CA Enterprise Log Manager

Versionshinweise

r12.1 SP2

CA-Produktreferenzen

Dieses Dokument bezieht sich auf die folgenden Produkte von CA:

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

Technischer Support – Kontaktinformationen

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

Änderungen in der Dokumentation

Seit der letzten Version dieser Dokumentation wurden folgende Aktualisierungen vorgenommen:

- Neue und geänderte Funktionen in Service Pack 12.1.02 - In diesem Kapitel werden die vereinfachte Agentenverwaltung, die Verwendung von CA Enterprise Log Manager als virtuelle Appliance, rollenbasierte Zugriffssteuerung bei API-Anmeldeaufrufen und die Aufbewahrung von Berichtskonfigurationen beschrieben. Außerdem sind Protokollsensor-Handbücher für die einzelnen Protokollsensoren enthalten.
- Die nachfolgenden bekannten Probleme wurden beseitigt, da sie entweder gelöst wurden oder für diese Aktualisierung nicht mehr gelten:
  - Die Genauigkeit der Statuszeit des Agenten ist von der NTP-Server-Konfiguration abhängig
  - Nach Massenbereitstellung von Connectors Zeit für Aktualisierung ermöglichen
  - Keine Leerzeichen bei Name für DVD-Einbindung zulässig
  - Das Aktivieren von SSL-Kommunikation verursacht ODBC-/JDBC-Verzögerungen
  - Integrationen mit Dateiprotokollsensoren 4.0.0.0 unterstützen SUSE Linux nicht
  - Leistungsverminderung bei zu vielen ausgewählten Integrationen
  - Keine Garantie für Syslog-Übermittlung über UDP
  - Syslog-Services bei UNIX-Konflikt
  - WMI-Protokollsensor generiert mehrere Benutzerberechtigungsereignisse
  - Übermäßige Anzahl von ELMAdapter-Protokolldateien
  - Manueller Import von Parsing-Dateien kann eine Änderung des Zeitlimitwerts erforderlich machen
  - Die benutzerdefinierte Datenzuordnung kann keine epSIM-Ereignisse (iTech) zuordnen
  - Ergebnisse von Aktionsalarmabfragen können unvollständig sein
  - Einschränkung von Abfragen bei mehreren Suchbegriffen
  - Keine Statusanzeige des geplanten Jobs nach Upgrade

- Gewisse Aktionsalarmjobs schlagen fehl, wenn Sie zu häufig geplant werden
- Fehler wegen ungenügenden Speicherplatzes bei Rechnern mit geringer Speicherkapazität
- Sperrung des Domänenkontos aufgrund von geänderten Proxy-Anmeldeinformationen
- Die Module für automatische Software-Updates müssen nach dem Upgrade neu ausgewählt werden
- Nach einer Konfigurationsänderung gibt "Proxy testen" eine falsche Erfolgsmeldung zurück.
- Fehler bei der Anwendung von zwei Unterdrückungsregeln
- Upgrade auf r12.1 macht einen Neustart von iGateway erforderlich
- Ein Upgrade auf r12.1 SP1 kann einen Neustart von iGateway erforderlich machen
- Ein aktualisierter Syslog-Protokollsensor unter r12.1 SP1 macht eine Aktualisierung zu Integrationen auf Windows-Agenten erforderlich
- Zugriffsbeschränkungen von einem Browser unter Windows Vista
- Aufrufe von API-Abfragen und -Berichten schlagen unter bestimmten Browsern fehl
- CAELM4Audit wird nicht mehr unterstützt

Weitere Informationen:

Aktualisieren mit automatischen Software-Updates (siehe Seite 11)
Neue und geänderte Funktionen in r12.1 SP1 (siehe Seite 39)
FIPS 140-2-Kompatibilität - Übersicht (siehe Seite 39)
Betriebsarten (siehe Seite 40)
Verschlüsselungsbibliotheken (siehe Seite 41)
Verwendete Algorithmen (siehe Seite 41)
Info zu Zertifikaten und Schlüsseldateien (siehe Seite 42)
Beschränkungen in der Unterstützung von FIPS (siehe Seite 44)
Konfigurieren von Microsoft Internet Explorer, um in FIPS-Modus auf CA Enterprise Log Manager zuzugreifen (siehe Seite 46)
Konfigurieren von Mozilla Firefox, um in FIPS-Modus auf CA Enterprise Log Manager zuzugreifen (siehe Seite 46)

Inhalt

Kapitel 1: Willkommen 11

Aktualisieren mit automatischen Software-Updates 11

Kapitel 2: Betriebsumgebung 15

Hardware- und Softwarevoraussetzungen 15
Erforderliche Energieeinstellungen für bestimmte HP- und IBM-Computer 17
Bildschirmauflösung 17
CA EEM-Serverreferenzen 18

Kapitel 3: Leistungsmerkmale 19

Protokollerfassung 20
Protokollspeicherung 23
Standarddarstellung von Protokollen 25
Konformitätsberichte 26
Alarm bei Verletzung von Richtlinien 28
Rollenbasierter Zugriff 29
Verwalten Von Automatischen-Software-aktualisieren 30
Unterstützung für IPv6-IP-Adressen 32

Kapitel 4: Neue und geänderte Funktionen in r12.1 35

Offener API-Zugriff 35
Ausführbare Alarme: CA IT PAM-Integration 36
Ausführbare Alarme: SNMP-Integration mit NSM-Produkten 36
ODBC- und JDBC-Zugriff 37
Relevanz von Identität und Asset: CA IT PAM-Integration 37
Erweiterte direkte Protokollerfassung durch den Standardagenten 38
Zeitplan für automatische Updates für Clients für automatische Software-Updates 38

Kapitel 5: Neue und geänderte Funktionen in r12.1 SP1 39

FIPS 140-2-Kompatibilität - Übersicht 39
Betriebsarten 40
Verschlüsselungsbibliotheken 41
    Verwendete Algorithmen 41

Info zu Zertifikaten und Schlüsseldateien 42
Beschränkungen in der Unterstützung von FIPS 44
Konfigurieren von Microsoft Internet Explorer, um in FIPS-Modus auf CA Enterprise Log Manager zuzugreifen 46
Konfigurieren von Mozilla Firefox, um in FIPS-Modus auf CA Enterprise Log Manager zuzugreifen 46
ISO-Image für Neuinstallationen 48

Kapitel 6: Neue und geänderte Funktionen in r12.1 SP2 49

CA Enterprise Log Manager als virtuelle Appliance 49
Vereinfachte Agentenverwaltung 49
Rollenbasierte Zugriffssteuerung bei API-Anmeldeaufrufen 50
Protokollsensor-Hilfsdateien 50
Beibehalten einer Berichtskonfiguration 50

