CA User Activity Reporting Module

Übersichtshandbuch

Version 12.5.03

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:

- Überblick über den Schnellstart: Dieses bereits vorhandene Thema ist aktualisiert worden und nimmt nun über Syslogs hinaus Bezug auf weitere Ereignistypen, die vom Standardagenten auf dem CA User Activity Reporting Module-Server erfasst werden können.
- Alarme zu Richtlinienverletzungen: Dieses bereits vorhandene Thema ist aktualisiert worden und nimmt nun Bezug auf die Möglichkeit, Alarme als SNMP-Traps an Netzwerk-Sicherheitsüberwachungssysteme zu senden und einen IT PAM Ereignis-/Alarmausgabeprozess, z. B. zur Erstellung eines Help-Desk-Tickets, auszuführen.
- Bookshelf: Dieses bereits vorhandene Thema ist aktualisiert worden und nimmt Bezug auf das neue API-Programmierungshandbuch, das nun im CA User Activity Reporting Module-Bookshelf zur Verfügung steht.

Weitere Informationen

Überblick über den Schnellstart (siehe Seite 13)
Alarm bei Verletzung von Richtlinien (siehe Seite 60)
Überblick über das Bookshelf mit Dokumentation (siehe Seite 72)

Inhalt

Kapitel 1: Einführung

Dieses Kapitel enthält folgende Themen:

Über dieses Handbuch

Dieses *Übersichtshandbuch* bietet eine Einführung in CA User Activity Reporting Module. Es beginnt mit kurzen Lernprogrammen, die sofort eine praktische Einführung in das Produkt ermöglichen. Das erste Lernprogramm befasst sich mit der Einrichtung und Aktivierung eines Single-Server CA Enterprise Log Managers und dem Anzeigen von Syslogs, die von einem UNIX-Gerät in unmittelbarer Netzwerknähe erfasst wurden. Das zweite Lernprogramm gibt eine Einführung in die Installation eines Agents auf einem Windows-Betriebssystem, die Konfiguration der Protokollerfassung und die Anzeige daraus resultierender Ereignisprotokolle. Anschließend beschreibt es die Hauptfunktionen und gibt Hinweise zu weiteren Informationen. Dieses Handbuch richtet sich an alle Benutzer.

Zusammenfassung des Inhalts:

Abschnitt	Inhalt
Info zu CA Enterprise Log Manager	Integration von CA User Activity Reporting Module in Ihre aktuelle Netzwerkumgebung
Schnellstartbereitstellung	Installation eines Single-Server-Systems, Konfiguration von Syslog-Ereignisquellen, Update des Syslog-Connectors für den Standardagent und Anzeigen von verfeinerten Ereignissen
Bereitstellung von Windows-Agents	Vorbereiten der Agentinstallation, Installation eines Agents für das Windows-Betriebssystem, Konfiguration eines Connectors für die agentbasierte Erfassung, Aktualisieren der Ereignisquelle und Anzeigen generierter Ereignisse
Hauptfunktionen	Wichtige Funktionen nutzen, darunter die Protokollerfassung, die Protokollspeicherung, Konformitätsberichte und Alarme
Weitere Informationen zu CA User Activity Reporting Module	Weitere Informationen über Kurzinfos, die Online-Hilfe und das Dokumentations-Bookshelf

Hinweis: Weitere Informationen zu unterstützten Betriebssystemen oder zu den Systemanforderungen finden Sie in den *Versionshinweisen*. Schrittweise Anleitungen für die Installation von CA User Activity Reporting Module und die erste Konfiguration finden Sie im *Implementierungshandbuch.* Weitere Informationen zum Installieren eines Agents finden Sie im *Agent-Installationshandbuch*. Weitere Informationen zum Verwenden und Verwalten des Produkts finden Sie im *Verwaltungshandbuch.* Hilfe zum Verwenden einer CA User Activity Reporting Module-Seite finden Sie in der Online-Hilfe.

Info

Ziel von CA User Activity Reporting Module ist die IT-Konformität und -Sicherung. Es werden Informationen zur IT-Aktivität erfasst, standardisiert und aggregiert und entsprechende Berichte erstellt. Außerdem werden Alarme ausgegeben, wenn aufgrund einer möglichen Konformitätsverletzung Handlungsbedarf entsteht. Sie können Daten von unterschiedlichen sicherheits- und nicht sicherheitsbezogenen Geräten sammeln.

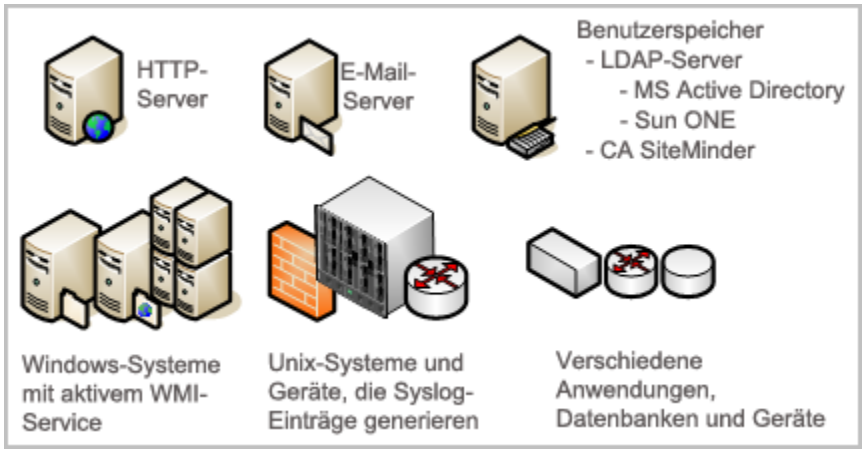
Ihr Netzwerk vor der Installation

Lokale Bestimmungen und Richtlinien schreiben die Aufbewahrung von Protokolldatensätzen vor. Zur Erfüllung dieser Vorgaben müssen Sie:

- Protokolle für Auditing-Zwecke verfügbar machen
- Protokolle über Jahre hinweg speichern
- Protokolle auf Anforderung wiederherstellen

Erschwerend für die Verwaltung von Protokolldatensätzen sind ihre große Anzahl, ihr Speicherort und ihre temporäre Natur. Protokolle werden durch Benutzer- und Prozessaktivitäten in der Software ständig generiert. Die Generierungsrate wird in Ereignissen pro Sekunde (EPS) gemessen. Für jedes aktive System, jede aktive Datenbank und jede aktive Anwendung in Ihrem Netzwerk werden Rohereignisse erfasst. An jeder Ereignisquelle müssen Ereignisprotokolle für die Speicherung gesichert werden, bevor sie überschrieben werden. Die Wiederherstellung von Ereignisprotokollen gestaltet sich schwierig, wenn Sicherungen aus anderen Ereignisquellen separat gespeichert werden.

Die Auswertung von Rohereignissen wird durch das Zeichenfolgenformat erschwert, bei dem der Ereignisschweregrad nicht hervorgehoben ist. Zudem variieren ähnliche Daten aus verschiedenen Systemen.



Ein optimaler Betrieb erfordert eine Lösung, in der sämtliche Protokolle konsolidiert werden, und die dafür sorgt, dass Protokolle gut lesbar sind, dass die Archivierung im Speicher automatisiert ist und die Protokollwiederherstellung vereinfacht wird. CA User Activity Reporting Module bietet diese Vorteile und gibt Ihnen die Möglichkeit, Alarme an Benutzer und Systeme zu senden, wenn kritische Ereignisse eintreten.

Installationsumfang

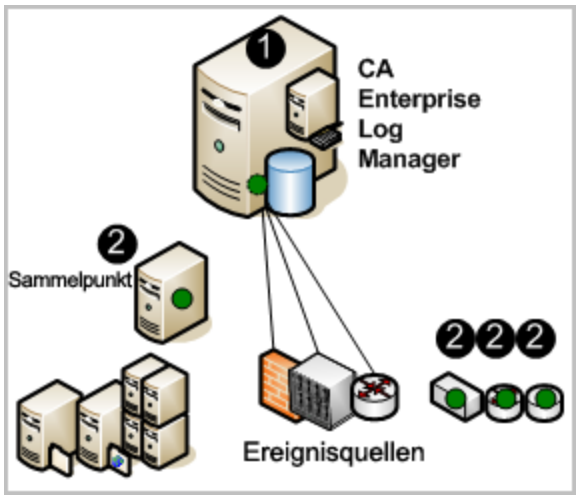
Es nimmt nur wenig Zeit in Anspruch, eine Single-Server-Lösung einzurichten und mit dem Erfassen von Ereignissen zu beginnen.

Die Installationsdatenträger enthalten folgende Komponenten:

- Betriebssystem (Red Hat Enterprise Linux) für die Soft-Appliance
- CA User Activity Reporting Module-Server
- CA User Activity Reporting Module-Agent (in dieser Dokumentation der Agent)

In der folgenden Abbildung ist CA User Activity Reporting Module ein Server, bestehend aus einem kleinen Server, einem dunklen (grünen) Kreis und einer Datenbank. Der kleine Server steht für das lokale Repository, das den Inhalt auf Anwendungsebene speichert. Der dunkle Kreis steht für den Standardagent, und die Datenbank steht für den Ereignisprotokollspeicher, in dem eingehende Ereignisprotokolle verarbeitet und für Abfragen und Berichte verfügbar gemacht werden.

Die dunklen (grünen) Kreise am Sammelpunkt und den anderen Ereignisquellen stehen für separat installierte Agents. Das Installieren von Agents ist optional. Mit dem Standardagent können Sie Syslogs von UNIX-kompatiblen Ereignissen erfassen, nachdem die erforderliche Konfiguration abgeschlossen ist.



Die Nummern in den Abbildungen beziehen sich auf folgende Schritte:

1. Installieren Sie das Betriebssystem für die Soft-Appliance und anschließend die CA User Activity Reporting Module-Anwendung. Sobald Sie die Quellen konfiguriert haben, um Syslogs an CA User Activity Reporting Module auszugeben und die Syslog-Ziele in der Konfiguration des Connectors des Standardagents angegeben haben, werden Syslogs erfasst und zur leichteren Interpretation verfeinert.
2. (Optional) Sie können einen Agent auf einem Host installieren, den Sie als Sammelpunkt bestimmt haben, oder Sie können Agents direkt auf den Hosts mit Quellen, zu erfassende Ereignisse generieren, installieren.

Hinweis: Weitere Informationen zum Installieren der Soft-Appliance finden Sie im *Implementierungshandbuch*. Weitere Informationen zum Installieren von Agents finden Sie im *Agent-Installationshandbuch*.

Weitere Informationen:

Installieren eines Agents (siehe Seite 39)

Kapitel 2: Schnellstartbereitstellung

Dieses Kapitel enthält folgende Themen:

Überblick über den Schnellstart

Sie können eine einfache, funktionsfähige CA User Activity Reporting Module-Bereitstellung mit einer Soft-Appliance erstellen. Mit Hilfe des vordefinierten Syslog-Connectors kann der Standardagent generierte Syslog-Ereignisse empfangen. Sie müssen lediglich Ihre Syslog-Quellen konfigurieren, um Syslog-Ereignisse an CA User Activity Reporting Module weiterzugeben, und die Syslog-Connector-Konfiguration bearbeiten, so dass die Syslog-Ziele erkannt werden. Die Bandbreite zwischen dem Server und den Syslog-Quellen sowie die Latenz bestimmen, was empfangen wird.

Protokollsensoren, einschließlich WinRM und ODBC, unterstützen die direkte Protokollerfassung von über zwanzig Nicht-Syslog-Ereignisquellen. Der WinRM-Protokollsensor ermöglicht die direkte Ereigniserfassung von Servern, auf denen Windows-Betriebssysteme ausgeführt werden, wie z. B. Forefront Security für Exchange-Server, Forefront Security für SharePoint-Server, Microsoft Office Communication Server und der virtuelle Server Hyper-V, sowie Services wie Active Directory Certificate Services. Der ODBC-Protokollsensor ermöglicht, von Oracle9i- oder SQL Server 2005-Datenbanken generierte Ereignisse zu erfassen. Einzelheiten hierzu finden Sie in der CA Enterprise Log Manager-Produktintegrationsmatrix.

Sie benötigen für die Installation von CA User Activity Reporting Module die EiamAdmin-Anmeldeinformationen. Als EiamAdmin-Superuser konfigurieren Sie ein Administratorkonto, das Sie für die Konfiguration verwenden. Wenn Sie sich mit den Administrator-Anmeldeinformationen anmelden, können Sie überprüfen, ob das Setup funktionsfähig ist, indem Sie die selbstüberwachenden Ereignisse anzeigen.

