melden Sie sich beim CA Enterprise Log Manager Server mit "caelmadmin" an.
2. Navigieren Sie zum iGateway-Ordner.

3. Öffnen Sie die Datei "caelm-java.group", und suchen Sie den Abschnitt mit den JVM-Einstellungen.
4. Fügen Sie, wie in der nachstehenden Graphik dargestellt, eine Zeile hinzu:

```
<JVMSettings>
        <loadjvm>true</loadjvm>
        <Javahome>/usr/java/latest/jre</javahome>
        <Properties
name="java.endorsed.dirs=/opt/CA/SharedComponents/iTechnology/endorsed">
            <System-
properties>java.endorsed.dirs=/opt/CA/SharedComponents/iTechnology/endorsed</
system-properties>
        </Properties>
    <Properties name="maxmemory"><jvm-property>-Xmx1250M</jvm-
property></Properties>
    </JVMSettings>
```

5. Speichern und schließen Sie die Datei "caelm-java.group".

Wichtiger Hinweis: Das Einstellen der JVM-Heapgröße kann bei der Verwendung der Option "In PDF-Datei exportieren" bei großen Datensätzen Probleme verursachen. Daher sollte diese Option im Idealfall nur bei kleinen Computern verwendet werden.

Sperrung des Domänenkontos aufgrund von geänderten Proxy-Anmeldeinformationen

Symptom:

In einer Umgebung mit einem CA Enterprise Log Manager-Server funktionieren Ihre Domänenanmeldeinformationen nicht, und Ihr Konto ist gesperrt.

Lösung:

Der CA Enterprise Log Manager-Server kontaktiert regelmäßig den CA-Software-Update-Server, um nach Produktaktualisierungen zu suchen. Wenn die Proxy-Anmeldeinformationen (wie z. B. Benutzer-ID und Kennwort) abgelaufen sind oder geändert wurden, kann CA Enterprise Log Manager den Software-Update-Server nicht kontaktieren und generiert ein selbstüberwachendes Ereignis für die fehlgeschlagene Anmeldung. Das selbstüberwachende Ereignis zeigt eine Meldung an, die etwa folgenden Wortlaut hat:

```
Verbindung zu Software-Update-Server konnte nicht hergestellt werden. Entweder der Server ist ausgefallen, die Verbindung wurde abgelehnt oder die Proxyserver-Einstellungen sind nicht korrekt. Bitte validieren Sie die Proxyserver-Einstellungen.
```

Wenn die fehlgeschlagenen Anmeldungen weiterhin zugelassen werden, wird das Domänenkonto, je nach den lokalen Richtlinien, möglicherweise gesperrt. Stellen Sie sicher, dass die Proxy-Anmeldeinformationen nicht geändert wurden oder abgelaufen sind.

Wir empfehlen, dass für das Service-Konto, das zum Kontaktieren des Software-Update-Servers verwendet wird, keine Richtlinie zum Kennwortablauf festgelegt wird.

Selbstüberwachendes Ereignis zur Neustartaufforderung wird nur einmal angezeigt

Symptom:

Wenn Sie angeben, dass ein Betriebssystemmodul automatische Updates herunterladen und ohne einen Neustart installieren soll, wird das folgende selbstüberwachende Ereignis nur einmal generiert: "Auf diesem Host sind Aktualisierungen für das Betriebssystem installiert ... Starten Sie den Rechner neu, damit die Änderungen wirksam werden!!!"

Lösung:

Das automatische Software-Update generiert ein Ereignis, durch das Sie daran erinnert werden, das Betriebssystem nur einmal neu zu starten, wenn ein manueller Neustart erforderlich ist. Es ist gute Praxis, einen Alarm für dieses Ereignis zu erstellen.

Die Module für automatische Software-Updates müssen nach dem Upgrade neu ausgewählt werden

Symptom:

Beim Upgrade von CA Enterprise Log Manager auf Version 12.1 werden sämtliche bisher ausgewählten Module für automatische Software-Updates von der Liste der ausgewählten Module in die Liste der verfügbaren Module verschoben. Dies verhindert weitere automatische Software-Updates für diese Module.

Lösung:

Nach Abschließen des Upgrades wählen Sie die Module wie folgt neu aus:

Module für automatische Software-Updates neu auswählen

1. Melden Sie sich in CA Enterprise Log Manager an. Klicken Sie auf die Registerkarte 'Verwaltung' und danach auf die untergeordnete Registerkarte 'Dienste'.
2. Öffnen Sie für alle Server, die Sie aktualisieren möchten, das Modul für automatische Software-Updates.
3. Mit der Wechselsteuerung können Sie die Module, die für Updates verfügbar sein sollen, von der Liste der verfügbaren Module in die Liste der ausgewählten Module verschieben.
4. Klicken Sie auf "Speichern".