Kapitel 7: Bekannte Probleme 51

Agenten und CA-Adapter 51
Abhängigkeiten bei der Agenteninstallation auf Red Hat Linux 4 51
Massenbereitstellung von Connectors mit IPv6-Adresse funktioniert nicht richtig 52
Ereignisquellenkonfiguration auf Domänenebene schlägt fehl 53
Einschränkung bei der Konfiguration von Ports 54
Kein Löschen des Standardagenten bei Entfernen des Servers aus einem Verbund 54
Berichte mit Daten, die vom CA SAPI Collector erfasst wurden, zeigen Ereignisse nicht ordnungsgemäß an 54
Der auf einem Solaris-Agentensystem ausgeführte Textdatei-Protokollsensor beendet den Empfang von Ereignissen 55
Sehr hoher Ereignisstrom führt dazu, dass der Agent nicht reagiert 56
Für einen Agenten gelöschte Connectors werden weiterhin auf der Benutzeroberfläche angezeigt 57
AIX-, HP-UX- und Solaris-Agenten werden nicht bereitgestellt 57
Anwendung (nicht Benutzeroberfläche) 57
Anmeldung beim CA Enterprise Log Manager Server mit EiamAdmin-Benutzernamen nicht möglich 58
Ereignisverfeinerung 58
Verschiedene Operatoren für Blockzuordnungen für Zeichenfolgenwerte und numerische Werte erforderlich 58
Abfragen und Berichte 59
Fehler beim einfachen Filter von Abfrageassistenten bei Sonderzeichen 59
Kennungen, die Sonderzeichen enthalten, können nicht gelöscht werden 59

Abfrageergebnis enthält beschädigte Werte 60
Abfrage- und Berichtsseiten zeigen Fehlermeldungen beim Laden der Benutzeroberfläche Fehlermeldungen an 60
Automatisches Software-Update 60
Automatischer Neustart nach Aktualisierung des Betriebssystems während SP-Upgrade 61
Fehler wegen ungenügenden Speicherplatzes bei Rechnern mit geringer Speicherkapazität 61
Selbstüberwachendes Ereignis zur Neustartaufforderung wird nur einmal angezeigt 62
Benutzer- und Zugriffsverwaltung 63
Einschränkung bei der Verwendung des Kalenders mit Zugriffsrichtlinien 63
Sonstiges 63
Ausbleibende Reaktionen von CA Enterprise Log Manager 63
Auswirkung von benutzerdefinierten Anwendungsnamen auf die Archivabfrage 64
Hohe Kontrasteinstellungen des Bildschirms 65
Fortlaufendes Beenden und Neustarten von iGateway 65
Maximaler Speicherplatz für virtuellen CA Enterprise Log Manager ist zu klein 66
Benutzer werden beim Aktualisieren des Browsers von CA Enterprise Log Manager abgemeldet 67
Nach dem Neustart von iGateway können auf der Dienst- oder der Explorer-Benutzeroberfläche Fehler auftreten 67
Uploads und Importe funktionieren ausschließlich mit Internet Explorer. 68
Die Benutzeroberfläche wird nach der Installation mit Remote EEM unerwarteterweise nicht richtig angezeigt. 69
Upgrade auf CA Audit erforderlich für die Interaktion mit CA Enterprise Log Manager 70

Kapitel 8: Behobene Probleme 71

Problemliste 72

Kapitel 9: Dokumentation 75

Bookshelf 75
Zugriff auf das Bookshelf 76

Anhang A: Vereinbarung gegenüber Drittparteien 77

Adaptive Communication Environment (ACE) 5.5.10 78
Software unter der Apache-Lizenz 81
Boost 1.39.0 85
DataDirect OpenAccess 6.0 86
JDOM 1.0 87
Red Hat Enterprise Linux 5.5 89

SNMP4J 1.9.3d 93
Sun JDK 1.6.0_7 97
PCRE 6.3 103
zlib 1.2.3 105
ZThread 2.3.2 106

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 61)

Kapitel 2: Betriebsumgebung

Dieses Kapitel enthält folgende Themen:

Hardware- und Softwarevoraussetzungen (siehe Seite 15)
Erforderliche Energieeinstellungen für bestimmte HP- und IBM-Computer (siehe Seite 17)
Bildschirmauflösung (siehe Seite 17)
CA EEM-Serverreferenzen (siehe Seite 18)

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/worldwide.

Kapitel 3: Leistungsmerkmale

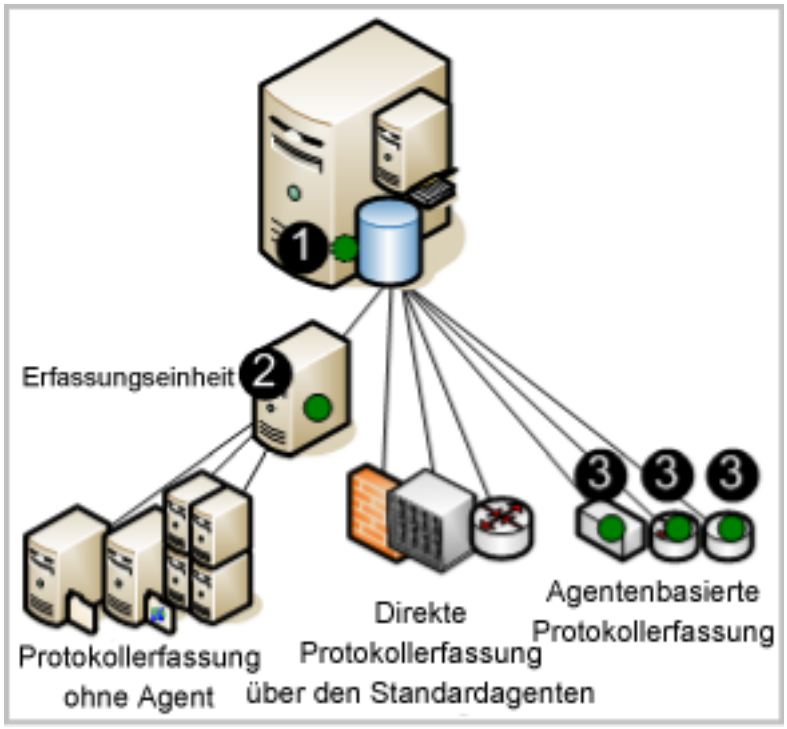
Dieses Kapitel enthält folgende Themen:

Protokollerfassung (siehe Seite 20)
Protokollspeicherung (siehe Seite 23)
Standarddarstellung von Protokollen (siehe Seite 25)
Konformitätsberichte (siehe Seite 26)
Alarm bei Verletzung von Richtlinien (siehe Seite 28)
Rollenbasierter Zugriff (siehe Seite 29)
Verwalten Von Automatischen-Software-aktualisieren (siehe Seite 30)
Unterstützung für IPv6-IP-Adressen (siehe Seite 32)