Installation eines Single-Server-Systems

Ein Single-Server-System ist die einfachste Art, abgefragte Ereignisse anzuzeigen. Stellen Sie sicher, dass Sie ein Gerät wählen, das die minimalen Hardwareanforderungen für eine CA User Activity Reporting Module-Soft-Appliance erfüllt oder übertrifft.

Hinweis: Die zertifizierte Hardwareliste, Informationen zur Unterstützung von Betriebssystemen und zur Systemsoftware sowie Dienstanforderungen finden Sie in den *Versionshinweisen*.

So installieren Sie einen CA User Activity Reporting Module für ein Single-Server-System:

1. Halten Sie die folgenden Informationen bereit:
   - Ein Kennwort, das als Stammkennwort verwendet wird.
   - Hostname für Ihre Anwendung
   - Wenn DHCP nicht verwendet wird, die statische IP-Adresse, Subnet-Maske und Standard-Gateway für Ihre Anwendung
   - Domäne der Anwendung

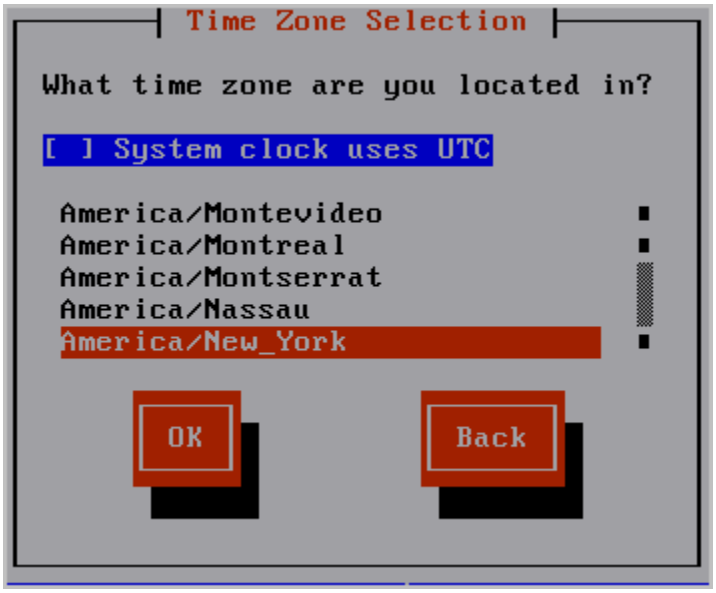
     Hinweis: Die Domäne muss auf den DNS-Servern in Ihrem Netzwerk registriert werden, um die Installation abzuschließen.
   - IP-Adressen der DNS-Server
   - (Optional) IP-Adresse des NTP-Zeitservers
   - Ein Kennwort für den Standard-Superuser-Installationsnamen "EiamAdmin"
   - CAELM.

     Dies ist der Standardanwendungsname für die CA User Activity Reporting Module-Anwendung.

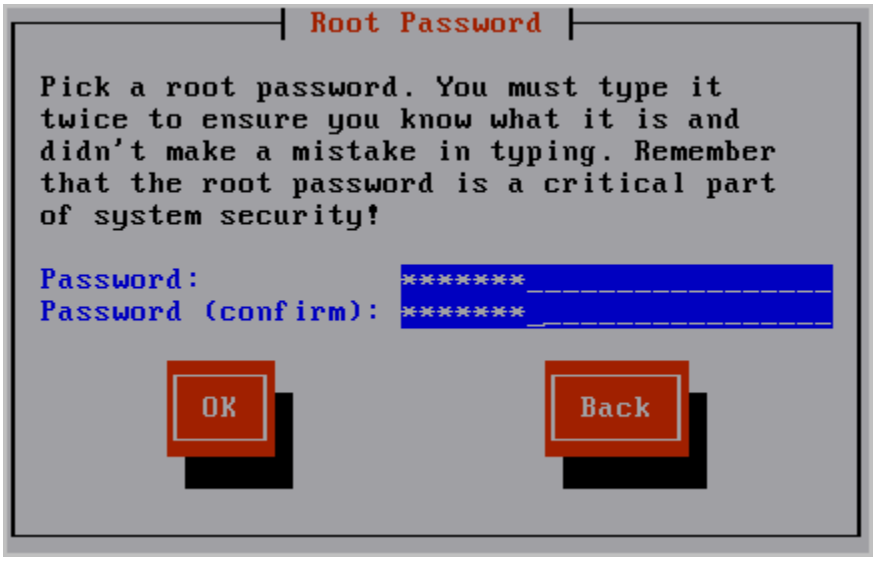
2. Installieren Sie das vorkonfigurierte Betriebssystem über den Datenträger, den Sie aus dem CA User Activity Reporting Module-Downloadpaket erstellt haben. Gehen Sie bei der Installation des Betriebssystems folgendermaßen vor:

   a. Wählen Sie einen Tastaturtyp aus. Der Standard ist USA.

   b. Wählen Sie eine Zeitzone (z. B. Amerika/New York), und wählen Sie "OK".



   c. Geben Sie das Kennwort ein, das als Stammkennwort verwendet werden soll. Geben Sie es erneut ein, um es zu bestätigen. Wählen Sie "OK".



Der Installationsfortschritt wird angezeigt.

d. Entnehmen Sie den Installationsdatenträger für das Betriebssystem, und drücken Sie die Eingabetaste, um das System neu zu starten.

Das System wird neu gestartet und wechselt in den nicht interaktiven Startmodus. Es werden Meldungen zum Installationsfortschritt angezeigt. Weitere Informationen zu dieser Installation werden in der folgenden Datei gespeichert: /tmp/pre-install_ca-elm.log.

Die folgende Eingabeaufforderung wird angezeigt:

```
Legen Sie den Datenträger "CA Enterprise Log Manager r12" für die
Anwendungsinstallation ein, und drücken Sie die Eingabetaste.
```

3. Legen Sie den Datenträger der CA User Activity Reporting Module-Anwendung ein. Drücken Sie die Eingabetaste.

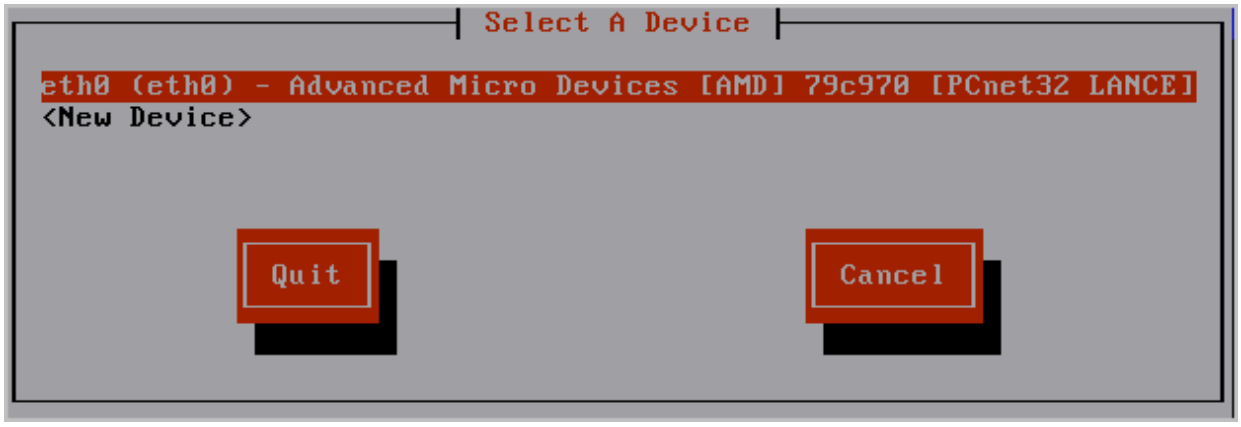
   Es wird überprüft, ob Ihr System die empfohlenen Mindestanforderungen für eine optimale Leistung erfüllt. Ist dies nicht der Fall, wird eine Meldung eingeblendet, in der Sie gefragt werden, ob Sie den Installationsprozess abbrechen möchten.

   Die folgende Eingabeaufforderung wird angezeigt:

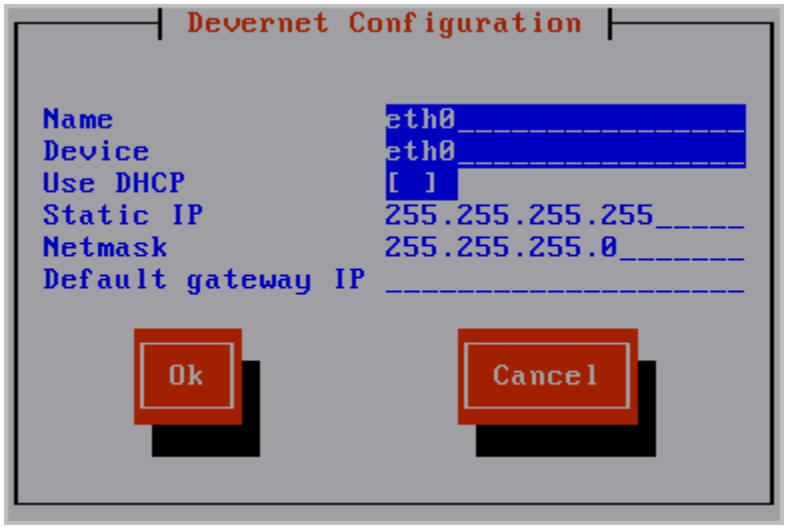
   ```
   Geben Sie einen neuen Hostnamen ein.
   ```

4. Geben Sie den Hostnamen für diese CA User Activity Reporting Module-Soft-Appliance ein. Geben Sie beispielsweise CALM1 ein.

5. Übernehmen Sie das Standardgerät "eth0". Drücken Sie die Eingabetaste, um zum nächsten Bildschirm zu wechseln.



6. Führen Sie einen der folgenden Schritte aus, und wählen Sie dann OK.
   - Wählen Sie "DHCP verwenden". Diese Option wird nur von Standalone-Testsystemen akzeptiert.
   - Geben Sie die statische IP-Adresse, die Subnet-Maske und eine Standard-Gateway-IP-Adresse ein, die mit dem eingegebenen Hostnamen verknüpft werden soll.



Die Netzwerkservices werden mit den neuen, angezeigten Einstellungen neu gestartet.

Die folgende Meldung wird angezeigt:

```
Möchten Sie die Netzwerkkonfiguration ändern? (n):
```

7. Überprüfen Sie die Netzwerkeinstellungen. Wenn Sie zufrieden sind, geben Sie n ein oder drücken Sie die Eingabetaste, wenn die Meldung angezeigt wird, in der Sie die Netzwerkeinstellungen ändern können.

   Die folgende Meldung wird angezeigt:

   ```
   Geben Sie den Domänennamen für dieses System ein:
   ```

8. Geben Sie Ihren Domänennamen ein, z. B. <ihrunternehmen>.com.

   Die folgende Meldung wird angezeigt:

   ```
   Geben Sie eine kommagetrennte Liste mit DNS-Servern ein, die verwendet werden können:
   ```

9. Geben Sie die IP-Adressen Ihrer internen DNS-Server ein. Sie müssen durch Kommas ohne Leerzeichen voneinander getrennt sein.

   Systemdatum und -zeit werden in der folgenden Meldung angezeigt:

   ```
   Möchten Sie Systemdatum und -zeit ändern? (n)
   ```

10. Überprüfen Sie das angezeigte Systemdatum und die Systemzeit. Wenn Sie zufrieden sind, drücken Sie die Eingabetaste oder geben Sie n ein.

    Die folgende Meldung wird angezeigt:

    ```
    Möchten Sie das System konfigurieren, um die Uhrzeit über NTP zu aktualisieren?
    ```

11. Wenn Sie einen NTP-Server (Network Time Protocol) verwenden, gehen Sie wie folgt vor. Wählen Sie andernfalls "Nein", und fahren Sie mit dem nächsten Schritt fort.

    a. Wählen Sie für diese Meldung "Ja".

       Wenn Sie "Ja" wählen, wird die folgende Meldung angezeigt:

       ```
       Geben Sie den Namen oder die IP-Adresse des NTP-Servers an.
       ```

    b. Geben Sie den Hostnamen oder die IP-Adresse des NTP-Servers ein.

       Es wird eine Bestätigungsmeldung mit dem ungefähren Wortlaut angezeigt: "Ihr System wurde so konfiguriert, dass die Uhrzeit um Mitternacht über den NTP-Server unter <ihrntpserver> aktualisiert wird."

12. Lesen Sie die angegebenen Endbenutzerlizenzverträge (End User License Agreements oder EULAs), und gehen Sie folgendermaßen vor:

    a. Lesen Sie die EULA für das Sun Java Development Kit (JDK).

       Am Ende der EULA wird die folgende Meldung angezeigt:

       ```
       Stimmen Sie den Bestimmungen des oben aufgeführten Lizenzvertrags zu? [Ja oder Nein]
       ```

    b. Geben Sie "Ja" ein, wenn Sie den Bestimmungen des oben aufgeführten Lizenzvertrags zustimmen.