Schaltfläche "Proxy testen" liefert nach Konfigurationsänderung falsch positive Ergebnisse

Symptom:

Wenn Sie Einstellungen des CA Enterprise Log Manager-Proxy-Servers nach einem erfolgreichen Test ändern und mit Hilfe der Schaltfläche "Proxy testen" erneut einen Test durchführen, wird eine Bestätigungsmeldung angezeigt – unabhängig davon, ob die neue Konfiguration korrekt ist oder nicht.

Lösung:

Bei der Schaltfläche "Proxy testen" erfolgt der Zugriff auf eine URL anhand der angegebenen Proxy-Konfiguration über den betreffenden Proxy. Die Daten einer Client-Authentifizierung werden von Proxy-Servern im Allgemeinen im Cache abgelegt, wenn sie gültig sind. Danach eingehende Anmeldeinformationen werden ignoriert, bis etwas Zeit verstrichen ist.

Nachdem über die Schaltfläche "Proxy testen" die Gültigkeit der Konfiguration festgestellt wurde, wird bei nachfolgenden Prüfungen von nicht korrekten Konfigurationen also möglicherweise für einen bestimmten Zeitraum fälschlicherweise angezeigt, dass die Konfigurationen gültig sind.

Zwei Unterdrückungsregeln werden nicht ordnungsgemäß angewendet

Symptom:

Die beiden folgenden Unterdrückungsregeln sind Teil von r12.0 und werden nicht ordnungsgemäß angewendet:

- TMCM - Meldungen zur erfolgreichen Aktualisierung von Virensignaturen & Viren-Engines
- TMCM - Erfolgsmeldungen zur Aktualisierung von Virensignaturen & Viren-Engines

Lösung:

Die Regeln werden wegen des kaufmännischen Und-Zeichens im Titel nicht ordnungsgemäß angewendet. Das Upgrade von r12.1 enthält die folgenden Ersatzregeln:

- TMCM - Meldungen zur erfolgreichen Aktualisierung von Virensignaturen und Viren-Engines
- Erfolgsmeldungen zur Aktualisierung von McAfee-Virensignaturen und -Viren-Engines

Verwenden Sie diese Regeln statt der älteren Versionen, die das kaufmännische Und-Zeichen enthalten.

Aktualisierung auf r12.1 erfordert Neustart von iGateway

Symptom:

In einer föderierten Umgebung wird die Aktualisierung von r12.0 auf r12.1 erst nach einem Neustart von iGateway abgeschlossen.

Lösung:

Die Binärdateien für die Aktualisierung werden vom Client für automatische Software-Updates zwar kopiert und extrahiert, aber nicht installiert: Sie verbleiben unverändert im Verzeichnis "/tmp/downloads". Daran erkennen Sie, dass der Aktualisierungsprozess bei einem automatischen Software-Update nicht abgeschlossen wurde. An diesem Punkt müssen Sie iGateway manuell neu starten. Dazu gehen Sie wie folgt vor:

So starten Sie den iGateway-Daemon oder -Service neu:

1. Melden Sie sich als "caelmadmin"-Benutzer beim CA Enterprise Log Manager-Server an.
2. Schalten Sie Benutzer mit dem folgenden Befehl zum Root-Konto um:

   ```
   su -
   ```

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

   ```
   $IGW_LOC/S99igateway stop
   ```

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

   ```
   $IGW_LOC/S99igateway start
   ```

Hierdurch kann die Aktualisierung abgeschlossen werden.

Ein Upgrade auf r12.1 SP1 kann einen Neustart von iGateway erforderlich machen

Symptom:

Upgrades von r12.1 auf r12.1 SP1 werden möglicherweise nicht zeitgerecht abgeschlossen. Wenn die Aktualisierung nach mehr als eineinhalb Stunden nicht abgeschlossen ist, kann ein Neustart von iGateway erforderlich sein.

Lösung:

Wir empfehlen den folgenden Vorgang, um dieses Problem zu identifizieren:

1. Schließen Sie das Inhalts-Update - Berichte und Integrationen - von 12.1 GA ab.
2. Schließen Sie das binäre Update - Server, Agent, BS-Module - zu SP1 ab.

So können Sie die Zeit zum Herunterladen der einzelnen Module, die je nach Modulgröße unterschiedlich sein kann, differenzieren. Wenn ein Teil des Updates zu viel Zeit benötig und nicht fertig gestellt wird, führen Sie über die CA Enterprise Log Manager-Benutzeroberfläche einen Neustart von iGateway durch.

So starten Sie den iGateway-Service 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.
4. Klicken Sie unter "Services" auf die Registerkarte "Verwaltung".
5. Klicken Sie auf "iGateway neu starten".