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

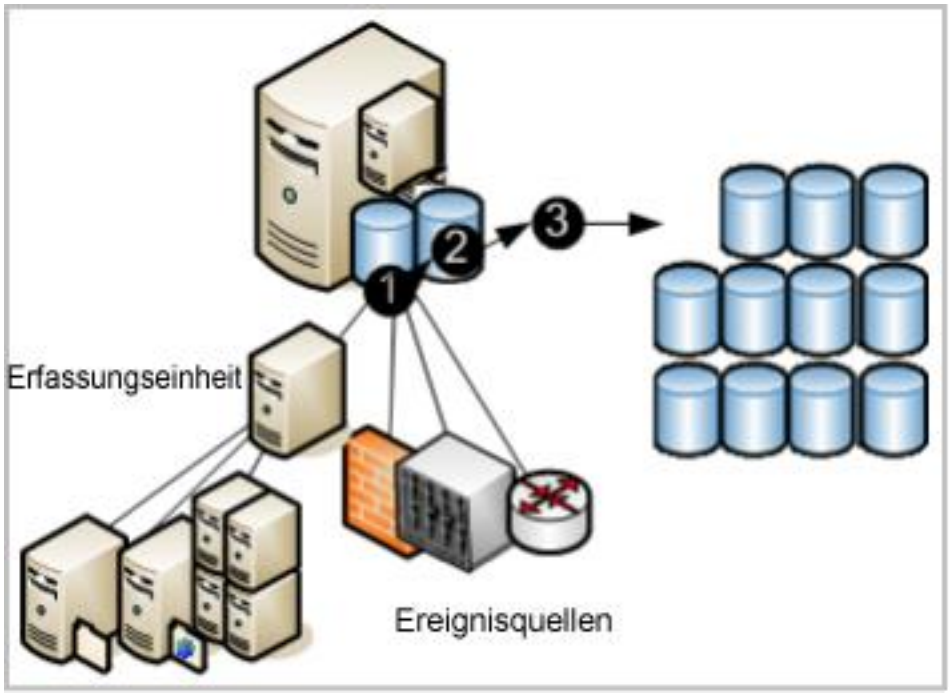
  Bei der agentbasierten Erfassung wird ein Agent überall dort installiert, wo ein oder mehrere Ereignisquellen ausgeführt werden und ein Connector für jede Ereignisquelle konfiguriert wurde.

  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.

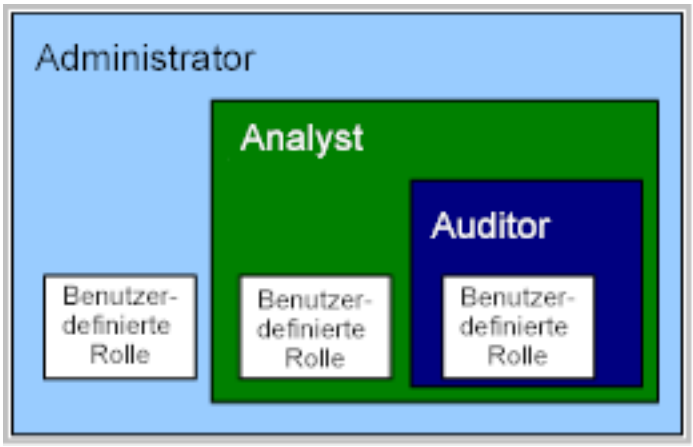
Hinweis: Einzelheiten zu Aktionsalarmen finden Sie im *CA Enterprise Log Manager-Administrationshandbuch*.

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.



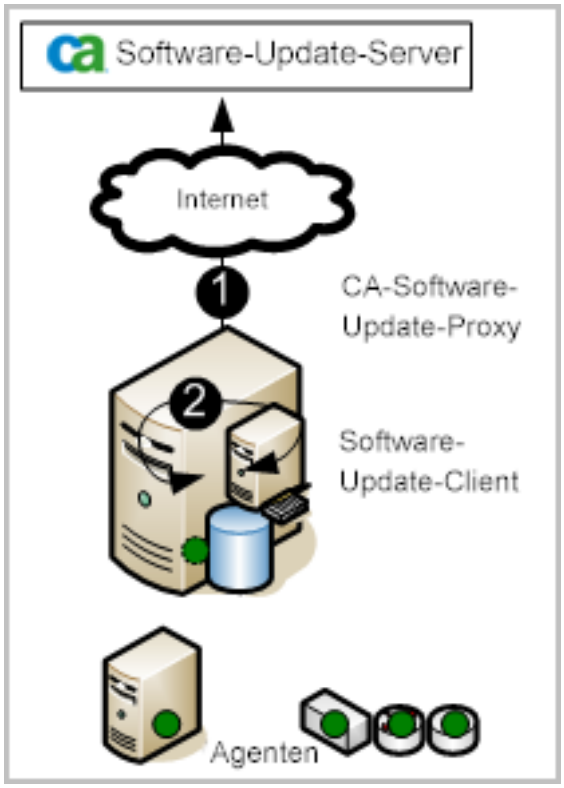
Administratoren können den Zugriff auf jede Ressource anpassen, indem sie eine benutzerdefinierte Anwendungsgruppe mit entsprechenden Richtlinien erstellen und diese Anwendungsgruppe oder Rolle bestimmten Benutzerkonten zuweisen.

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 (siehe Seite 35)
Ausführbare Alarme: CA IT PAM-Integration (siehe Seite 36)
Ausführbare Alarme: SNMP-Integration mit NSM-Produkten (siehe Seite 36)
ODBC- und JDBC-Zugriff (siehe Seite 37)
Relevanz von Identität und Asset: CA IT PAM-Integration (siehe Seite 37)
Erweiterte direkte Protokollerfassung durch den Standardagenten (siehe Seite 38)
Zeitplan für automatische Updates für Clients für automatische Software-Updates (siehe Seite 38)

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 (siehe Seite 39)
Betriebsarten (siehe Seite 40)
Verschlüsselungsbibliotheken (siehe Seite 41)
Info zu Zertifikaten und Schlüsseldateien (siehe Seite 42)
Beschränkungen in der Unterstützung von FIPS (siehe Seite 44)
Konfigurieren von Microsoft Internet Explorer, um in FIPS-Modus auf CA Enterprise Log Manager zuzugreifen (siehe Seite 46)
Konfigurieren von Mozilla Firefox, um in FIPS-Modus auf CA Enterprise Log Manager zuzugreifen (siehe Seite 46)
ISO-Image für Neuinstallationen (siehe Seite 48)

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 40)
Verschlüsselungsbibliotheken (siehe Seite 41)
Verwendete Algorithmen (siehe Seite 41)
Info zu Zertifikaten und Schlüsseldateien (siehe Seite 42)
Beschränkungen in der Unterstützung von FIPS (siehe Seite 44)
Konfigurieren von Microsoft Internet Explorer, um in FIPS-Modus auf CA Enterprise Log Manager zuzugreifen (siehe Seite 46)
Konfigurieren von Mozilla Firefox, um in FIPS-Modus auf CA Enterprise Log Manager zuzugreifen (siehe Seite 46)

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/Schlüsseldateiname	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.
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.

Zertifikats/Schlüsseldateiname	Verzeichnis	Beschreibung
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: Neue und geänderte Funktionen in r12.1 SP2

Dieses Kapitel enthält folgende Themen:

CA Enterprise Log Manager als virtuelle Appliance (siehe Seite 49)
Vereinfachte Agentenverwaltung (siehe Seite 49)
Rollenbasierte Zugriffssteuerung bei API-Anmeldeaufrufen (siehe Seite 50)
Protokollsensor-Hilfsdateien (siehe Seite 50)
Beibehalten einer Berichtskonfiguration (siehe Seite 50)

CA Enterprise Log Manager als virtuelle Appliance

Sie können CA Enterprise Log Manager als virtuelle Appliance im Open Virtualization Format (OVF) bereitstellen. Die Bereitstellung der virtuellen Appliance benötigt weniger Zeit als die Bereitstellung eines CA Enterprise Log Manager-Servers auf einem virtuellen Rechner.