       Die Produktregistrierungsinformationen werden angezeigt, gefolgt von dieser Meldung:

       ```
       Drücken Sie zum Fortfahren die Eingabetaste.
       ```

    c. Drücken Sie die Eingabetaste.

       Die folgenden Meldungen geben an, dass zur Vorbereitung der CA User Activity Reporting Module-Installation die Systemeinstellungen konfiguriert werden. Der CA-Endbenutzer-Lizenzvertrag (EULA) wird angezeigt.

    d. Lesen Sie die CA EULA.

       Am Ende des Lizenzvertrags wird die folgende Meldung angezeigt:

       ```
       Stimmen Sie den Bestimmungen des oben aufgeführten Lizenzvertrags zu? [Ja oder Nein]:
       ```

    e. Geben Sie "Ja" ein, wenn Sie den Bestimmungen des Lizenzvertrags zustimmen.

       Die CA EEM-Serverinformationen werden angezeigt.

13. Befolgen Sie die folgenden Eingabeaufforderungen, um CA EEM zu konfigurieren.

    ```
    Verwenden Sie einen lokalen oder einen Remote-EEM-Server?
    Geben Sie I (lokal) oder r (remote) ein:
    ```

    a. Um ein Standalone-Testsystem zu erstellen, geben Sie l für "lokal" ein.

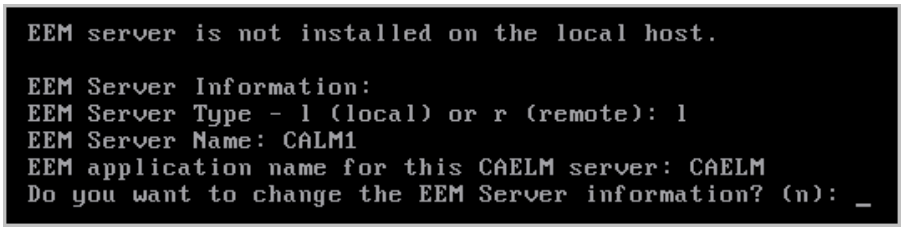
       ```
       Geben Sie das Kennwort für den Benutzer "EiamAdmin" des EEM-Servers ein:
       Bestätigen Sie das Kennwort für den Benutzer "EiamAdmin" des EEM-Servers:
       ```

    b. Geben Sie das Kennwort ein, das Sie dem EiamAdmin-Standard-Superuser zugewiesen haben, und bestätigen Sie es durch erneute Eingabe.

       ```
       Geben Sie einen Anwendungsnamen für diesen CAELM-Server (CAELM) ein:
       ```

c. Drücken Sie die Eingabetaste, um CAELM zu akzeptieren, den Standardanwendungsnamen für CA User Activity Reporting Module.

   Die bisher eingegebenen EEM-Serverinformationen werden mit einer Meldung eingeblendet, in der Sie gefragt werden, ob Sie Änderungen vornehmen möchten.



d. Drücken Sie die Eingabetaste oder geben Sie "n" für "Nein" ein, um die eingegebenen CA EEM-Serverinformationen zu akzeptieren.

Der Installationsvorgang wird gestartet. Die folgenden Meldungen zeigen den erfolgreichen Fortschritt der einzelnen
CA User Activity Reporting Module-Komponenten, den Abschluss der Registrierungen, den Empfang von Zertifikaten, den Import von Dateien und die Konfiguration der Komponenten. Die folgende Meldung bestätigt, dass die CA ELM-Installation erfolgreich abgeschlossen wurde. Nach Abschluss der Installation zeigt das System die Anmeldeadresse der Konsole an.

14. Antworten Sie auf die folgende Eingabeaufforderung:

    ```
    Do you want to run CAELM Server in FIPS mode? [Möchten Sie den CAELM-
    Server im FIPS-Modus starten?]
    Geben Sie "Yes" [Ja] oder "No" [Nein] ein.
    ```

    Wenn Sie "y" eingeben, wird der CA User Activity Reporting Module-Server im FIPS-Modus hochgefahren. Wenn Sie "n" eingeben, wird er im Nicht-FIPS-Modus hochgefahren.

15. Notieren Sie sich diese Adresse. Diese Adresse müssen Sie in einem Browser eingeben, um auf diesen CA User Activity Reporting Module-Server zuzugreifen. Diese lautet https://<hostname>:5250/spin/calm.

    Es wird eine Anmeldeaufforderung für den <hostname> angezeigt. Diese können Sie außer Acht lassen.

    Hinweis: Wenn Sie von dieser Anmeldeaufforderung aus die Eingabeaufforderung des Betriebssystems anzeigen möchten, geben Sie "caelmadmin" und das Standardkennwort ein, d. h. das Kennwort, das Sie dem Benutzerkonto für "EiamAdmin" zugewiesen haben. Mit diesem caelmadmin-Konto können Sie sich bei der Anwendung auf der Konsole oder über SSH anmelden.

16. Fahren Sie wie folgt fort:
    - Wenn Sie eine statische IP-Adresse konfiguriert haben, müssen Sie die IP-Adresse mit den in Schritt 9 festgelegten DNS-Servern registrieren.
    - Wenn Sie DHCP konfiguriert haben, aktualisieren Sie Ihre Hostdatei auf dem Gerät, von dem aus Sie über einen Browser auf diesen Server zugreifen möchten.
    - Gehen Sie zu der URL, die Sie in Schritt 14 notiert haben, und konfigurieren Sie den ersten Administrator.

Aktualisieren der Windows-Hostdatei

Während der Installation von CA User Activity Reporting Module können Sie einen oder mehrere DNS-Server festlegen oder DHCP wählen. Wenn Sie DHCP gewählt haben, müssen Sie Ihre Windows-Hostdatei auf dem Computer aktualisieren, über den Sie mit Ihrem Browser auf CA User Activity Reporting Module zugreifen möchten.

So aktualisieren Sie Ihre Hostdatei auf dem Host mit Ihrem Browser:

1. Öffnen Sie den Windows Explorer, und navigieren Sie zu C:\WINDOWS\system32\drivers\etc.
2. Öffnen Sie die Hostdatei mit einem Editor, z. B. Notepad.
3. Fügen Sie einen Eintrag mit der IP-Adresse des CA User Activity Reporting Module-Servers und den entsprechenden Hostnamen hinzu.
4. Wählen Sie im Menü "Datei" die Option "Speichern", und schließen Sie die Datei anschließend.

Konfigurieren des ersten Administrators

Nach der Installation eines Single-Server-CA User Activity Reporting Module bereiten Sie die Konfiguration vor, indem Sie die URL von CA User Activity Reporting Module von einer Remote-Workstation aus aufrufen, sich anmelden und ein Administratorkonto erstellen, mit dem Sie die Konfiguration vornehmen können.

Hinweis: Für diese Schnellstartbereitstellung werden der Standardbenutzerspeicher und die Standardkennwortrichtlinien akzeptiert. Normalerweise werden diese konfiguriert, bevor der erste Administrator hinzugefügt wird.

So konfigurieren Sie den ersten Administrator:

1. Öffnen Sie in Ihrem Browser die folgende URL, wobei der Hostname entweder aus dem Hostnamen oder der IP-Adresse des Servers besteht, auf dem Sie CA User Activity Reporting Module installiert haben.

   `https://<hostname>:5250/spin/calm`

2. Falls ein Sicherheitsalarm eingeblendet wird, gehen Sie folgendermaßen vor:

   a. Klicken Sie auf "Zertifikat anzeigen".

   b. Klicken Sie auf "Zertifikat installieren", übernehmen Sie die Standardeinstellungen, und schließen Sie den Import-Assistenten ab.

      Es wird eine Sicherheitswarnung eingeblendet, die Sie darauf hinweist, dass Sie ein Zertifikat installieren, das vorgibt, den Hostnamen des CA User Activity Reporting Module-Servers zu repräsentieren.

   c. Klicken Sie auf "Ja".

      Das Stammzertifikat wird installiert, und es wird eine Meldung eingeblendet, dass der Import erfolgreich war.

   d. Klicken Sie auf "OK".

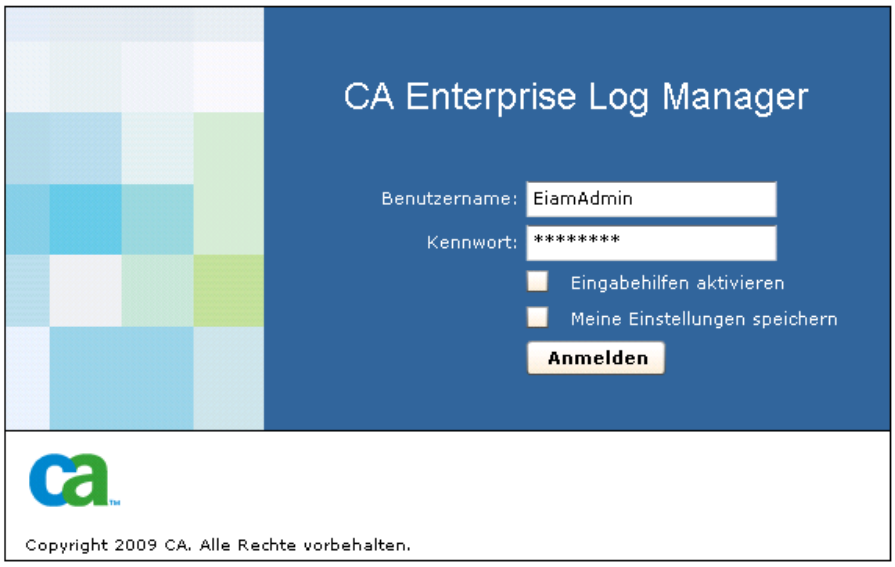
      Das Dialogfeld "Vertrauenswürdige Zertifikate" wird angezeigt.

   e. (Optional) Klicken Sie auf den Pfad des Zertifikats, und stellen Sie sicher, dass der Zertifikatstatus "OK" lautet.

   f. Klicken Sie auf "OK" und anschließend auf "Ja".

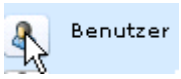
      Die Anmeldeseite wird angezeigt.

3. Melden Sie sich mit dem Benutzernamen "EiamAdmin" und dem Kennwort an, das Sie bei der Installation der Software verwendet haben. Klicken Sie auf "Anmelden".

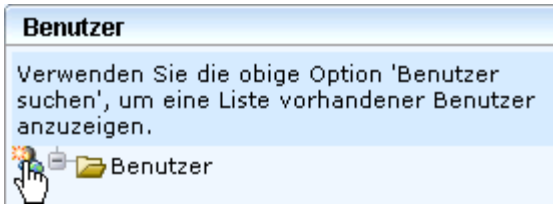


Die Anwendung wird mit der Administrator-Registerkarte und aktiver Unterregisterkarte für die Benutzer- und Zugriffsverwaltung geöffnet.

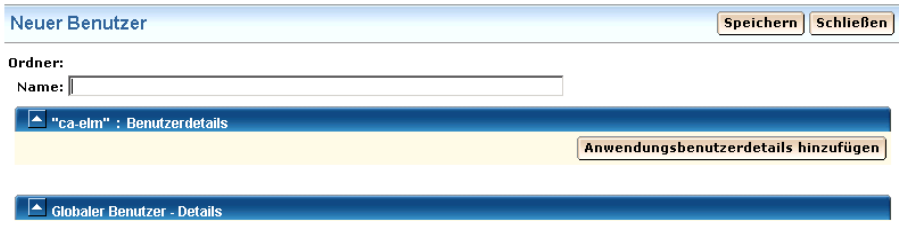
4. Klicken Sie auf "Benutzer".



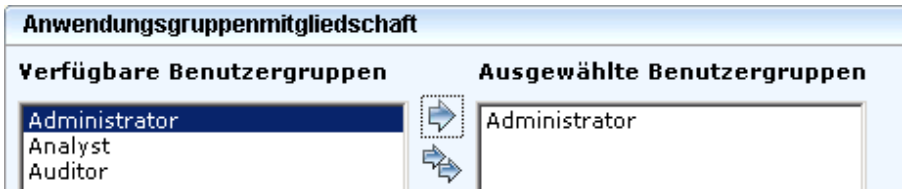
5. Klicken Sie auf "Neuen Benutzer hinzufügen".