Ein aktualisierter Syslog-Protokollsensor unter r12.1 SP1 macht eine Aktualisierung zu Integrationen auf Windows-Agenten erforderlich

Symptom:

Wenn Sie die Aktualisierung des Integrationsmoduls während des Upgrades auf r12.1 SP1 nicht anwenden, werden Connectors, die den Syslog-Protokollsensor verwenden, nicht mehr funktionieren. Der folgende Fehler wird in der Protokolldatei des Agenten angezeigt:

```
[6072] 03/09/10 17:22:51 ERROR :: MySAX2Handler::fatalError: at line1
[6072] 03/09/10 17:22:51 ERROR :: XMLTree::ParseUsingSAX2:error parsing
stringintruvert/jsp/admin/Login.jsp
[6072] 03/09/10 17:22:51 ERROR :: XMLTree::Parse Exit ParseUsingSAX2 FAILURE
[6072] 03/09/10 17:22:51 ERROR :: HTTP_Processor::ParseRequestXML: Unknown
request format:intruvert/jsp/admin/Login.jsp
```

Überprüfen Sie zusätzlich die Version der Integration. Wenn es sich um eine frühere Version als 12.1.5104.0 handelt, müssen Sie das Upgrade anwenden.

Lösung:

Wenden Sie die Aktualisierung des Integrationsmoduls an. Führen Sie danach ein Upgrade für all jene Integrationen durch, die Version 12.1.5104.0 oder später des Syslog-Protokollsensors verwenden. Alternativ können Sie die Schritten durchführen, die im Abschnitt "Aktualisierung mehrerer Connector-Konfigurationen" des *Administrationshandbuchs* beschrieben werden.

Eine Liste der Integrationen, die den Syslog-Protokollsensor verwenden, können Sie in der CA Enterprise Log Manager-Produktintegrationsmatrix einsehen: https://support.ca.com/irj/portal/anonymous/phpdocs?filePath=0/8238/8238_integration_certmatrix.html.

Benutzer- und Zugriffsverwaltung

Im Folgenden werden die bekannten Probleme in Verbindung mit der Benutzer- und Zugriffsverwaltung aufgeführt.

Zugriffsbeschränkungen von einem Browser unter Windows Vista

Symptom:

Wenn Sie sich bei CA Enterprise Log Manager von einem Computer mit einem Windows Vista SP1-Betriebssystem anmelden, das IPv6-aktiviert ist, haben Sie von keinem Browser Zugriff auf die Funktionen der Schaltflächen in der Unterregisterkarte "Benutzer- und Zugriffsverwaltung" der Registerkarte "Verwaltung".

Benutzer, die sich mit EiamAdmin-Anmeldeinformationen oder den Anmeldeinformationen eines CA Enterprise Log Manager-Benutzerkontos, dem eine Administratorrolle zugewiesen wurde, anmelden, sollten Zugriff auf diese Funktionen haben. Diese Einschränkung liegt nicht bei Benutzern vor, die von einem anderen Windows-Betriebssystem zu CA Enterprise Log Manager browsen. Sie liegt nur beim Browsen zu CA Enterprise Log Manager von einem Windows Vista-Computer mit einer URL im folgenden Format vor: https://[*ipv6-Adresse*]:5250/spin/calm. Der folgende URL ist ein Beispiel:

```
Beispiel:  https://[::FFFF:192.168.00.00]:5250/spin/eiam
```

Lösung:

Sie können dieses Problem umgehen, indem Sie über einen anderen URL auf die Funktionen der Benutzer- und Zugriffsverwaltung zugreifen.

1. Geben Sie die folgende URL in Ihren Browser ein, wobei die IPv6-Adresse die URL zu Ihrem CA Enterprise Log Manager-Verwaltungsserver ist.

   `https://[ipv6-Adresse]:5250/spin/eiam`

2. Wählen Sie "CAELM" in der Dropdown-Liste "Anwendung" aus.
3. Geben Sie als Benutzername und Kennwort entweder "EiamAdmin" mit dem Kennwort für dieses Konto oder die Anmeldeinformationen für einen CA Enterprise Log Manager-Benutzer mit Administratorrolle ein.
4. Klicken Sie auf die Registerkarte "Identitäten verwalten", um Benutzer und Gruppen zu konfigurieren.
5. Klicken Sie auf die Registerkarte "Zugriffsrichtlinien verwalten", um Tests oder Kalender zu konfigurieren.
6. Klicken Sie auf die Registerkarte "Konfigurieren", "EEM-Server", um globale Benutzer, globale Gruppen oder Kennwortrichtlinien zu konfigurieren.

Einschränkung bei der Verwendung des Kalenders mit Zugriffsrichtlinien

Symptom:

An bestimmten Tagen und zu bestimmten Uhrzeiten, die in einem Kalender mit einer Richtlinie angegeben sind, die Zugriff ausdrücklich gewährt, haben Sie als Benutzer oder als Gruppe eingeschränkten Zugriff auf CA Enterprise Log Manager. Der Kalender funktioniert jedoch nicht wie erwartet bei einer Richtlinie, die den Zugriff ausdrücklich verweigert.