OVF ist ein offener Standard für das Packen und Bereitstellen virtueller Appliances. CA Enterprise Log Manager verwendet das auf OVF basierte Dateiformat Virtual Machine Disk (VMDK).

Informationen zum Bereitstellen von CA Enterprise Log Manager als virtuelle Appliance finden Sie im *Implementierungshandbuch.*

Vereinfachte Agentenverwaltung

Diese aktualisierte Funktion vereinfacht die Bereitstellung neuer CA Enterprise Log Manager-Server. Diese Funktion bietet folgende Möglichkeiten:

- Aktualisieren Sie eine Liste von CA Enterprise Log Manager-Servern auf der Ebene des Agenten-Explorer oder einer einzelnen Agentengruppe.
- Wenn Sie zu einer vorhandenen Serverliste einen neuen Server hinzufügen Sie, aktualisiert CA Enterprise Log Manager die Serverliste in jedem Agenten.

Zusätzliche Informationen zur vereinfachten Agentenverwaltung finden Sie im *Administrationshandbuch* und in der *Online-Hilfe*.

Rollenbasierte Zugriffssteuerung bei API-Anmeldeaufrufen

Sie können rollenbasierte Zugriffssteuerung für bei CA Enterprise Log Manager angemeldete Benutzer über API ausführen. Sie können die Datenzugriffsfilter, die auf die Abfrage angewendet werden, im XML-Format festlegen. Sie können mit dieser Spezifikation z. B. eine Abfrage oder ein Berichtsergebnis entsprechend Ihrer Rolle filtern, wenn Sie sich mit Zertifikatsnamen und Zertifikatskennwort authentifizieren.

Informationen zum Zugriffsfilter-XML finden Sie im *API-Programmierhandbuch.*

Protokollsensor-Hilfsdateien

Mit dieser Version wird für jeden Protokollsensor ein Protokollsensorhandbuch zur Verfügung gestellt. Sie können über den Integrationsassistenten der Benutzeroberfläche auf die Protokollsensorhandbücher zugreifen.

Beibehalten einer Berichtskonfiguration

Sie können die Konfiguration eines Berichts beibehalten, indem Sie im Integrationsassistenten die Option "Nach Ablauf beibehalten" aktivieren. Nachdem der Bericht generiert wurde, können Sie die Berichtskonfiguration ändern und den Bericht neu planen. Diese Funktion besteht sowohl für einmalige als auch sofort auszuführende Berichte.

Zusätzliche Informationen zur vereinfachten Agentenverwaltung finden Sie im *Administrationshandbuch* und in der *Online-Hilfe*.

Kapitel 7: Bekannte Probleme

Dieses Kapitel enthält folgende Themen:

Agenten und CA-Adapter (siehe Seite 51)
Anwendung (nicht Benutzeroberfläche) (siehe Seite 57)
Ereignisverfeinerung (siehe Seite 58)
Abfragen und Berichte (siehe Seite 59)
Automatisches Software-Update (siehe Seite 60)
Benutzer- und Zugriffsverwaltung (siehe Seite 63)
Sonstiges (siehe Seite 63)

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.

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.

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

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.

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".

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.

Für einen Agenten gelöschte Connectors werden weiterhin auf der Benutzeroberfläche angezeigt

Symptom:

Gelöschte Connectors von Agenten, die per Remote-Zugriff mit einem CA Enterprise Log Manager-Server kommunizieren, auf dem CA EEM-Server installiert ist, werden weiterhin auf der Benutzeroberfläche des CA Enterprise Log Manager-Servers angezeigt.

Lösung:

Beim Aktualisieren der Konfiguration eines Agenten benötigt CA Enterprise Log Manager maximal 5 Minuten, um den aktualisierten Status dieses Agenten mit den anderen Agenten in einer Föderation zu synchronisieren. Überprüfen Sie den Status eines gelöschten Connectors nach 5 Minuten.

AIX-, HP-UX- und Solaris-Agenten werden nicht bereitgestellt

Symptom:

Wenn Sie CA Enterprise Log Manager r12.1 SP2 mit einem ISO-Image oder einer virtuellen Appliance installieren, werden AIX-, HP-UX- und Solaris-Agentenpakete nicht bereitgestellt.

Lösung:

Verwenden Sie nach Abschluss der Installation das System für automatische Software-Updates, um die benötigten Agentenpakete herunterzuladen.

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*.

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.

Abfragen und Berichte

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

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.

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.

Abfrageergebnis enthält beschädigte Werte

Symptom:

Wenn Sie für eine Spalte eine andere SQL-Funktion als TRIM, TOLOWER, TOUPPER oder eine Gruppenreihenfolgeneinstellung auswählen, und für andere Spalten nicht dieselbe Einstellung vornehmen, enthält das Abfrageergebnis beschädigte Werte.

Lösung:

Wenn Sie für eine Spalte eine andere SQL-Funktion als TRIM, TOLOWER, TOUPPER oder eine Gruppenreihenfolgeneinstellung auswählen, müssen Sie für die restlichen Spalten dieselbe Einstellung vornehmen.

Abfrage- und Berichtsseiten zeigen Fehlermeldungen beim Laden der Benutzeroberfläche Fehlermeldungen an

Symptom:

Wenn ein CA Enterprise Log Manager-Server die Abfragen- und Berichtsseiten lädt, wird auf der Benutzeroberfläche folgender Fehler angezeigt:

```
Error getting query/report results: HTTP request error
```

Lösung:

Dieser Fehler tritt auf, wenn für Erfassungs- und Berichtsserver, die CA Enterprise Log Manager als virtuelle Appliance benutzen, eine mittlere Konfiguration verwendet wurde. Bei einem Hub-and-Spoke-Modell wird nachdrücklich empfohlen, für Erfassungsserver eine mittlere und für Berichtsserver eine große Bereitstellungskonfiguration zu verwenden.

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.

Lösung:

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".

Wichtig! Das Einstellen der JVM-Heapgröße kann bei der Verwendung der Option "In PDF-Datei exportieren" bei großen Datensätzen Probleme verursachen. Diese Option sollte demnach nur auf kleinen Computern verwendet werden, die mit weniger RAM und Prozessor-Leistung als empfohlen betrieben werden.

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.