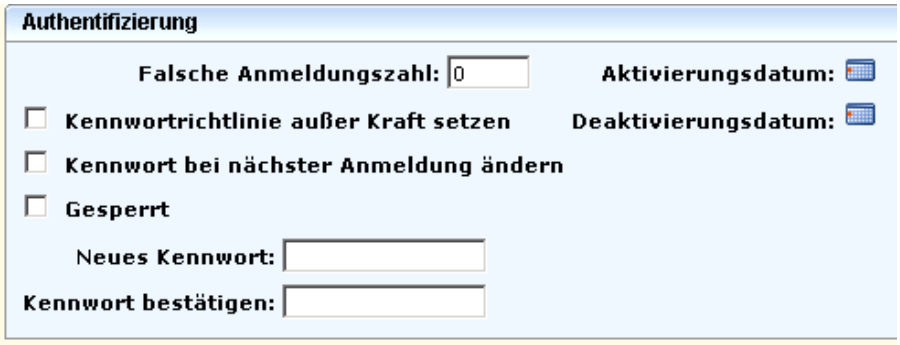
6. Geben Sie Ihren Namen in das Feld "Name" ein, und klicken Sie auf "Anwendungsbenutzerdetails hinzufügen".



7. Wählen Sie "Administrator", und verschieben Sie ihn in die Liste "Ausgewählte Benutzergruppen".



8. Geben Sie unter "Authentifizierung" in den beiden Feldern für Eingabe und Bestätigung ein Kennwort für das neue Konto ein.



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

10. Klicken Sie in der Symbolleiste auf "Abmelden".

    Die Anmeldeseite wird angezeigt.

11. Melden Sie sich mit den gerade definierten Administratoranmeldeinformationen erneut bei CA User Activity Reporting Module an.

    CA User Activity Reporting Module wird geöffnet. Nun stehen alle Funktionen zur Verfügung. Die Registerkarte "Abfragen und Berichte" wird mit der untergeordneten Registerkarte "Abfragen" angezeigt.

12. (Optional) Zeigen Sie Ihre Anmeldeversuche wie folgt an:

    a. Wählen Sie in der Abfragekennungsliste den Eintrag "Systemzugriff".

    b. Wählen Sie in der Abfragekennungsliste den Eintrag "Systemzugriff - Details".

    Das Abfrageergebnis zeigt Ihre beiden Anmeldeversuche an, zuerst als "EiamAdmin", dann mit Ihrem Administratornamen. Beide Anmeldeversuche sind mit S für "Successful" (Erfolgreich) markiert.

CA-Schweregrad	Datum ▼	Konto	Benutzer	Host	Protokoll...	Kategorie	Aktion	Ergebnis
Informationen	Donnerstag, 12. November 2009, 18:29	song11	song11	ca-elm	CALM	System Access	Login Attempt	S
Informationen	Donnerstag, 12. November 2009, 18:23	liuyue	liuyue	ca-elm	CALM	System Access	Login Attempt	S
Informationen	Donnerstag, 12. November 2009, 18:15	miao	miao	ca-elm	CALM	System Access	Login Attempt	S
Informationen	Donnerstag, 12. November 2009, 18:09	admin	admin	ca-elm	CALM	System Access	Login Attempt	S

Konfigurieren von Syslog-Ereignisquellen

Um die direkte Erfassung von Syslog-Ereignissen durch den Standardagent zu ermöglichen, der auf jedem CA User Activity Reporting Module-Server existiert, müssen Sie zunächst die Syslog-Ereignisquellen definieren, über die Sie Ereignisse erfassen möchten, und die damit verbundene Integration festlegen. Anschließend führen Sie die beiden folgenden Schritte in beliebiger Reihenfolge durch:

- Konfigurieren Sie die Syslog-Ereignisquellen. Melden Sie sich bei den Hosts an, auf denen eine Syslog-Ereignisquelle ausgeführt wird, und konfigurieren Sie sie wie im Connector-Handbuch für diese Syslog-Integration beschrieben.
- Konfigurieren Sie den Syslog-Connector auf dem Standardagent, um Ziel-Syslog-Integrationen hinzuzufügen, die mit den konfigurierten Ereignisquellen verknüpft sind.

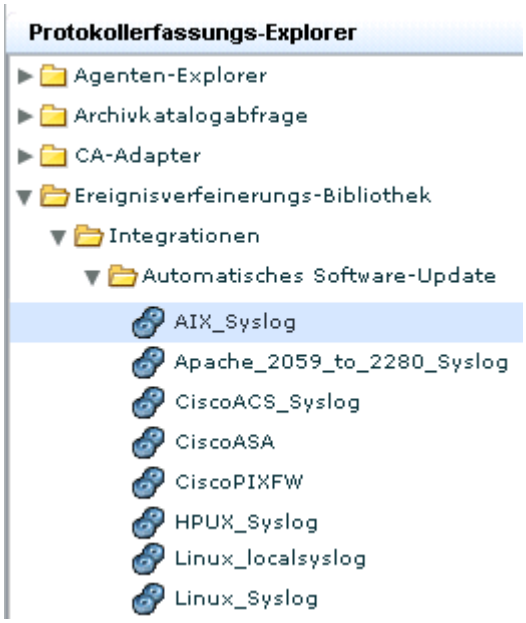
Sobald Sie diese beiden Konfigurationsschritte abgeschlossen haben, beginnt die Erfassung und Verfeinerung der Ereignisse. Dann können Sie CA User Activity Reporting Module verwenden, um im Standardformat für Sie wichtige Ereignisse anzuzeigen oder entsprechende Berichte zu erstellen. Sie können auch Alarme generieren, wenn bestimmte Ereignisse eintreten.

So konfigurieren Sie eine ausgewählte Syslog-Ereignisquelle:

1. Melden Sie sich bei dem Host an, auf dem sich eine Ziel-Syslog-Ereignisquelle befindet.
2. Starten Sie CA User Activity Reporting Module über einen Browser auf diesem Host.
3. Klicken Sie auf die Registerkarte "Verwaltung" und die untergeordnete Registerkarte "Protokollerfassung".

   Der Protokollerfassungs-Explorer wird geöffnet.
4. Erweitern Sie die Punkte "Ereignisverfeinerungs-Bibliothek", "Integrationen" und "Automatische Software-Updates".

   Eine Liste vordefinierter Integrationen wird angezeigt. Eine kurzes Beispiel:



5. Wählen Sie die Integration für die Ereignisquelle, die Sie konfigurieren müssen. Wenn Sie beispielsweise Syslogs erfassen möchten, die von einem AIX-Betriebssystem generiert wurden, müssen Sie "AIX_Syslog" wählen.

   Das Fenster "Integrationsdetails" wird angezeigt.

6. Klicken Sie auf die Schaltfläche "Hilfe" über dem Integrationsnamen im rechten Fensterbereich.

   Das Connector-Handbuch für die ausgewählte Integration wird angezeigt.

7. Klicken Sie auf den Bereich in den Konfigurationsanforderungen der Ereignisquelle. In diesem Beispiel wird beschrieben, wie Sie die Ereignisquelle des AIX-Betriebssystems konfigurieren, damit die Syslogs an CA User Activity Reporting Module gesendet werden.

Beispiel: Alternative Quelle für Connector-Handbücher: Support Online

Sie können ein ausgewähltes Connector-Handbuch über die CA User Activity Reporting Module-Benutzeroberfläche oder über den CA Support Online öffnen. Das folgende Beispiel zeigt, wie Sie ein Connector-Handbuch über die alternative Quelle öffnen.

1. Melden Sie sich bei CA Support Online an.
2. Wählen Sie im Dropdown-Listenfeld "Produkt auswählen" den CA Enterprise Log Manager.
3. Blättern Sie zum Produktstatus, und wählen Sie "CA Enterprise Log Manager Certification Matrix".
4. Wählen Sie die Produktintegrationsmatrix.
5. Suchen Sie die Kategorie für die Integration, die mit der Ereignisquelle verknüpft ist, die Sie konfigurieren. Wenn es sich bei der Ereignisquelle beispielsweise um das AIX-Betriebssystem handelt, gehen Sie zur Kategorie "Betriebssystem", und klicken Sie auf die AIX-Verknüpfung.

Produkt	Version	Log-Sensor
Betriebssysteme		
AIX	5.1 5.2 5.3	syslog

Bearbeiten des Syslog-Connectors

Jeder CA User Activity Reporting Module verfügt über einen Standardagent. Wenn CA User Activity Reporting Module installiert wurde, verfügt der Standardagent über einen teilweise konfigurierten Connector mit Namen "Syslog_Connector", der auf dem Listener "Syslog" basiert. Der Listener empfängt Syslog-Rohereignisse auf den Standard-Ports, sobald Sie die Ereignisquellen konfiguriert haben, die Syslogs an CA User Activity Reporting Module senden sollen. Damit CA User Activity Reporting Module diese Rohereignisse verfeinern kann, müssen Sie diesen Syslog_Connector editieren. Bestimmte Bearbeitungen sind erforderlich, andere sind optional.

- Sie müssen die Syslog-Ziele angeben, wenn Sie diesen Connector bearbeiten. Als Syslog-Ziele wählen Sie jede Integration, die einer oder mehreren Ereignisquellen entspricht, die Sie konfiguriert haben oder konfigurieren möchten. Durch die Angabe der Syslog-Ziele ist CA User Activity Reporting Module in der Lage, Ereignisse korrekt zu verfeinern.
- Optional können Sie Unterdrückungsregeln anwenden, die Akzeptanz von Syslogs für vertrauenswürdige Hosts beschränken, neben 514 (dem bekannten UDP-Port) und 1468 (dem Standard-TCP-Port) noch weitere Ports zum Abhören festlegen und/oder eine neue Zeitzone für einen vertrauenswürdigen Host hinzufügen.

So bearbeiten Sie den Syslog-Connector für einen Standardagent:

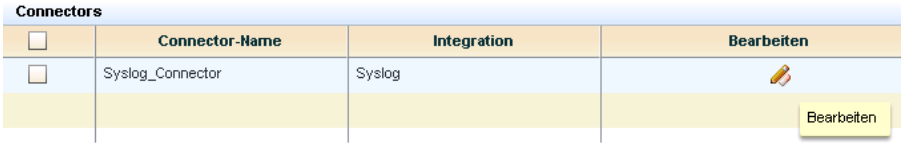
1. Klicken Sie auf die Registerkarte "Verwaltung".

   Die untergeordnete Registerkarte "Protokollerfassung" wird angezeigt.

2. Erweitern Sie den Agent-Explorer und dann die Standard-Agentengruppe oder die benutzerdefinierte Gruppe mit dem zu konfigurierenden CA User Activity Reporting Module.

3. Wählen Sie den Namen eines CA User Activity Reporting Module-Servers.

   Der Connector mit dem Namen Syslog_Connector wird angezeigt.



4. Klicken Sie auf Bearbeiten.

   Der Assistent zum Bearbeiten von Connectors wird geöffnet. Der Schritt "Connector-Details" ist ausgewählt.

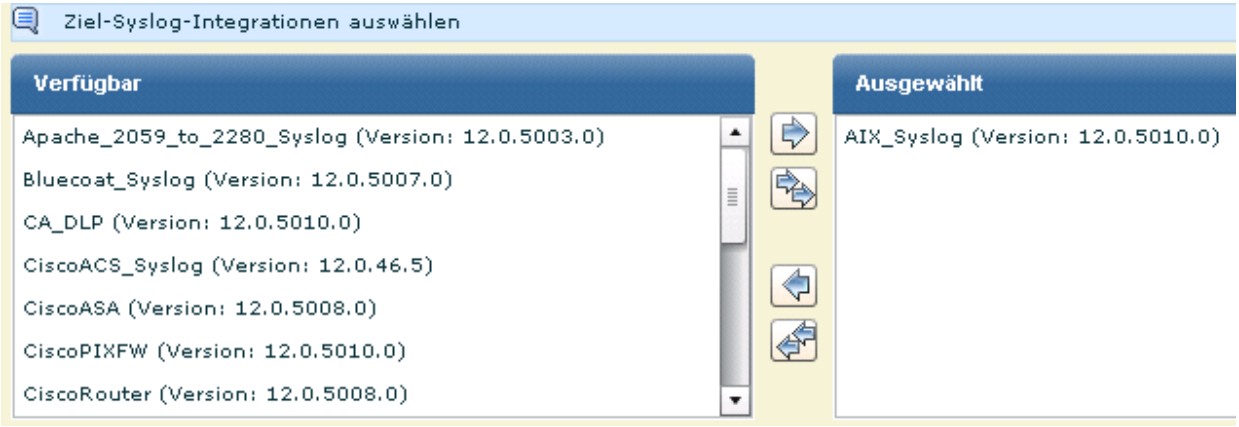
5. (Optional) Klicken Sie auf "Unterdrückungsregeln anwenden". Wenn Sie bestimmte Syslog-Ereignistypen unterdrücken, also *nicht* erfassen möchten, verschieben Sie diesen Ereignistyp von der Liste "Verfügbar" in die Liste "Ausgewählt". Wählen Sie das Ereignis, das Sie verschieben möchten, und klicken Sie auf die Schaltfläche "Verschieben".