Lösung:

Verwenden Sie den Richtlinientyp, der den Zugriff ausdrücklich gewährt, um die Zeiten zu beschränken, an denen Sie einer Gruppe Zugriff gewähren möchten, anstatt eine Richtlinie zu verwenden, die den Zugriff ausdrücklich verweigert.

Sonstiges

Im Folgenden werden die verschiedenen bekannten Probleme erläutert.

Ausbleibende Reaktionen von CA Enterprise Log Manager

Symptom:

CA Enterprise Log Manager reagiert manchmal nicht. Das bedeutet, dass die Benutzeroberfläche nicht auf Benutzeranfragen reagiert und interne Anfragen vom Agenten zum Agentenmanager aufhören. Die Protokollerfassung wird jedoch fortgeführt.

Lösung:

Gehen Sie folgendermaßen vor, um den iGateway-Prozess zu beenden und erneut zu starten:

1. Melden Sie sich bei dem CA Enterprise Log Manager-Server, der nicht reagiert über "ssh" als caelmadmin-Benutzer an.
2. Schalten Sie Benutzer mit dem folgenden Befehl zum Root-Konto um, und stellen Sie das entsprechende Kennwort bereit:

   ```
   su -
   ```

3. Wechseln Sie in das Verzeichnis "$IGW_LOC".

   Standardmäßig ist iGateway im Verzeichnis /opt/CA/SharedComponents/iTechnology gespeichert.

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

   ```
   ./S99igateway stop
   ```

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

   ```
   ./S99igateway start
   ```

Aufrufe von API-Abfragen und -Berichten schlagen unter bestimmten Browsern fehl

Symptom:

Bei der Verwendung der offenen Schnittstelle geben die Aufrufe von getQueryViewer oder getReportViewer an Microsoft Internet Explorer 7 oder 8 oder Mozilla Firefox keine Ergebnisse zurück.

Lösung:

Unter den erwähnten Browsern erkennt die CA Enterprise Log Manager-API den Parameter "Server" der URL des API-Aufrufs nicht. Um dieses Problem zu vermeiden, geben Sie bei getQueryViewer- oder getReportViewer-Aufrufen keine Serverparameter an. Sobald die CA Enterprise Log Manager-Benutzeroberfläche angezeigt wird, wählen Sie den gewünschten Server aus der Dropdown-Liste der Protokollmanager-Server im oberen Bereich der Startseite aus.

Weitere Informationen zu URLs von API-Aufrufen finden Sie im *CA Enterprise Log Manager-API-Programmierhandbuch*.

CAELM4Audit wird nicht mehr unterstützt

CA Enterprise Log Manager r12.1 SP1 verwendet CA EEM r8.4 SP3, welches nicht für die Verwendung mit CA Audit zertifiziert ist. Dies bedeutet, dass CA Audit in einer nicht unterstützten Konfiguration ausgeführt wird, da die Integration zwischen CA Enterprise Log Manager und CA Audit die gemeinsame Benutzung eines CA EEM-Servers erfordert.

Da CA Audit außerdem nicht FIPS-konform ist, hört die Benutzeroberfläche des Audit-Administrator beim Aktivieren des CA Enterprise Log Manager-FIPS-Modus zu funktionieren auf.

Auswirkung von benutzerdefinierten Anwendungsnamen auf die Archivabfrage

Symptom:

In einer Umgebung mit mehreren CA Enterprise Log Manager-Servern, die denselben Verwaltungsserver verwenden, werden durch eine Archivabfrage gewöhnlich Ergebnisse aus den Archivverzeichnissen aller Server zurückgegeben. Wenn Sie jedoch bei der Installation des CA Enterprise Log Manager-Verwaltungsservers einen benutzerdefinierten Anwendungsnamen festlegen und nicht den Standardnamen "CAELM" übernehmen, funktioniert die Archivabfrage nicht wie erwartet. Stattdessen werden durch die Archivabfrage nur für den Server, auf dem die Abfrage ausgeführt wird, Ergebnisse zurückgegeben. Ergebnisse von weiteren Servern werden wie folgt angezeigt: *<host>User CERT-custom: Access is denied*.

Lösung:

Führen Sie die Archivkatalogabfrage separat auf jedem CA Enterprise Log Manager-Server aus.

Hohe Kontrasteinstellungen des Bildschirms

Symptom:

In Windows wird nur die hohe Kontrasteinstellung "Kontrast Schwarz" unterstützt. Die anderen drei Optionen für hohen Kontrast werden nicht unterstützt. Zu den Optionen für hohen Kontrast zählen "Kontrast Nr. 1", "Kontrast Nr. 2", "Kontrast Schwarz" und "Kontrast Weiß".