Benutzer- und Zugriffsverwaltung

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

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
   ```

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".

Upgrade auf CA Audit erforderlich für die Interaktion mit CA Enterprise Log Manager

Symptom:

Bei der Installation eines CA Enterprise Log Manager-Servers wird ein vorhandener CA Embedded Entitlements Manager-Server, der mit CA Audit r8 SP2 installiert wurde, verwendet. Beim Zugriff auf die Audit-Administrator-Benutzeroberfläche wird bei dem Versuch, Agentendetails zu bearbeiten, die folgende Fehlermeldung zurückgegeben:

```
"Warnung: Es sind keine Protokollmanager-Server verfügbar."
```

Alle Felder in der Seite "Agentendetails bearbeiten" des Audit-Administrators sind leer.

Die Ursache ist eine inkompatible Interaktion zwischen dem r8.1-CA EEM-Server und dem r8.4-CA EEM-Client, der in CA Enterprise Log Manager r12.1 vorliegt. Die ältere Version unterstützt eine Funktion nicht, die vom neueren SDK aufgerufen wird.

Lösung:

Sie können das Übereinstimmungsproblem zwischen den beiden Versionen lösen und CA Enterprise Log Manager mit CA Audit r8 SP2 verwenden, indem Sie die vorhandene CA Audit-Implementierung auf CA Audit r8 SP2 CR1 aktualisieren. Danach können Sie die Funktionen CA Enterprise Log Manager-Agent und -Agentenmanager mit CA Audit verwenden.

Kapitel 8: Behobene Probleme

Dieses Kapitel enthält folgende Themen:

Problemliste (siehe Seite 72)

Problemliste

Folgende Erweiterungsanfragen wurden in CA Enterprise Log Manager r12.1 SP2 eingearbeitet:

- 18853365-1
- 18853310-1
- 18699660-1
- 18713453-1
- 19079108-1
- 19046629-1
- 19078906-1
- 18853408-1

Folgende von Kunden berichteten Probleme wurden in CA Enterprise Log Manager r12.1 SP2 behoben:

- 19201526-1
- 19078767-2
- 19222906
- 19179699-1
- 19266092-1
- 19313624-1
- 19379354
- 19399295
- 19454801
- 19468531
- 19188433-7
- 19581946
- 19602784
- 19173006-1
- 18977697-1
- 19188433-4
- 19255064-1

- 19188433-3
- 19222992
- 19236219
- 19188433-5
- 19378391-1
- 19280900-1
- 19289970-1
- 19297282-1
- 19370519
- 19373496
- 19467808
- 19428046
- 19459527
- 19543395
- 19539006-1

Kapitel 9: Dokumentation

Dieses Kapitel enthält folgende Themen:

Bookshelf (siehe Seite 75)
Zugriff auf das Bookshelf (siehe Seite 76)

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) 5.5.10 (siehe Seite 78)
Software unter der Apache-Lizenz (siehe Seite 81)
Boost 1.39.0 (siehe Seite 85)
DataDirect OpenAccess 6.0 (siehe Seite 86)
JDOM 1.0 (siehe Seite 87)
Red Hat Enterprise Linux 5.5 (siehe Seite 89)
SNMP4J 1.9.3d (siehe Seite 93)
Sun JDK 1.6.0_7 (siehe Seite 97)
PCRE 6.3 (siehe Seite 103)
zlib 1.2.3 (siehe Seite 105)
ZThread 2.3.2 (siehe Seite 106)

Adaptive Communication Environment (ACE) 5.5.10

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

ACE(TM), TAO(TM), CIAO(TM), and CoSMIC(TM) (henceforth referred to as "DOC software") are copyrighted by Douglas C. Schmidt and his research group at Washington University, University of California, Irvine, and Vanderbilt University, Copyright (c) 1993-2008, all rights reserved. Since DOC software is open-source, freely available software, you are free to use, modify, copy, and distribute--perpetually and irrevocably--the DOC software 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 any code built using DOC software that you release. No copyright statement needs to be provided if you just ship binary executables of your software products.

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

The ACE, TAO, CIAO, and CoSMIC web sites are maintained by the DOC Group at the Institute for Software Integrated Systems (ISIS) and the Center for Distributed Object Computing of Washington University, St. Louis for the development of open-source software as part of the open-source software community. Submissions are provided by the submitter ``as is|&"&| with no warranties whatsoever, including any warranty of merchantability, noninfringement of third party intellectual property, or fitness for any particular purpose. In no event shall the submitter be liable for any direct, indirect, special, exemplary, punitive, or consequential damages, including without limitation, lost profits, even if advised of the possibility of such damages. Likewise, DOC software is 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. 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 DOC software 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.

DOC software is 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 around the world provide commercial support for DOC software, however.

DOC software is Y2K-compliant, as long as the underlying OS platform is Y2K-compliant. Likewise, DOC software is compliant with the new US daylight savings rule passed by Congress as "The Energy Policy Act of 2005," which established new daylight savings times (DST) rules for the United States that expand DST as of March 2007. Since DOC software obtains time/date and calendaring information from operating systems users will not be affected by the new DST rules as long as they upgrade their operating systems accordingly.

The names ACE(TM), TAO(TM), CIAO(TM), CoSMIC(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. This license grants no permission to call products or services derived from this source ACE(TM), TAO(TM), CIAO(TM), or CoSMIC(TM), nor does it grant permission for the name Washington University, UC Irvine, or Vanderbilt University to appear in their names.

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
- Qpid 0.5.0
- 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 1.39.0

Dieses Produkt enthält Boost v.1.39.0, welches in Übereinstimmung mit der nachfolgenden Lizenzvereinbarung vertrieben wird:

Boost Software License - Version 1.0 - August 17th, 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.

DataDirect OpenAccess 6.0

Das lizenzierte Programm enthält die Technologie OpenAccess ODBC von Progress Software Corporation ("Progress"), für die Folgendes gilt: In no event will Progress or its suppliers be liable for any damages including direct, special, consequential, and indirect damages.

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.

Red Hat Enterprise Linux 5.5

Dieses CA-Produkt wird mit Red Hat Enterprise Linux Version 5.5 ("Red-Hat-Software"), dessen Verwendung von den folgenden Bedingungen geregelt wird:

Red Hat Software ist eine Open Source-Software, die mit diesem CA-Softwareprogramm ("CA-Produkt") verwendet wird. Die Red Hat-Software wird nicht von CA, Inc ("CA") besessen. Für die Verwendung, Kopie, Verbreitung und Änderung der Red Hat-Software gelten das End User License Agreement Red Hat Enterprise Linux and Red Hat Applications ("Red Hat-Lizenz") sowie Lizenzverträge, auf die sich dieses bezieht, einschließlich der General Public License Version 2 ("GPL"). Eine Kopie der GPL-Lizenz befindet sich in einem Verzeichnis innerhalb der Red Hat-Software. Die LGPL-Lizenz steht auch hier zur Verfügung: http://www.gnu.org/licenses/gpl-2.0.html. Oder schreiben Sie an: Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA. Die Bedingungen des Red Hat-Lizenzvertrags werden weiter unten aufgeführt. CA stellt den Quellcode der Red Hat Software unter http://opensrcd.ca.com/ips/04237_5/ zur Verfügung. Die Verwendung des CA-Produkts unterliegt ausschließlich dem CA-Endbenutzer-Lizenzvertrag ("EULA") und nicht der Red Hat- oder GPL-Lizenz. Sofern nicht dezidiert anders im EULA festgelegt, dürfen Sie CA-Produktcode nicht verwenden, ändern oder weitergeben. Die Red Hat-Software wird IN DER VORLIEGENDEN FORM ZUR VERFÜGUNG GESTELLT. JEGLICHE AUSDRÜCKLICHE ODER STILLSCHWEIGENDE GARANTIE, EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF, DIE GARANTIE FÜR DIE VERMARKTBARKEIT UND DIE EIGNUNG FÜR EINEN BESTIMMTEN ZWECK WERDEN AUSGESCHLOSSEN. Weitere Details des Haftungsausschlusses hinsichtlich der Red Hat-Software finden Sie in der Red Hat-Lizenz und direkt in der GPL-Lizenz. Innerhalb der Grenzen des anwendbaren Rechts lehnt CA jegliche Gewährleistung und Haftung in Zusammenhang mit der Verwendung der Red Hat-Software ab.

LICENSE AGREEMENT

RED HAT® ENTERPRISE LINUX®

AND RED HATÂ® APPLICATIONS