6. Klicken Sie auf den Schritt "Connector-Konfiguration".

   Standardmäßig werden alle verfügbaren Integrationen ausgewählt.

7. Wählen Sie Syslog-Ziele, indem Sie die Syslog-Integrationen für Ziele von der Liste "Verfügbar" in die Liste "Ausgewählt" verschieben.

   Wenn Sie beispielsweise das AIX-Betriebssystem auf einem Host in Ihrem Netzwerk konfiguriert haben, sollten Sie das Syslog-Ziel "AIX_Syslog" aus der Liste "Verfügbar" in die Liste "Ausgewählt" verschieben.



8. (Optional) Geben Sie die vertrauenswürdigen Hosts an, von denen der Syslog-Connector eingehende Ereignisse akzeptieren soll. Geben Sie in das Eingabefeld die IP-Adresse ein, und klicken Sie auf "Hinzufügen". Wiederholen Sie dies für alle vertrauenswürdigen Hosts. Wenn dann ein Ereignis von einem Host empfangen wird, der nicht als vertrauenswürdig konfiguriert wurde, wird dieses Ereignis abgelehnt.

   Hinweis: Es ist eine gute Übung, vertrauenswürdige Hosts zu konfigurieren. Normalerweise konfigurieren Sie alle Hosts, auf denen Sie Ereignisse konfiguriert haben, die Syslogs an CA User Activity Reporting Module senden sollen. Durch die Angabe von vertrauenswürdigen Hosts stellen Sie sicher, dass der Standardagent keine Ereignisse von Schurkensystemen akzeptiert, die ein Angreifer konfiguriert hat, um Ereignisse an den Syslog-Listener zu senden.

9. (Optional) Fügen Sie Ports hinzu.

   Sie können typischerweise die Standard-UPD- und TCP-Ports für den Standardagent akzeptieren.

   Hinweis: Sie erreichen Leistungsverbesserungen, indem Sie einen Syslog-Connector für verschiedene Ereignistypen definieren und für jeden einen eigenen Port festlegen. Stellen Sie sicher, dass die Ports nicht verwendet werden, wenn Sie neue Ports zuweisen.

10. (Optional) Fügen Sie nur eine Zeitzone hinzu, wenn Sie Syslogs von Geräten erfassen, deren Zeitzone sich von der Soft-Appliance unterscheidet.

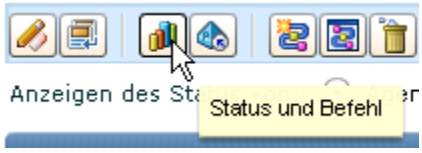
    a. Klicken Sie auf "Ordner erstellen", und erweitern Sie den Ordner.

    b. Markieren Sie den leeren Eintrag unter dem Ordner. Geben Sie die IP-Adresse eines vertrauenswürdigen Hosts ein, den Sie für diesen Connector definiert haben, oder den NTP-Time-Server, den Sie bei der Installation von CA User Activity Reporting Module festgelegt haben.

11. Klicken Sie auf "Speichern" und "Schließen".

12. Zeigen sie den Staus an.

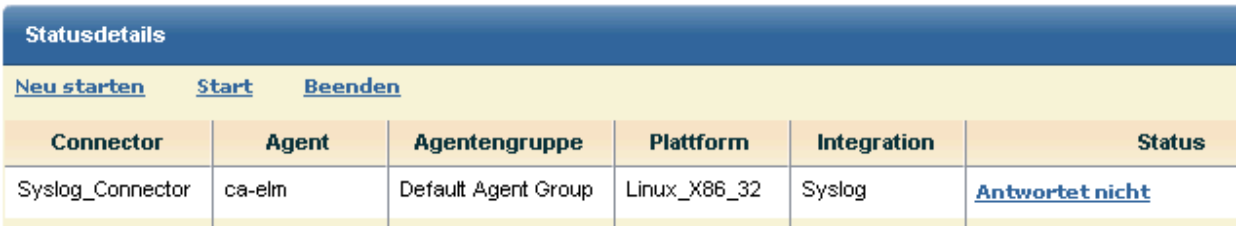
    a. Klicken Sie auf "Status und Befehl".



"Anzeigen des Status von Agents" ist ausgewählt. In der Spalte "Agenten" wird der Hostname des installierten Servers angezeigt, da sich der Standardagent auf diesem Server befindet. Der Status "Wird ausgeführt" wird angezeigt.

b. Klicken Sie auf den Link "Wird ausgeführt", um Details anzuzeigen.

c. Klicken Sie auf die Schaltfläche "Connectors", um den Status des Connectors anzuzeigen.



d. Klicken Sie auf den Link "Wird ausgeführt".

Die Felder "Prozent der CPU", "Arbeitsspeicherverwendung", Durchschnittliche Ereignisse pro Sekunde (EPS)" und "Anzahl der gefilterten Ereignisse" werden angezeigt.

Anzeigen von Syslog-Ereignissen

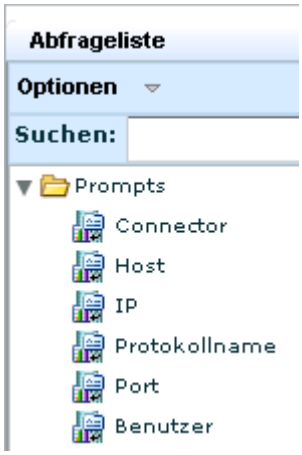
Eine der schnellsten Möglichkeiten, Abfrageergebnisse für Ereignisse anzuzeigen, die von einem Syslog-Listener erfasst wurden, ist die Verwendung der Eingabeaufforderung für den Host.

So zeigen Sie Syslog-Ereignisse an:

1. Wählen Sie die Registerkarte "Abfragen und Berichte".

   Die untergeordnete Registerkarte "Abfragen" wird angezeigt.

2. Erweitern Sie die Eingabeaufforderung auf der Abfrageliste, und wählen Sie den Host.

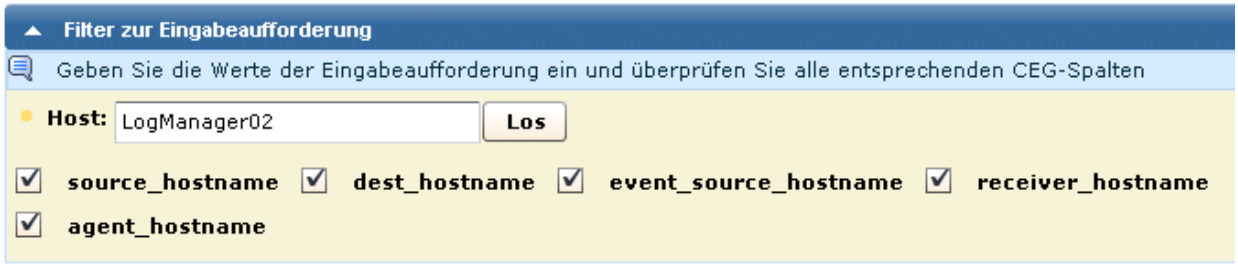


3. Übermitteln Sie eine Abfrage für Ereignisse, die vom Standardagent erfasst wurden.

   a. Geben Sie den Namen des Standardagents im Feld "Host" ein. Dies ist auch der Name des CA User Activity Reporting Module, auf dem er sich befindet.

   b. Wählen Sie "agent_hostname".

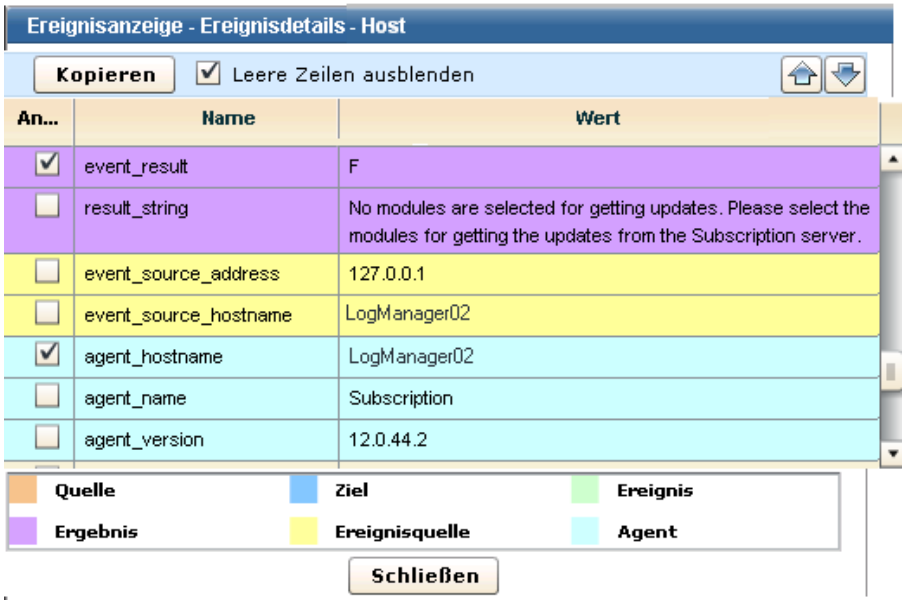
   c. Klicken Sie auf "Los".



4. Zeigen Sie die Ergebnisse an, die weiter verfolgt werden sollen.
   a. Klicken Sie auf die Spalte "Ergebnisse", um nach Ergebnissen zu sortieren.
   b. Blättern Sie zum ersten Ergebnis für "F" wie "Fehler". Angenommen, es handelt sich dabei um eine Konfigurationswarnung der Kategorie "Konfigurationsverwaltung".
   c. Doppelklicken Sie auf die Zeile, um die Details anzuzeigen.

   Die Ereignisanzeige wird geöffnet.

5. Blättern Sie zu dem Bereich, in dem das Ergebnis angezeigt wird. In diesem Beispiel handelt es sich bei dem Fehler um eine Warnung, die Sie im Modul für automatische Software-Updates konfigurieren müssen. Diese Warnung sollten Sie ignorieren, bis Sie alle gewünschten
   CA User Activity Reporting Module-Server installiert haben.



Kapitel 3: Bereitstellung von Windows-Agents

Dieses Kapitel enthält folgende Themen:

Erstellen eines Benutzerkontos für den Agent

Bevor Sie einen Agent auf einem Windows-Betriebssystem installieren, erstellen Sie im Ordner der Windows-Benutzer ein Konto für den Agent. Ziel dieses Agentkontos mit eingeschränkten Rechten ist es, den Agent mit den geringsten Berechtigungen auszuführen. Sie geben den Benutzernamen und das Kennwort ein, die Sie hier bei der Installation des Agents erstellt haben.

Hinweis: Sie können diesen Schritt überspringen und bei der Installation die Anmeldeinformationen der Domäne eines Administrators für den Agent eingeben. Diese Vorgehensweise wird jedoch nicht empfohlen.

So erstellen Sie ein Windows-Benutzerkonto für den Agent:

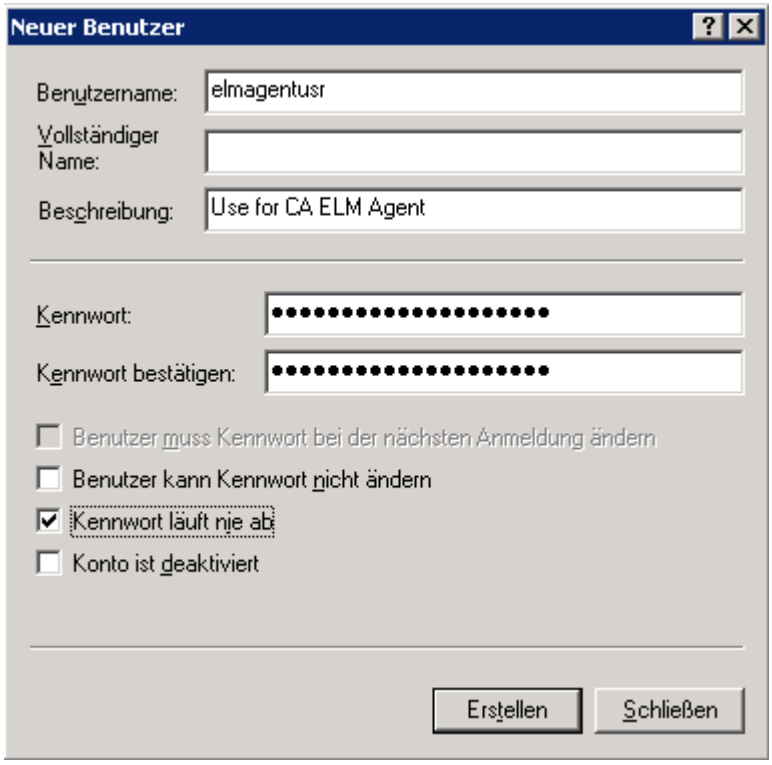
1. Melden Sie sich bei dem Host an, auf dem Sie den Agent installieren möchten. Verwenden Sie die Verwaltungsanmeldeinformationen.
2. Klicken Sie auf "Start", "Programme", "Verwaltung", "Computerverwaltung".
3. Erweitern Sie "Lokale Benutzer und Gruppen".