Lösung:

Wählen Sie die Einstellung "Kontrast Schwarz" aus, wenn eine hohe Kontrasteinstellung erforderlich ist. Um diese Option festzulegen, wählen Sie aus der Systemsteuerung "Anzeige" aus. Diese Eingabehilfeoption wird im Dialogfeld "Anzeigeeigenschaften" auf der Registerkarte "Darstellung" in der Dropdownliste "Farbschema" festgelegt.

Fortlaufendes Beenden und Neustarten von iGateway

Symptom:

Die CA Enterprise Log Manager-Benutzeroberfläche reagiert während einzelner Vorgänge nicht. Eine Überprüfung des CA Enterprise Log Manager-Servers ergibt, dass iGateway beendet und neu gestartet wird, jedoch nicht aktiviert bleibt. Überprüfen Sie iGateway mithilfe des folgenden Prozesses:

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

   ```
   su - root
   ```

4. Prüfen Sie mithilfe des folgenden Befehls, ob der iGateway-Prozess ausgeführt wird:

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

   Das Betriebssystem gibt Informationen zu iGateway-Prozessen sowie eine Liste von Prozessen, die unter iGateway ausgeführt werden, zurück.

Lösung:

Beheben Sie das Problem durch folgende Schritte:

1. Gehen Sie zu $IGW_LOC (/opt/CA/SharedComponents/iTechnology), und suchen Sie folgende Datei:

   ```
   saf_epSIM.*
   ```

   Es gibt verschiedene Versionen, die fortlaufend nummeriert sind, wie z. B. saf_epSIM.1, saf_epSIM.2, saf_epSIM.3 usw.

2. Benennen Sie die Datei mit der niedrigsten Zahl um, und speichern Sie sie an einem anderen Ort zur Übermittlung an den CA-Support.
3. Wenn iGateway nicht automatisch neu gestartet wird, nehmen Sie einen Neustart vor:

   a. Melden Sie sich als "root"-Benutzer an.

   b. Greifen Sie auf eine Eingabeaufforderung zu, und geben Sie den folgenden Befehl ein:

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

Maximaler Speicherplatz für virtuellen CA Enterprise Log Manager ist zu klein

Symptom:

In VMware ESX Server v3.5 kann bei einem zugewiesenen Speicherplatz von 512 GB keine virtuelle Maschine erstellt werden. Der virtuelle CA Enterprise Log Manager-Server benötigt mehr als den maximalen Speicherplatz von 256 GB, um das Ereignisvolumen zu verarbeiten.

Lösung:

VMWare ESX Server verwendet eine Standardblockgröße von 1 MB und kalkuliert den maximalen Speicherplatz unter Verwendung dieses Werts. Wenn die Blockgröße auf 1 MB festgelegt ist, wird standardmäßig ein maximaler Speicherplatz von 256 GB festgelegt. Wenn Sie mehr als 256 GB virtuellen Speicherplatz konfigurieren möchten, können Sie die Standardblockgröße erweitern.

So erstellen Sie einen größeren virtuellen Datenträger:

1. Greifen Sie auf die Servicekonsole im VMware ESX Server zu.
2. Erweitern Sie die Blockgröße mit dem folgenden Befehl auf 2 MB:

   ```
   vmkfstools --createfs vmfs3 --blocksize 2M vmhba0:0:0:3
   ```

   In diesem Befehl bedeutet der Wert "2M" 512 GB (2 x 256).
3. Starten Sie den VMware ESX Server neu.
4. Erstellen Sie eine neue virtuelle Maschine mit einem Speicherplatz von 512 GB.

Weitere Informationen zu diesem und anderen Befehlen finden Sie in der Dokumentation zu VMware ESX Server.

Benutzer werden beim Aktualisieren des Browsers von CA Enterprise Log Manager abgemeldet

Symptom:

Wenn Sie den Browser aktualisieren, während Sie bei CA Enterprise Log Manager angemeldet sind, wird Ihre Sitzung beendet, und Sie werden abgemeldet.

Lösung:

Die Browser-Aktualisierung wird von CA Enterprise Log Manager aufgrund der Einschränkungen von Flex nicht unterstützt. Vermeiden Sie die Aktualisierung Ihres Browsers.

Nach dem Neustart von iGateway können auf der Dienst- oder der Explorer-Benutzeroberfläche Fehler auftreten

Symptom:

Wenn Sie unmittelbar nach einem Neustart von iGateway auf ein Objekt in der Dienst- oder Explorer-Schnittstellenverzeichnisstruktur von CA Enterprise Log Manager klicken, wird anstelle des gewünschten Inhalts möglicherweise die Fehlermeldung "Network error on receive" angezeigt.

Lösung:

Dieser Fehler tritt auf, wenn Sie nach dem Neustart von iGateway versuchen, auf eines der beschriebenen Objekte zuzugreifen, während sie noch neu geladen werden. Warten Sie fünf Minuten, damit der Ladevorgang abschließen kann, und klicken Sie danach auf das gewünschte Dienst- oder Explorerelement.