This end user license agreement ("EULA") governs the use of any of the versions of Red Hat Enterprise Linux, any Red Hat Applications (as set forth at www.redhat.com/licenses/products), and any related updates, source code, appearance, structure and organization (the "Programs"), regardless of the delivery mechanism.

1. License Grant. Subject to the following terms, Red Hat, Inc. ("Red Hat") grants to you ("User") a perpetual, worldwide license to the Programs pursuant to the GNU General Public License v.2. The Programs are either a modular operating system or an application consisting of hundreds of software components. With the exception of certain image files identified in Section 2 below, the license agreement for each software component is located in the software component's source code and permits User to run, copy, modify, and redistribute (subject to certain obligations in some cases) the software component, in both source code and binary code forms. This EULA pertains solely to the Programs and does not limit User's rights under, or grant User rights that supersede, the license terms of any particular component.

2. Intellectual Property Rights. The Programs and each of their components are owned by Red Hat and others and are protected under copyright law and under other laws as applicable. Title to the Programs and any component, or to any copy, modification, or merged portion shall remain with the aforementioned, subject to the applicable license. The "Red Hat" trademark and the "Shadowman" logo are registered trademarks of Red Hat in the U.S. and other countries. This EULA does not permit User to distribute the Programs or their components using Red Hat's trademarks, regardless of whether the copy has been modified. User should read the information found at http://www.redhat.com/about/corporate/trademark/ before distributing a copy of the Programs. User may make a commercial redistribution of the Programs only if, (a) a separate agreement with Red Hat authorizing such commercial redistribution is executed or other written permission is granted by Red Hat or (b) User modifies any files identified as "REDHAT-LOGOS" to remove and replace all images containing the "Red Hat" trademark or the "Shadowman" logo. Merely deleting these files may corrupt the Programs.

3. Limited Warranty. Except as specifically stated in this Section 3, a separate agreement with Red Hat, or a license for a particular component, to the maximum extent permitted under applicable law, the Programs and the components are provided and licensed "as is" without warranty of any kind, expressed or implied, including the implied warranties of merchantability, non-infringement or fitness for a particular purpose. Red Hat warrants that the media on which the Programs and the components are furnished will be free from defects in materials and manufacture under normal use for a period of 30 days from the date of delivery to User. Red Hat does not warrant that the functions contained in the Programs will meet User's requirements or that the operation of the Programs will be entirely error free, appear precisely as described in the accompanying documentation, or comply with regulatory requirements. This warranty extends only to the party that purchases services pertaining to the Programs from Red Hat or a Red Hat authorized distributor.

4. Limitation of Remedies and Liability. To the maximum extent permitted by applicable law, User's exclusive remedy under this EULA is to return any defective media within 30 days of delivery along with a copy of User's payment receipt and Red Hat, at its option, will replace it or refund the money paid by User for the media. To the maximum extent permitted under applicable law, neither Red Hat, any Red Hat authorized distributor, nor the licensor of any component provided to User under this EULA will be liable to User for any incidental or consequential damages, including lost profits or lost savings arising out of the use or inability to use the Programs or any component, even if Red Hat, such authorized distributor or licensor has been advised of the possibility of such damages. In no event shall Red Hat's liability, an authorized distributor's liability or the liability of the licensor of a component provided to User under this EULA exceed the amount that User paid to Red Hat under this EULA during the twelve months preceding the action.

5. Export Control. As required by the laws of the United States and other countries, User represents and warrants that it: (a) understands that the Programs and their components may be subject to export controls under the U.S. Commerce Department's Export Administration Regulations ("EAR"); (b) is not located in a prohibited destination country under the EAR or U.S. sanctions regulations (currently Cuba, Iran, Iraq, North Korea, Sudan and Syria, subject to change as posted by the United States government); (c) will not export, re-export, or transfer the Programs to any prohibited destination or persons or entities on the U.S. Bureau of Industry and Security Denied Parties List or Entity List, or the U.S. Office of Foreign Assets Control list of Specially Designated Nationals and Blocked Persons, or any similar lists maintained by other countries, without the necessary export license(s) or authorizations(s); (d) will not use or transfer the Programs for use in connection with any nuclear, chemical or biological weapons, missile technology, or military end-uses where prohibited by an applicable arms embargo, unless authorized by the relevant government agency by regulation or specific license; (e) understands and agrees that if it is in the United States and exports or transfers the Programs to eligible end users, it will, to the extent required by EAR Section 740.17(e), submit semi-annual reports to the Commerce Department's Bureau of Industry and Security, which include the name and address (including country) of each transferee; and (f) understands that countries including the United States may restrict the import, use, or export of encryption products (which may include the Programs and the components) and agrees that it shall be solely responsible for compliance with any such import, use, or export restrictions.

6. Third Party Programs. Red Hat may distribute third party software programs with the Programs that are not part of the Programs. These third party programs are not required to run the Programs, are provided as a convenience to User, and are subject to their own license terms. The license terms either accompany the third party software programs or can be viewed at http://www.redhat.com/licenses/thirdparty/eula.html. If User does not agree to abide by the applicable license terms for the third party software programs, then User may not install them. If User wishes to install the third party software programs on more than one system or transfer the third party software programs to another party, then User must contact the licensor of the applicable third party software programs.

7. General. If any provision of this agreement is held to be unenforceable, that shall not affect the enforceability of the remaining provisions. This agreement shall be governed by the laws of the State of New York and of the United States, without regard to any conflict of laws provisions. The rights and obligations of the parties to this EULA shall not be governed by the United Nations Convention on the International Sale of Goods.

SNMP4J 1.9.3d

Dieses Produkt enthält SNMP4J 1.9.3d und wird in Übereinstimmung mit folgender Lizenzvereinbarung vertrieben:

Apache License

Version 2.0, January 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

Sun JDK 1.6.0_7

Dieses Produkt wird mit Sun JDK 1.6.0_7 (JAVA SE DEVELOPMENT KIT (JDK), VERSION 6) (Sun JDK) vertrieben. Sun JDK wurde und in Übereinstimmung mit dem nachstehenden Sun Microsystems, Inc. (Sun) Binary Code License Agreement vertrieben. Wie in in dieser Lizenz in Abschnitt G von Supplemental License vermerkt, legt Sun in der mit dem Sun JDK mitgelieferten Datei "THIRDPARTYLICENSEREADME.txt" zusätzliche Copyright-Hinweise und Lizenzbedingungen vor, die auf Teile des Sun JDK anwendbar sein können.

Sun Microsystems, Inc. Binary Code License Agreement for the JAVA SE DEVELOPMENT KIT (JDK), VERSION 6