4. Klicken Sie mit der rechten Maustaste auf "Benutzer" und wählen Sie "Neuer Benutzer".

   Das Windows-Dialogfeld "Neuer Benutzer" wird geöffnet.

5. Geben Sie einen Benutzernamen und das Kennwort ein. Bestätigen Sie das Kennwort durch erneute Eingabe. Ein effektives Kennwort besteht aus einer Mischung von alphanumerischen Zeichen und Sonderzeichen. Beispiel: calmr12_agent. Optional können Sie eine Beschreibung eingeben.

   Wichtig! Notieren Sie den Namen und das Kennwort oder speichern Sie sie. Sie benötigen ihn bei der Installation des Agents.



6. Klicken Sie auf "Erstellen". Klicken Sie auf "Schließen".

Weitere Informationen:

Installieren eines Agents (siehe Seite 39)

Festlegen des Authentifizierungsschlüssels für einen Agenten

Bevor Sie den ersten Agent installieren, müssen Sie den Authentifizierungsschlüssel des Agents kennen. Sie können den Standardwert verwenden, wenn kein Schlüssel festgelegt wurde, den aktuellen Schlüssel verwenden, sofern ein solcher eingerichtet wurde, oder einen neuen Schlüssel festlegen. Der hier konfigurierte Authentifizierungsschlüssel des Agenten muss bei der Installation der einzelnen Agents angegeben werden. Dieser Schritt kann nur von einem Administrator durchgeführt werden.

So legen Sie den Authentifizierungsschlüssel des Agenten fest:

1. Öffnen Sie den Browser auf dem Host, auf dem Sie den Agent installieren möchten, und geben Sie die URL des CA User Activity Reporting Module-Servers für diesen Agent an. Beispiel:

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

2. Melden Sie sich beim CA User Activity Reporting Module-Server an. Geben Sie Ihren Benutzernamen und Ihr Kennwort ein, und klicken Sie auf "Anmelden".

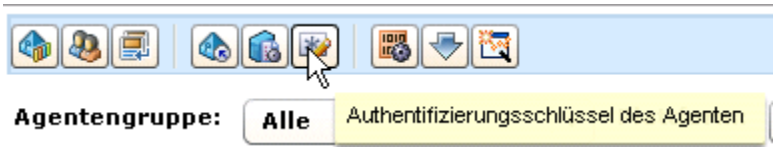
3. Klicken Sie auf die Registerkarte "Verwaltung".

   Im linken Fensterbereich wird der Protokollerfassungs-Explorer angezeigt.

4. Wählen Sie den Agent-Explorer-Ordner.

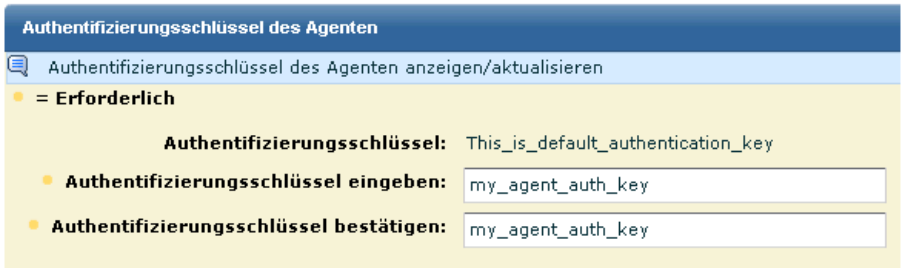
   Im Hauptbereich wird eine Symbolleiste angezeigt.

5. Klicken Sie auf "Authentifizierungsschlüssel des Agenten".



6. Geben Sie den Authentifizierungsschlüssel des Agenten ein, der für die Agentinstallation verwendet werden soll, oder notieren Sie den aktuellen Eintrag.

   Wichtig! Notieren Sie diesen Schlüssel oder zeichnen Sie ihn auf. Sie benötigen ihn bei der Installation des Agents.



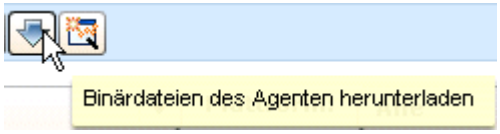
7. Klicken Sie auf "Speichern".
8. Fahren Sie mit dem Herunterladen des Agentinstallationsprogramms fort (nächster Schritt).

Herunterladen des Agentinstallationsprogramms

Wenn Sie nur den Authentifizierungsschlüssel des Agenten festlegen, können Sie das Agentinstallationsprogramm auf den Desktop herunterladen.

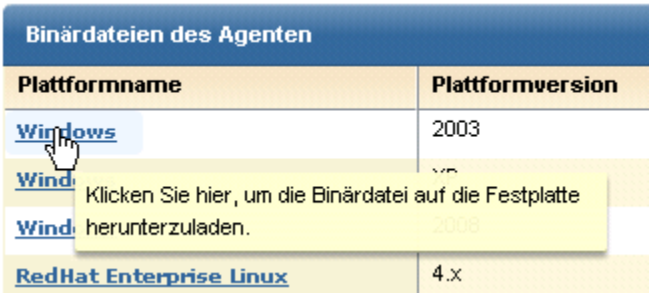
So laden Sie das Agentinstallationsprogramm herunter:

1. Klicken Sie in der Symbolleiste des Agent-Explorers auf "Binärdateien des Agents herunterladen".



   Im Hauptbereich werden Verknüpfungen zu den verfügbaren Binärdateien des Agents angezeigt.

2. Klicken Sie auf die Windows-Verknüpfung, um den Agent auf einem Server mit dem Betriebssystem Windows Server 2003 zu installieren.



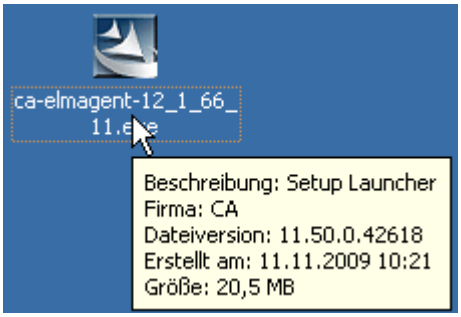
Das Dialogfeld "Speicherort für den Download nach <IP-Adresse>" wird geöffnet.

3. Wählen Sie den Desktop, und klicken Sie auf "Speichern".

Es wird ein Meldungsfeld geöffnet, das den Fortschritt des Downloads der ausgewählten Binärdateien des Agents anzeigt, gefolgt von einer Bestätigungsmeldung.

4. Klicken Sie auf "OK".
5. Minimieren Sie den Browser, unterbrechen Sie jedoch nicht die Verbindung, so dass Sie die Installation schnell überprüfen können, nachdem sie abgeschlossen ist.

   Auf dem Desktop wird das Setup-Startprogramm für die Agentinstallation angezeigt.



Installieren eines Agents

Bevor Sie beginnen, sollten Sie Folgendes bereit halten:

- IP-Adresse des CA User Activity Reporting Module-Servers, von dem Sie das Agentprogramm heruntergeladen haben
- Benutzername und Kennwort des Benutzerkontos, das Sie für den Agent erstellt haben
- Authentifizierungsschlüssel des Agenten, den Sie festgelegt haben

So installieren Sie einen Agent für einen Windows-Host:

1. Doppelklicken Sie auf das Startprogramm für die Agentinstallation.

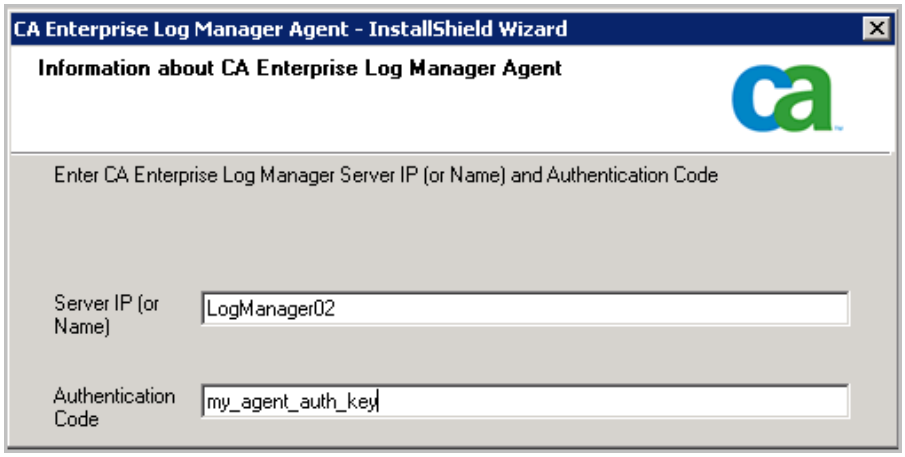
Der Installations-Assistent wird gestartet.

2. Klicken Sie auf "Weiter", lesen Sie den Lizenzvertrag, klicken Sie auf "Ich stimme den Bedingungen des Lizenzvertrags zu.", um fortzufahren, und klicken Sie auf "Weiter".
3. Akzeptieren Sie den angebotenen Installationspfad oder ändern Sie ihn, und klicken Sie auf "Weiter".
4. Geben Sie die erforderlichen Informationen wie folgt ein:
   a. Geben Sie den Hostnamen des CA User Activity Reporting Module-Servers ein, an den dieser Agent die erfassten Protokolle weiterleiten soll.

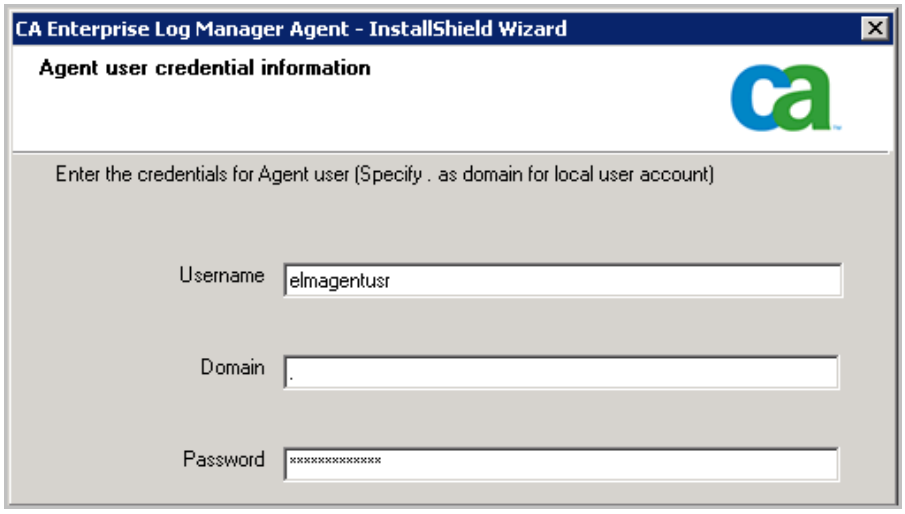
      Hinweis: Da CA User Activity Reporting Module in diesem Beispielszenario DHCP für die IP-Adressenzuordnung verwendet, dürfen Sie hier keine IP-Adresse eingeben. Andernfalls besteht die Gefahr, dass der Agent neu installiert werden muss, falls sich die IP-Adresse des Servers ändert.

   b. Geben Sie den Authentifizierungsschlüssel des Agenten ein.

   Beispiel:



5. Geben Sie Namen und Kennwort des Benutzerkontos ein, das Sie für den Agent eingerichtet haben, und klicken Sie auf "Weiter".



6. Klicken Sie auf "Weiter". Optional können Sie eine Datei für den exportierten Connector angeben.

   Die Seite "Kopieren der Dateien starten" wird angezeigt.

7. Klicken Sie auf "Weiter".

   Die Installation des Agents ist abgeschlossen.

8. Klicken Sie auf "Fertig stellen".

9. Fahren Sie mit der Konfiguration der Connectors für diesen Agent fort.

   Nachdem Sie die Connectors konfiguriert haben, werden die erfassten Ereignisse über Port 17001 an den CA User Activity Reporting Module-Ereignisprotokollspeicher gesendet.

   Wichtig! Wenn Sie über den Host, auf dem Sie den Agent installiert haben, keinen ausgehenden Datenverkehr zulassen und die Windows Firewall verwenden, müssen Sie diesen Port auf Ihrer Windows Firewall öffnen.