Uploads und Importe funktionieren ausschließlich mit Internet Explorer.

Symptom:

Der Großteil der CA Enterprise Log Manager-Tasks kann mit Mozilla Firefox, Safari oder Chrome erfolgreich durchgeführt werden. Uploads oder Importe schlagen mit diesen Browsern jedoch fehl. Beispiele:

- Beim Import einer Abfragedefinition erscheint die Fehlermeldung "E/A-Fehler: Fehler bei der Anforderung".
- Das Upload einer CSV-Datei mit dem Assistenten zur Massenbereitstellung von Connectors schlägt fehl, obwohl die Meldung "Datei wird hochgeladen." erscheint.

Lösung:

Rufen Sie CA Enterprise Log Manager mit Microsoft Internet Explorer auf, wenn Sie Dateien hochladen oder importieren möchten.

Die Benutzeroberfläche wird nach der Installation mit Remote EEM unerwarteterweise nicht richtig angezeigt.

Symptom:

Nach der Installation von CA Enterprise Log Manager mit einem Remote-EEM-Server, wird die Benutzeroberfläche bei der ersten Anmeldung manchmal nicht richtig angezeigt. Überprüfen der iGateway-Protokolldateien zeigt, dass die Services "agentmanager", "calmreporter", "subscclient" und "subscproxy" nicht gestartet wurden.

Die Protokolldateien haben etwa folgende Syntax:

```
[1087523728] 23.09.09 20:35:32 ERROR :: Certificate::loadp12 :
etpki_file_to_p12 failed [ errorcode : -1 ]

[1087523728] 23.09.09 20:35:32 ERROR :: Certificate::loadp12 :
etpki_file_to_p12 failed [ errorcode : -1 ]

[1087523728] 23.09.09 20:35:32 ERROR :: Certificate::loadp12 :
etpki_file_to_p12 failed [ errorcode : -1 ]

[1087527824] 23.09.09 17:00:07 ERROR ::
OutProcessSponsorManager::stopSponsorGroup : terminating safetynet process
for SponsorGroup [ caelm-msgbroker ] didn't respond OK for the termination
call

[1087527824] 23.09.09 17:00:07 ERROR ::
OutProcessSponsorManager::stopSponsorGroup : terminating safetynet process
for SponsorGroup [ caelm-oaserver ] didn't respond OK for the termination
call

[1087527824] 23.09.09 17:00:07 ERROR ::
OutProcessSponsorManager::stopSponsorGroup : terminating safetynet process
for SponsorGroup [ caelm-sapicollector ] didn't respond OK for the
termination call

[1087527824] 23.09.09 17:07:46 ERROR :: OutProcessSponsorManager::start :
SponsorGroup [ caelm-java ] failed to start ]

[1087527824] 23.09.09 17:07:49 ERROR :: SponsorManager::start : Sponsor [
agentmanager ] failed to load

[1087527824] 23.09.09 17:07:49 ERROR :: SponsorManager::start : Sponsor [
calmreporter ] failed to load

[1087527824] 23.09.09 17:07:49 ERROR :: SponsorManager::start : Sponsor [
subscclient ] failed to load

[1087527824] 23.09.09 17:07:49 ERROR :: SponsorManager::start : Sponsor [
subscproxy ] failed to load
```

Lösung:

Sie können dieses Problem beheben, indem Sie iGateway neu starten und sich erneut bei der Schnittstelle anmelden.

So starten Sie den iGateway-Service 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.
4. Klicken Sie unter "Services" auf die Registerkarte "Verwaltung".
5. Klicken Sie auf "iGateway neu starten".

Kapitel 7: Behobene Probleme

Dieses Kapitel enthält folgende Themen:

In r12.1 SP1 behobene Probleme

Die folgenden von Kunden berichteten Probleme wurden in CA Enterprise Log Manager r12.1 SP1 behoben:

- 18789166-1
- 18790979-1
- 18955095-1
- 18973282-1
- 18982868-1
- 18988854-1
- 19005999-1
- 19066155-1
- 19077668-1
- 19087827-1
- 19127553-1
- 19176852-1
- 19182913-1
- 19188433-2

Kapitel 8: Dokumentation

Dieses Kapitel enthält folgende Themen:

Bookshelf

Der Bookshelf ermöglicht von einem zentralen Ort aus Zugriff auf die gesamte Dokumentation von CA Enterprise Log Manager. Der Bookshelf enthält Folgendes:

- Eine gemeinsame, erweiterbare Inhaltsliste für alle Handbücher im HTML-Format
- Volltextsuche über alle Handbücher mit bewerteten Suchergebnissen und im Inhalt hervorgehobenen Suchbegriffen

  Hinweis: Wenn Sie nach ausschließlich numerischen Begriffen suchen, leiten Sie den Suchwert durch ein Sternchen ein.
- Klickelemente ("Brotkrümel"), die zu übergeordneten Themen führen
- Gemeinsamer Index für alle Handbücher
- Links zu PDF-Versionen der Handbücher zum Drucken

Zugriff auf das Bookshelf

Bookshelfs zu CA-Produktdokumentationen stehen in Form von .zip-Dateien namens "All Guides Including a Searchable Index" zum Download zur Verfügung.