SUN MICROSYSTEMS, INC. ("SUN") IS WILLING TO LICENSE THE SOFTWARE IDENTIFIED BELOW TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS BINARY CODE LICENSE AGREEMENT AND SUPPLEMENTAL LICENSE TERMS (COLLECTIVELY "AGREEMENT"). PLEASE READ THE AGREEMENT CAREFULLY. BY DOWNLOADING OR INSTALLING THIS SOFTWARE, YOU ACCEPT THE TERMS OF THE AGREEMENT. INDICATE ACCEPTANCE BY SELECTING THE "ACCEPT" BUTTON AT THE BOTTOM OF THE AGREEMENT. IF YOU ARE NOT WILLING TO BE BOUND BY ALL THE TERMS, SELECT THE "DECLINE" BUTTON AT THE BOTTOM OF THE AGREEMENT AND THE DOWNLOAD OR INSTALL PROCESS WILL NOT CONTINUE.

1. DEFINITIONS. "Software" means the identified above in binary form, any other machine readable materials (including, but not limited to, libraries, source files, header files, and data files), any updates or error corrections provided by Sun, and any user manuals, programming guides and other documentation provided to you by Sun under this Agreement. "General Purpose Desktop Computers and Servers" means computers, including desktop, laptop and tablet computers, or servers, used for general computing functions under end user control (such as but not specifically limited to email, general purpose Internet browsing, and office suite productivity tools).

The use of Software in systems and solutions that provide dedicated functionality (other than as mentioned above) or designed for use in embedded or function-specific software applications, for example but not limited to: Software embedded in or bundled with industrial control systems, wireless mobile telephones, wireless handheld devices, kiosks, TV/STB, Blu-ray Disc devices, telematics and network control switching equipment, printers and storage management systems, and other related systems are excluded from this definition and not licensed under this Agreement. "Programs" means Java technology applets and applications intended to run on the Java Platform Standard Edition (Java SE) platform on Java-enabled General Purpose Desktop Computers and Servers.

2. LICENSE TO USE. Subject to the terms and conditions of this Agreement, including, but not limited to the Java Technology Restrictions of the Supplemental License Terms, Sun grants you a non-exclusive, non-transferable, limited license without license fees to reproduce and use internally Software complete and unmodified for the sole purpose of running Programs. Additional licenses for developers and/or publishers are granted in the Supplemental License Terms.

3. RESTRICTIONS. Software is confidential and copyrighted. Title to Software and all associated intellectual property rights is retained by Sun and/or its licensors. Unless enforcement is prohibited by applicable law, you may not modify, decompile, or reverse engineer Software. You acknowledge that Licensed Software is not designed or intended for use in the design, construction, operation or maintenance of any nuclear facility. Sun Microsystems, Inc. disclaims any express or implied warranty of fitness for such uses. No right, title or interest in or to any trademark, service mark, logo or trade name of Sun or its licensors is granted under this Agreement. Additional restrictions for developers and/or publishers licenses are set forth in the Supplemental License Terms.

4. LIMITED WARRANTY. Sun warrants to you that for a period of ninety (90) days from the date of purchase, as evidenced by a copy of the receipt, the media on which Software is furnished (if any) will be free of defects in materials and workmanship under normal use. Except for the foregoing, Software is provided "AS IS". Your exclusive remedy and Sun's entire liability under this limited warranty will be at Sun's option to replace Software media or refund the fee paid for Software. Any implied warranties on the Software are limited to 90 days. Some states do not allow limitations on duration of an implied warranty, so the above may not apply to you. This limited warranty gives you specific legal rights. You may have others, which vary from state to state.

5. DISCLAIMER OF WARRANTY. UNLESS SPECIFIED IN THIS AGREEMENT, ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT THESE DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

6. LIMITATION OF LIABILITY. TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT WILL SUN OR ITS LICENSORS BE LIABLE FOR ANY LOST REVENUE, PROFIT OR DATA, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL OR PUNITIVE DAMAGES, HOWEVER CAUSED REGARDLESS OF THE THEORY OF LIABILITY, ARISING OUT OF OR RELATED TO THE USE OF OR INABILITY TO USE SOFTWARE, EVEN IF SUN HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. In no event will Sun's liability to you, whether in contract, tort (including negligence), or otherwise, exceed the amount paid by you for Software under this Agreement. The foregoing limitations will apply even if the above stated warranty fails of its essential purpose. Some states do not allow the exclusion of incidental or consequential damages, so some of the terms above may not be applicable to you.

7. TERMINATION. This Agreement is effective until terminated. You may terminate this Agreement at any time by destroying all copies of Software. This Agreement will terminate immediately without notice from Sun if you fail to comply with any provision of this Agreement. Either party may terminate this Agreement immediately should any Software become, or in either party's opinion be likely to become, the subject of a claim of infringement of any intellectual property right. Upon Termination, you must destroy all copies of Software..

8. EXPORT REGULATIONS. All Software and technical data delivered under this Agreement are subject to US export control laws and may be subject to export or import regulations in other countries. You agree to comply strictly with all such laws and regulations and acknowledge that you have the responsibility to obtain such licenses to export, re-export, or import as may be required after delivery to you.

9. TRADEMARKS AND LOGOS. You acknowledge and agree as between you and Sun that Sun owns the SUN, SOLARIS, JAVA,JINI, FORTE, and iPLANET trademarks and all SUN, SOLARIS, JAVA, JINI, FORTE, and iPLANET-related trademarks, service marks, logos and other brand designations ("Sun Marks"), and you agree to comply with the Sun Trademark and Logo Usage Requirements currently located at http://www.sun.com/policies/trademarks. Any use you make of the Sun Marks inures to Sun's benefit.

10. U.S. GOVERNMENT RESTRICTED RIGHTS. If Software is being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), then the Government's rights in Software and accompanying documentation will be only as set forth in this Agreement; this is in accordance with 48 CFR 227.7201 through 227.7202-4 (for Department of Defense (DOD) acquisitions) and with 48 CFR 2.101 and 12.212 (for non-DOD acquisitions).

11. GOVERNING LAW. Any action related to this Agreement will be governed by California law and controlling U.S. federal law. No choice of law rules of any jurisdiction will apply.

12. SEVERABILITY. If any provision of this Agreement is held to be unenforceable, this Agreement will remain in effect with the provision omitted, unless omission would frustrate the intent of the parties, in which case this Agreement will immediately terminate.

13. INTEGRATION. This Agreement is the entire agreement between you and Sun relating to its subject matter. It supersedes all prior or contemporaneous oral or written communications, proposals, representations and warranties and prevails over any conflicting or additional terms of any quote, order, acknowledgment, or other communication between the parties relating to its subject matter during the term of this Agreement. No modification of this Agreement will be binding, unless in writing and signed by an authorized representative of each party.

SUPPLEMENTAL LICENSE TERMS

These Supplemental License Terms add to or modify the terms of the Binary Code License Agreement. Capitalized terms not defined in these Supplemental Terms shall have the same meanings ascribed to them in the Binary Code License Agreement. These Supplemental Terms shall supersede any inconsistent or conflicting terms in the Binary Code License Agreement, or in any license contained within the Software.

A. Software Internal Use and Development License Grant. Subject to the terms and conditions of this Agreement and restrictions and exceptions set forth in the Software "README" file incorporated herein by reference, including, but not limited to the Java Technology Restrictions of these Supplemental Terms, Sun grants you a non-exclusive, non-transferable, limited license without fees to reproduce internally and use internally the Software complete and unmodified for the purpose of designing, developing, and testing your Programs.