Weitere Informationen:

Herunterladen des Agentinstallationsprogramms (siehe Seite 38)
Erstellen eines Benutzerkontos für den Agent (siehe Seite 35)
Festlegen des Authentifizierungsschlüssels für einen Agenten (siehe Seite 37)

Erstellen eines Connectors basierend auf NTEventLog

Nach der Installation eines Agents können Sie einen Connector erstellen, um die Ereignisquelle für die Erfassung von Ereignissen festzulegen. Da Sie einen Agent auf einem Server mit Windows-Betriebssystem installiert haben, erstellen Sie einen Connector basierend auf der NTEventLog-Integration und legen die Einstellungen für den WMILogSensor wie im Connector-Handbuch beschrieben fest. Dieses Handbuch öffnen Sie über den Assistenten zum Erstellen neuer Connectors. Sie geben den Namen des Hosts an, auf dem der Agent für eine agentbasierte Protokollerfassung installiert ist. Optional können Sie einen anderen WMI Protokollsensor für diesen Connector hinzufügen und einen Host angeben, der nicht dem Host entspricht, auf dem der Agent installiert ist. So ermöglichen Sie die Protokollverbindung ohne Agent. Der/die zusätzliche(n) Host(s) müssen sich in derselben Domäne befinden und über denselben Windows-Administrator verfügen wie der erste hinzugefügte Host.

So erstellen Sie einen Connector basierend auf NTEventLog:

1. Maximieren Sie den Browser, der den CA User Activity Reporting Module Agent-Explorer anzeigt.
2. Erweitern Sie den Agent-Explorer und anschließend die Standard-Agentengruppe.

   Der Name des Computers, auf dem der Agent installiert wurde, wird angezeigt.

3. Wählen Sie diesen Agent.

   Das Feld "Agenten-Connectors" wird angezeigt.

4. Klicken Sie auf "Neuen Connector erstellen".

   Der Assistent zum Erstellen von neuen Connectors wird geöffnet. Der Schritt "Erstellung von neuem Connector" ist ausgewählt.

5. Belassen Sie die Auswahl von "Integrationen" und wählen Sie aus der Integrations-Dropdownliste NTEventLog.

   Die Felder "Connector-Name" und "Beschreibung" werden auf Grundlage der Auswahl unter "Integration" ausgefüllt.

6. Bearbeiten Sie den Connector-Namen, um einen eindeutigen Namen zu definieren. Erweitern Sie den Namen möglicherweise durch den Namen des Zielservers, z. B. NTEventLog_Connector_USER001LAB.

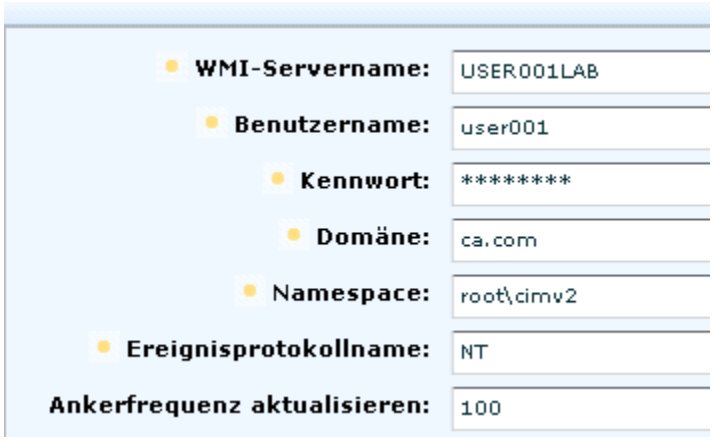
7. Wählen Sie den Schritt "Connector-Konfiguration".

   Der Bereich "Sensorkonfiguration" wird eingeblendet. Er enthält eine Hilfe-Schaltfläche mit einer Verknüpfung zum Connector-Handbuch für NTEventLog, in dem Sie Hilfe zu den Feldern für die Sensorkonfiguration finden.

8. Klicken Sie auf die Schaltfläche zum Anzeigen von Details für WMI-Quellen.

9. Konfigurieren Sie die WMILogSensor-Einstellungen des lokalen Computers für die agentbasierte Protokollerfassung. Weitere Informationen erhalten Sie, wenn Sie auf "Hilfe" klicken.

   Das folgende Beispiel zeigt eine Konfiguration, bei der der Benutzer ein Windows-Administrator auf dem angegebenen WMI-Server ist. Die Domäne gilt für den WMI-Server.



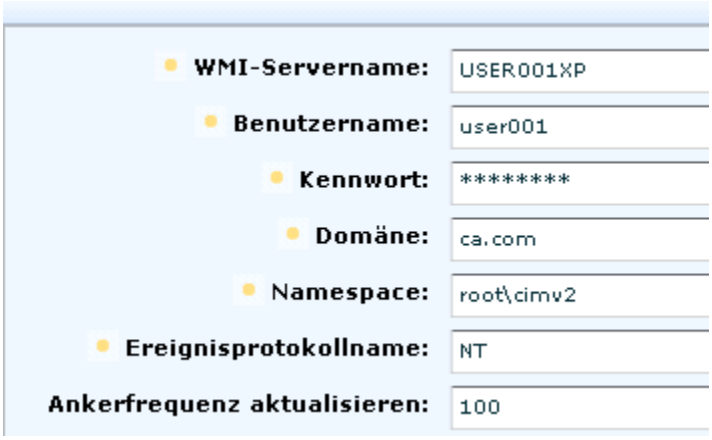
10. (Optional) Konfigurieren Sie mit demselben Connector einen WMI-Sensor für einen anderen Computer für die Protokollerfassung ohne Agent.

    a. Klicken Sie auf die Schaltfläche "Übergeordneten Knoten wiederholen".

       Die folgende Abbildung zeigt eine Konfiguration mit zwei WMI-Quellen.

b. Konfigurieren Sie die WMILogSensor-Einstellungen für einen anderen Computer.

Das folgende Beispiel zeigt eine Konfiguration für einen zweiten WMI-Protokollsensor in derselben Domäne und mit denselben Administrator-Anmeldeinformationen.



11. Klicken Sie auf "Speichern" und "Schließen".
12. Um den Status des Connectors anzuzeigen, den Sie konfiguriert haben, gehen Sie folgendermaßen vor:
    a. Wählen Sie im linken Fensterbereich den Agent aus.
    b. Klicken Sie auf "Status und Befehl".
    c. Wählen Sie "Anzeigen des Status von Connectors".

    Das Fenster "Statusdetails" wird angezeigt.

13. Klicken Sie auf den Link "Wird ausgeführt".

    Der angezeigte Status des Ziels, das im Connector konfiguriert wurde, umfasst Prozent der CPU, Arbeitsspeicherverwendung und durchschnittliche Ereignisse pro Sekunde (EPS).

Konfigurieren einer Windows-Ereignisquelle

Nachdem Sie einen Connector mit der NTEventLog-Integration auf dem Agent konfiguriert haben, sollten Sie Ereignisse in der Ereignisanzeige anzeigen können. Falls Ereignisse nicht an die Ereignisanzeige weitergeleitet werden, sollten Sie die Windows-Einstellungen für die lokalen Richtlinien auf der Ereignisquelle ändern.

So konfigurieren Sie lokale Richtlinien auf der Ereignisquelle für einen NTEventLog-Connector:

1. Wenn der Protokollerfassungs-Explorer nicht bereits angezeigt wird, klicken Sie auf die Registerkarte "Verwaltung".
2. Erweitern Sie die Punkte "Ereignisverfeinerungs-Bibliothek", "Integrationen" und "Automatische Software-Updates", wählen Sie "NTEventLog", und klicken Sie auf die Hilfeverknüpfung über dem Integrationsnamen im Teilfenster "Integrationsdetails anzeigen".

   Das Connector-Handbuch für das NT-Ereignisprotokoll (Sicherheit, Anwendung, System) wird geöffnet.
3. Minimieren Sie die Benutzeroberfläche von CA User Activity Reporting Module, und befolgen Sie die Anweisungen im Connector-Handbuch, um lokale Richtlinien einer Ereignisquelle auf einem Windows-Betriebssystem zu bearbeiten.

   Hinweis: Wenn es sich bei Ihrem System um Windows Server 2003 handelt, wählen Sie in der Systemsteuerung die Optionen "Verwaltung", "Lokale Sicherheitsrichtlinie", und erweitern Sie anschließend die lokalen Sicherheitsrichtlinien.
4. (Optional) Wenn Sie einen WMI-Sensor für einen zweiten WMI-Server konfiguriert haben, bearbeiten Sie auch die lokalen Richtlinien dieses Servers.
5. Maximieren Sie CA User Activity Reporting Module.

Anzeigen von Protokollen der Windows-Ereignisquellen

Eine der schnellsten Möglichkeiten, Abfrageergebnisse für eingehende Ereignisse anzuzeigen, ist die Verwendung der Eingabeaufforderung für den Host. Sie können auch Abfragen oder Berichte auswählen.

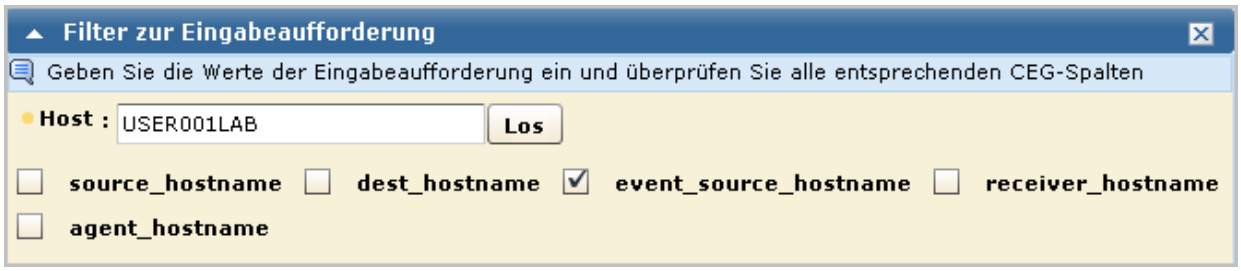
So zeigen Sie eingehende Ereignisprotokolle an:

1. Wählen Sie die Registerkarte "Abfragen und Berichte".

   Die untergeordnete Registerkarte "Abfragen" wird angezeigt.

2. Erweitern Sie die Eingabeaufforderung auf der Abfrageliste, und wählen Sie den Host.

3. Geben Sie den Namen des WMI-Servers ein, der im Feld "Host" für den Sensor konfiguriert wurde. Entfernen Sie alle anderen Markierungen, und klicken Sie auf "Los".



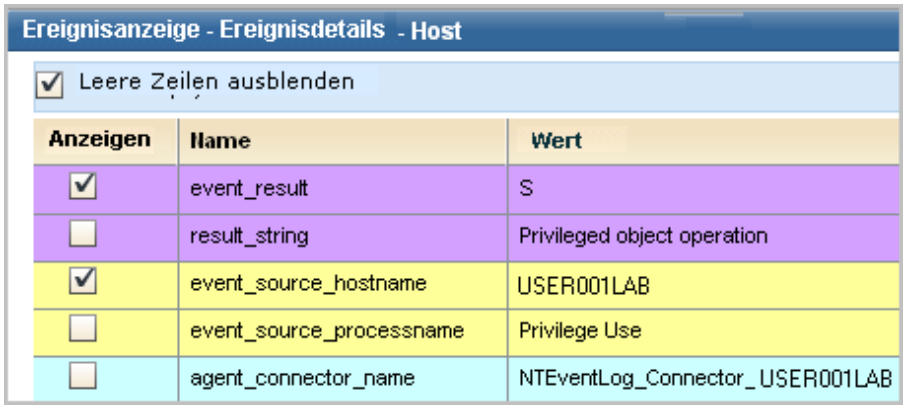
   Die Ereignisse der WMI-Server-Ereignisquelle werden angezeigt.