Zugriff auf das CA Enterprise Log Manager-Bookshelf

1. Gehen Sie zu Search Documentation / Guides
2. Geben Sie als Produkt "CA Enterprise Log Manager" ein, wählen Sie eine Version und eine Sprache aus, und klicken Sie auf "Go".
3. Laden Sie die .zip-Datei auf Ihren Desktop oder einen anderen Speicherort herunter.
4. Öffnen Sie die .zip-Datei auf und ziehen Sie den Ordner mit dem Bookshelf auf Ihren Desktop, oder extrahieren Sie ihn zu einem anderen Speicherort.
5. Öffnen Sie den Bookshelf-Ordner.
6. Öffnen Sie das Bookshelf.
   - Wenn sich das Bookshelf auf dem lokalen System befindet und Sie Internet Explorer verwenden, öffnen Sie die Datei "Bookshelf.hta".
   - Wenn sich das Bookshelf auf dem Remote-System befindet oder Sie Mozilla Firefox verwenden, öffnen Sie die Datei "Bookshelf.html".

   Das Bookshelf wird geöffnet.

Anhang A: Vereinbarung gegenüber Drittparteien

Dieses Kapitel enthält folgende Themen:

Adaptive Communication Environment (ACE)

Copyright und Lizenzierungsinformationen für ACE(TM), TAO(TM) und CIAO(TM).

ACE(TM), TAO(TM) and CIAO(TM) are copyrighted by Douglas C. Schmidt and his research group at Washington University, University of California, Irvine, and Vanderbilt University Copyright (c) 1993-2003, all rights reserved. Since ACE TAO CIAO are open-source, free software, you are free to use, modify, copy, and distribute--perpetually and irrevocably--the ACE TAO CIAO source code and object code produced from the source, as well as copy and distribute modified versions of this software. You must, however, include this copyright statement along with code built using ACE TAO CIAO.

You can use ACE TAO CIAO in proprietary software and are under no obligation to redistribute any of your source code that is built using ACE TAO CIAO. Note, however, that you may not do anything to the ACE TAO CIAO code, such as copyrighting it yourself or claiming authorship of the ACE TAO CIAO code, that will prevent ACE TAO CIAO from being distributed freely using an open-source development model. You needn't inform anyone that you're using ACE TAO CIAO in your software, though we encourage you to let us know so we can promote your project in the ACE TAO CIAO success stories.

ACE TAO CIAO are provided as is with no warranties of any kind, including the warranties of design, merchantability, and fitness for a particular purpose, noninfringement, or arising from a course of dealing, usage or trade practice. Moreover, ACE TAO CIAO are provided with no support and without any obligation on the part of Washington University, UC Irvine, Vanderbilt University, their employees, or students to assist in its use, correction, modification, or enhancement. A number of companies provide commercial support for ACE and TAO, however. ACE, TAO and CIAO are Y2K-compliant, as long as the underlying OS platform is Y2K-compliant.

Washington University, UC Irvine, Vanderbilt University, their employees, and students shall have no liability with respect to the infringement of copyrights, trade secrets or any patents by ACE TAO CIAO or any part thereof. Moreover, in no event will Washington University, UC Irvine, or Vanderbilt University, their employees, or students be liable for any lost revenue or profits or other special, indirect and consequential damages.

The ACE, TAO and CIAO web sites are maintained by the Center for Distributed Object Computing of Washington University for the development of open-source software as part of the open-source software community. By submitting comments, suggestions, code, code snippets, techniques (including that of usage), and algorithms, submitters acknowledge that they have the right to do so, that any such submissions are given freely and unreservedly, and that they waive any claims to copyright or ownership. In addition, submitters acknowledge that any such submission might become part of the copyright maintained on the overall body of code, which comprises the ACE, TAO and CIAO software. By making a submission, submitter agree to these terms. Furthermore, submitters acknowledge that the incorporation or modification of such submissions is entirely at the discretion of the moderators of the open-source ACE TAO CIAO projects or their designees.

The names ACE(TM), TAO(TM), CIAO(TM), Washington University, UC Irvine, and Vanderbilt University, may not be used to endorse or promote products or services derived from this source without express written permission from Washington University, UC Irvine, or Vanderbilt University. Further, products or services derived from this source may not be called ACE(TM), TAO(TM), or CIAO(TM) nor may the name Washington University, UC Irvine, or Vanderbilt University appear in their names, without express written permission from Washington University, UC Irvine, and Vanderbilt University.