B. License to Distribute Software. Subject to the terms and conditions of this Agreement and restrictions and exceptions set forth in the Software README file, including, but not limited to the Java Technology Restrictions of these Supplemental Terms, Sun grants you a non-exclusive, non-transferable, limited license without fees to reproduce and distribute the Software, provided that (i) you distribute the Software complete and unmodified and only bundled as part of, and for the sole purpose of running, your Programs, (ii) the Programs add significant and primary functionality to the Software, (iii) you do not distribute additional software intended to replace any component(s) of the Software, (iv) you do not remove or alter any proprietary legends or notices contained in the Software, (v) you only distribute the Software subject to a license agreement that protects Sun's interests consistent with the terms contained in this Agreement, and (vi) you agree to defend and indemnify Sun and its licensors from and against any damages, costs, liabilities, settlement amounts and/or expenses (including attorneys' fees) incurred in connection with any claim, lawsuit or action by any third party that arises or results from the use or distribution of any and all Programs and/or Software.

C. License to Distribute Redistributables. Subject to the terms and conditions of this Agreement and restrictions and exceptions set forth in the Software README file, including but not limited to the Java Technology Restrictions of these Supplemental Terms, Sun grants you a non-exclusive, non-transferable, limited license without fees to reproduce and distribute those files specifically identified as redistributable in the software "README" file ("Redistributables") provided that: (i) you distribute the Redistributables complete and unmodified, and only bundled as part of Programs, (ii) the Programs add significant and primary functionality to the Redistributables, (iii) you do not distribute additional software intended to supersede any component(s) of the Redistributables (unless otherwise specified in the applicable README file), (iv) you do not remove or alter any proprietary legends or notices contained in or on the Redistributables, (v) you only distribute the Redistributables pursuant to a license agreement that protects Sun's interests consistent with the terms contained in the Agreement, (vi) you agree to defend and indemnify Sun and its licensors from and against any damages, costs, liabilities, settlement amounts and/or expenses (including attorneys' fees) incurred in connection with any claim, lawsuit or action by any third party that arises or results from the use or distribution of any and all Programs and/or Software.

D. Java Technology Restrictions. You may not create, modify, or change the behavior of, or authorize your licensees to create, modify, or change the behavior of, classes, interfaces, or subpackages that are in any way identified as "java", "javax", "sun" or similar convention as specified by Sun in any naming convention designation.

E. Distribution by Publishers. This section pertains to your distribution of the Software with your printed book or magazine (as those terms are commonly used in the industry) relating to Java technology ("Publication"). Subject to and conditioned upon your compliance with the restrictions and obligations contained in the Agreement, in addition to the license granted in Paragraph 1 above, Sun hereby grants to you a non-exclusive, nontransferable limited right to reproduce complete and unmodified copies of the Software on electronic media (the "Media") for the sole purpose of inclusion and distribution with your Publication(s), subject to the following terms: (i) You may not distribute the Software on a stand-alone basis; it must be distributed with your Publication(s); (ii) You are responsible for downloading the Software from the applicable Sun web site; (iii) You must refer to the Software as JavaTM SE Development Kit 6; (iv) The Software must be reproduced in its entirety and without any modification whatsoever (including, without limitation, the Binary Code License and Supplemental License Terms accompanying the Software and proprietary rights notices contained in the Software); (v) The Media label shall include the following information: Copyright 2006, Sun Microsystems, Inc. All rights reserved. Use is subject to license terms. Sun, Sun Microsystems, the Sun logo, Solaris, Java, the Java Coffee Cup logo, J2SE, and all trademarks and logos based on Java are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries. to only apply to the Sun Software; (vi) You must clearly identify the Software as Sun's product on the Media holder or Media label, and you may not state or imply that Sun is responsible for any third-party software contained on the Media; (vii) You may not include any third party software on the Media which is intended to be a replacement or substitute for the Software; (viii) You shall indemnify Sun for all damages arising from your failure to comply with the requirements of this Agreement. In addition, you shall defend, at your expense, any and all claims brought against Sun by third parties, and shall pay all damages awarded by a court of competent jurisdiction, or such settlement amount negotiated by you, arising out of or in connection with your use, reproduction or distribution of the Software and/or the Publication. Your obligation to provide indemnification under this section shall arise provided that Sun: (a) provides you prompt notice of the claim; (b) gives you sole control of the defense and settlement of the claim; (c) provides you, at your expense, with all available information, assistance and authority to defend; and (d) has not compromised or settled such claim without your prior written consent; and (ix) You shall provide Sun with a written notice for each Publication; such notice shall include the following information: (1) title of Publication, (2) author(s), (3) date of Publication, and (4) ISBN or ISSN numbers. Such notice shall be sent to Sun Microsystems, Inc., 4150 Network Circle, M/S USCA12-110, Santa Clara, California 95054, U.S.A , Attention: Contracts Administration.

F. Source Code. Software may contain source code that, unless expressly licensed for other purposes, is provided solely for reference purposes pursuant to the terms of this Agreement. Source code may not be redistributed unless expressly provided for in this Agreement.

G. Third Party Code. Additional copyright notices and license terms applicable to portions of the Software are set forth in the THIRDPARTYLICENSEREADME.txt file. In addition to any terms and conditions of any third party opensource/freeware license identified in the THIRDPARTYLICENSEREADME.txt file, the disclaimer of warranty and limitation of liability provisions in paragraphs 5 and 6 of the Binary Code License Agreement shall apply to all Software in this distribution.

H. Termination for Infringement. Either party may terminate this Agreement immediately should any Software become, or in either party's opinion be likely to become, the subject of a claim of infringement of any intellectual property right.

I. Installation and Auto-Update. The Software's installation and auto-update processes transmit a limited amount of data to Sun (or its service provider) about those specific processes to help Sun understand and optimize them. Sun does not associate the data with personally identifiable information. You can find more information about the data Sun collects at http://java.com/data/.

For inquiries please contact: Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A.

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.

THE BASIC LIBRARY FUNCTIONS

Written by: Philip Hazel

Email local part: ph10

Email domain: cam.ac.uk

University of Cambridge Computing Service,

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

THE C++ WRAPPER FUNCTIONS

Contributed by: Google Inc.

THE "BSD" LICENCE

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.

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.