If you have any suggestions, additions, comments, or questions, please let me know.

Douglas C. Schmidt

Software unter der Apache-Lizenz

Dieses Produkt benützt die folgenden Software von Apache:

- Ant 1.6.5
- Formatting Objects Processor (FOP) 0.95
- Jakarta POI 3.0
- Log4cplus 1.0.2
- Log4J 1.2.15
- Quarz 1.5.1
- Xerces-C 2.6.0

Teile-Dieses-Produkts-Enthalten-Software, als Von-Apachen-Software-Gründungs-Entwickelt-Wurde sterben. Diese-Apache-Software-Wird in Übereinstimmung-Mit-Der-Nachfolgenden-Lizenzvereinbarung-Vertrieben:

Apache-Lizenz

Version 2.0, Januar 2004

http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

'License' shall mean the terms and conditions for use, reproduction,and distribution as defined by Sections 1 through 9 of this document.

'Licensor' shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

'Legal Entity' shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, 'control' means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

'You' (or 'Your') shall mean an individual or Legal Entity exercising permissions granted by this License.

'Source' form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

'Object' form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and versions to other media types.

'Work' shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

'Derivative Works' shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

'Contribution' shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, 'submitted' means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as 'Not a Contribution.'

'Contributor' shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s)with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

(a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

(b) You must cause any modified files to carry prominent notices stating that You changed the files; and

(c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

(d) If the Work includes a 'NOTICE' text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an 'AS IS' BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

boost 1.35.0

Dieses Produkt umfasst Software, die gemäß dem folgenden Lizenzvertrag vertrieben wird:

Boost-Softwarelizenz - Version 1.0, 17. August 2003

Permission is hereby granted, free of charge, to any person or organization obtaining a copy of the software and accompanying documentation covered by this license (the "Software") to use, reproduce, display, distribute, execute, and transmit the Software, and to prepare derivative works of the Software, and to permit third-parties to whom the Software is furnished to do so, all subject to the following:

The copyright notices in the Software and this entire statement, including the above license grant, this restriction and the following disclaimer, must be included in all copies of the Software, in whole or in part, and all derivative works of the Software, unless such copies or derivative works are solely in the form of machine-executable object code generated by a source language processor.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR ANYONE DISTRIBUTING THE SOFTWARE BE LIABLE FOR ANY DAMAGES OR OTHER LIABILITY, WHETHER IN CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

JDOM 1.0

Dieses Produkt umfasst Software, die vom JDOM-Projekt (http://www.jdom.org/) entwickelt wurde. Die JDOM-Software wird in Übereinstimmung mit dem folgenden Lizenzvertrag vertrieben.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions, and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the disclaimer that follows these conditions in the documentation and/or other materials provided with the distribution.

3. The name "JDOM" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact

4. Products derived from this software may not be called "JDOM", nor may "JDOM" appear in their name, without prior written permission from the JDOM Project Management .

In addition, we request (but do not require) that you include in the end-user documentation provided with the redistribution and/or in the software itself an acknowledgement equivalent to the following: "This product includes software developed by the JDOM Project (http://www.jdom.org/)." Alternatively, the acknowledgment may be graphical using the logos available at http://www.jdom.org/images/logos.

THIS SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE JDOM AUTHORS OR THE PROJECT CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Diese Software ist das Ergebnis der freiwilligen Beiträge vieler Einzelpersonen, die sich am JDOM-Projekt beteiligen, und wurde ursprünglich von Jason Hunter und Brett McLaughlin entwickelt. Weitere Informationen zum JDOM-Projekt erhalten Sie unter http://www.jdom.org.

PCRE 6.3

Teile dieses Produkts umfassen Software, die von Philip Hazel entwickelt wurde. Die Software von University of Cambridge Computing Service wird in Übereinstimmung mit dem folgenden Lizenzvertrag vertrieben.

DIE GRUNDLEGENDEN BIBLIOTHEKSFUNKTIONEN

Verfasst von: Philip Hazel

Lokaler Teil der E-Mail-Adresse: ph10

E-Mail-Domäne: cam.ac.uk

University of Cambridge Computing Service,

Cambridge, England. Tel.: +44 1223 334714.

DIE C++ WRAPPER-FUNKTIONEN

Bereitgestellt von: Google Inc.

Die "BSD"-LIZENZ

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of the University of Cambridge nor the name of Google Inc. nor the names of their contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS"

AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Ende

zlib 1.2.3

Dieses Produkt umfasst zlib, ein von Jean-loup Gailly und Mark Adler entwickeltes Programm.

ZThread 2.3.2

Teile dieses Produkts umfassen Software, die von Eric Crahen entwickelt wurde. Die Software "ZThread" wird in Übereinstimmung mit dem folgenden Lizenzvertrag vertrieben.