4. Klicken Sie auf "CA-Schweregrad", und blättern Sie, bis Sie eine Warnung gefunden haben. Im Folgenden wird ein verkürztes Beispiel ohne die Spalten "Datum" und "Ereignisquelle" angezeigt:

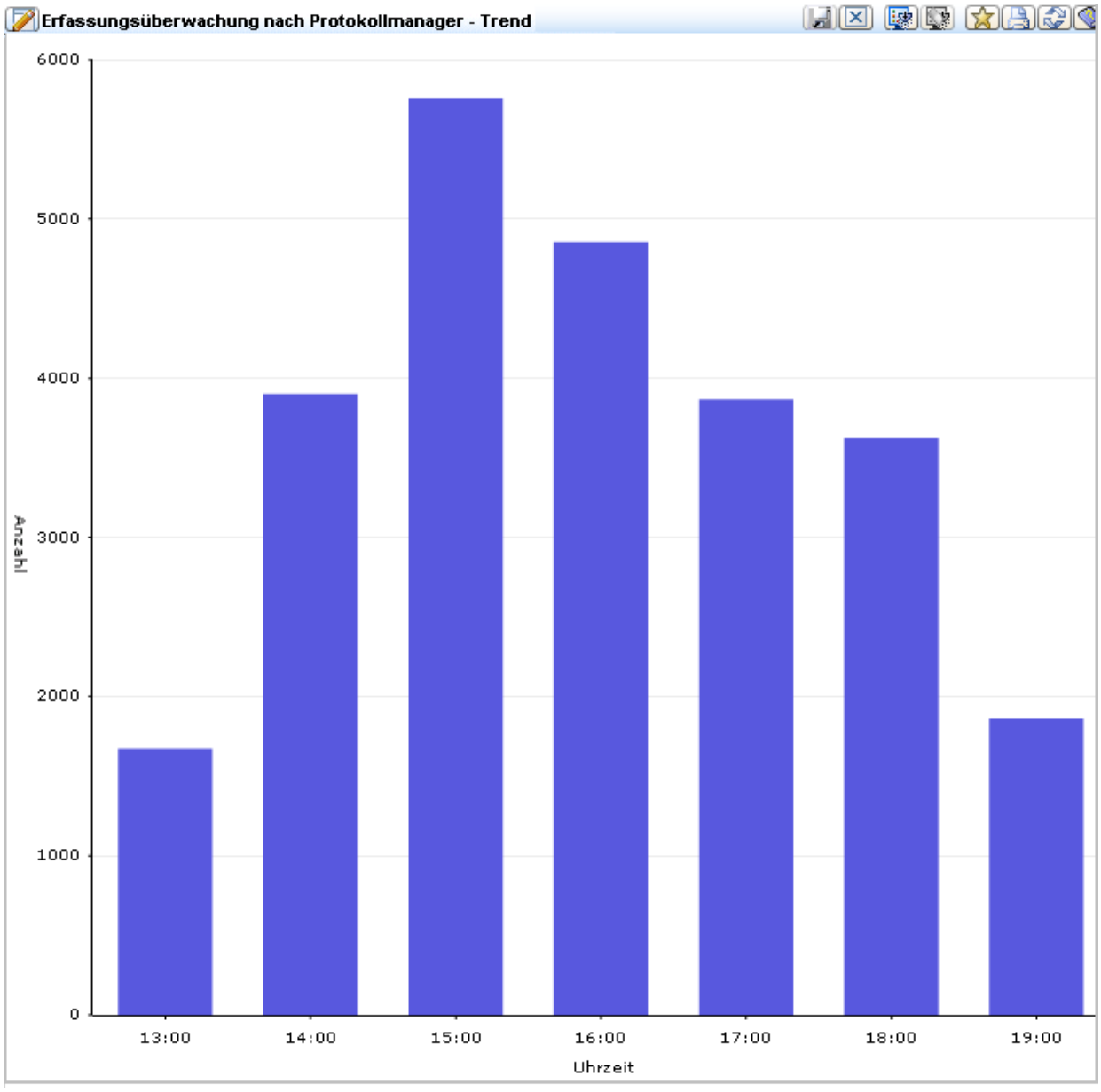
CA-Schweregrad	Quellbenutzer	Ergebnis	Kategorie	Aktion	Protokollname
Warnung	calm_agent	S	System Access	Privilege Use	NT-Security

5. Klicken Sie auf "Rohereignisse anzeigen", um die Rohereignisse für die Warnung anzuzeigen.

6. Doppelklicken Sie auf die Warnung, um die Ereignisanzeige mit weiteren Daten zu öffnen. Das folgende Beispiel zeigt einige Zeilen mit Beispieldaten:



7. Klicken Sie auf die Registerkarte "Abfragen und Berichte", klicken Sie in der Abfrageliste auf eine Abfrage, z. B. "Erfassungsüberwachung nach Log Manager - Trend". Zeigen Sie das entsprechende Balkendiagramm an.



8. Klicken Sie auf "Berichte". Geben Sie unter "Berichtsliste" im Feld "Suchen" den Eintrag "selbst" ein, um den Berichtsnamen "Selbstüberwachende Ereignisse des Systems" anzuzeigen. Wählen Sie diesen Bericht, um eine Liste der Ereignisse anzuzeigen, die vom CA User Activity Reporting Module-Server generiert wurden.

Hinweis: Weitere Informationen zum Planen von Berichten mit Informationen, die Sie analysieren möchten, finden Sie in der Online-Hilfe oder im *Verwaltungshandbuch*.

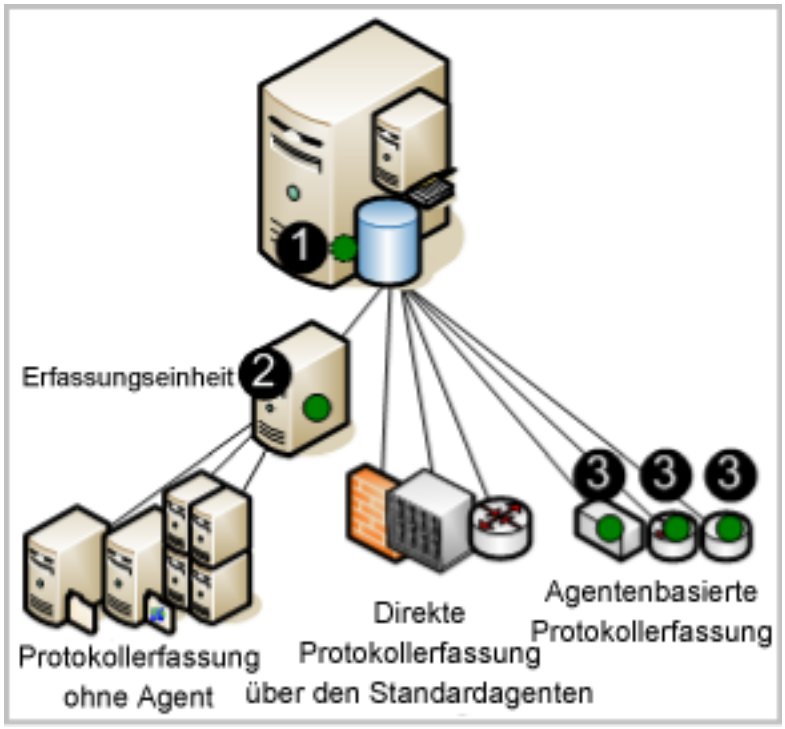
Kapitel 4: Hauptfunktionen

Dieses Kapitel enthält folgende Themen:

Protokollerfassung

Der CA User Activity Reporting Module-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 User Activity Reporting Module, 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 User Activity Reporting Module 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 User Activity Reporting Module-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 User Activity Reporting Module-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

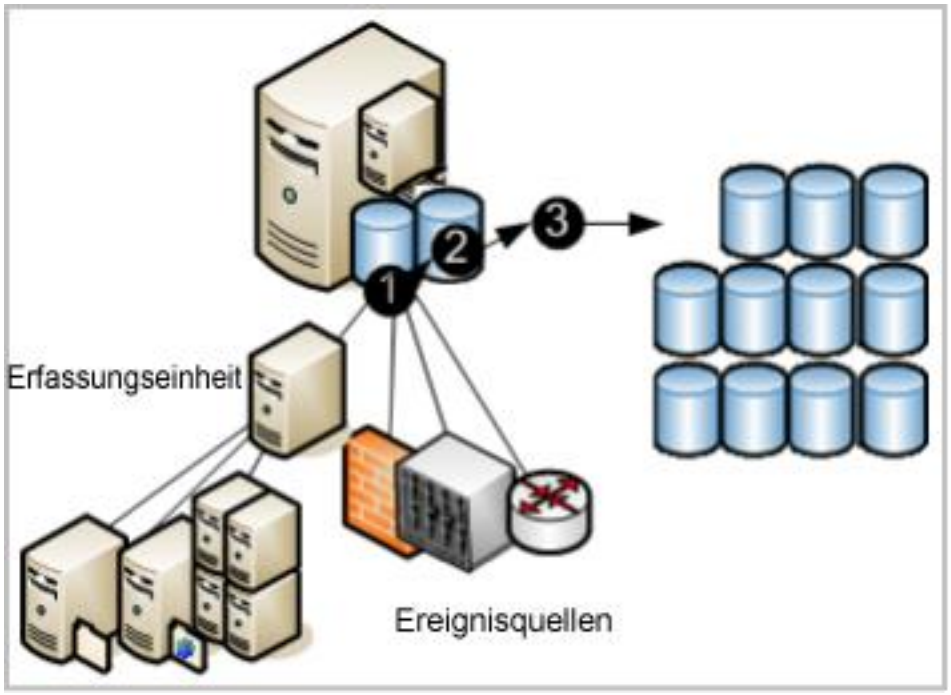
  Bei der agentbasierten Erfassung wird ein Agent überall dort installiert, wo ein oder mehrere Ereignisquellen ausgeführt werden und ein Connector für jede Ereignisquelle konfiguriert wurde.

  Vorteil: Sie können Protokolle von Quellen erfassen, auch wenn die Bandbreite zwischen Quelle und CA User Activity Reporting Module 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 User Activity Reporting Module 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 User Activity Reporting Module 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 User Activity Reporting Module 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 User Activity Reporting Module-Verwaltungshandbuch*. Details zum Normalisieren und Kategorisieren von Ereignissen finden Sie in der Online-Hilfe im Abschnitt zur ELM-Schemadefinition.

Konformitätsberichte

Mit CA User Activity Reporting Module 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 User Activity Reporting Module 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 User Activity Reporting Module-Verwaltungshandbuch*.

Alarm bei Verletzung von Richtlinien

Mit CA User Activity Reporting Module können Sie bei Ereignissen, die ein zeitnahes Eingreifen erfordern, das Versenden von Alarmen automatisieren. Sie können Aktionsalarme auch jederzeit über CA User Activity Reporting Module 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

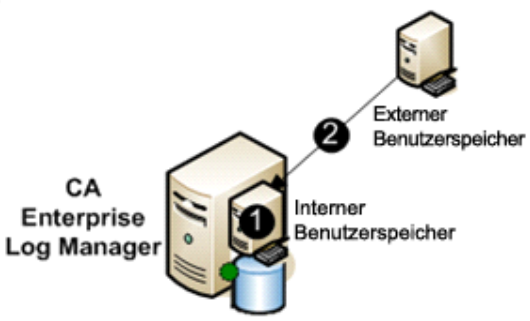
Schlüssellisten können manuell, durch Import einer Datei oder durch Ausführen eines CA IT PAM-Prozesses mit dynamischen Werten aktualisiert werden.

Hinweis: Einzelheiten zu Aktionsalarmen finden Sie im *CA User Activity Reporting Module-Administrationshandbuch*.

Verwaltung von Berechtigungen

Wenn Sie den Benutzerspeicher konfigurieren, können Sie entscheiden, ob Sie den Standardbenutzerspeicher von CA User Activity Reporting Module verwenden möchten, um Benutzerkonten einzurichten, oder ob Sie einen externen Benutzerspeicher referenzieren möchten, auf dem bereits Benutzerkonten definiert wurden. Die zugrunde liegende Datenbank ist für CA User Activity Reporting Module exklusiv. Es wird kein kommerzielles Datenbankmanagementsystem (DBMS) verwendet.

Als externe Benutzerspeicher werden CA SiteMinder und LDAP-Verzeichnisse wie beispielsweise Microsoft Active Directory, Sun One und Novell eDirectory unterstützt. Wenn Sie einen externen Benutzerspeicher referenzieren, werden die Informationen der Benutzerkonten automatisch im schreibgeschützten Format geladen (siehe Pfeil in der folgenden Abbildung). Sie definieren ausschließlich anwendungsspezifische Details für ausgewählte Konten. Es werden keine Daten vom internen Benutzerspeicher in den referenzierten externen Benutzerspeicher verschoben.



Die Nummern in den Abbildungen beziehen sich auf folgende Schritte:

1. Der interne Benutzerspeicher verwaltet Berechtigungen, indem die von den Benutzern bei der Anmeldung eingegebenen Informationen authentifiziert werden. Anschließend erhalten die Benutzer Zugriff auf verschiedene Funktionen der Benutzeroberfläche, und zwar auf der Grundlage von Berechtigungen, die mit den Rollen der entsprechenden Benutzerkonten verknüpft sind. Wenn Name und Kennwort des Benutzers, der sich anmeldet, von einem externen Benutzerspeicher geladen wurden, müssen die eingegebenen Anmeldeinformationen den geladenen Anmeldeinformationen entsprechen.
2. Der externe Benutzerspeicher dient lediglich dem Laden der Benutzerkonten in den internen Benutzerspeicher. Diese werden automatisch geladen, wenn die Referenz auf den Benutzerspeicher gespeichert wird.

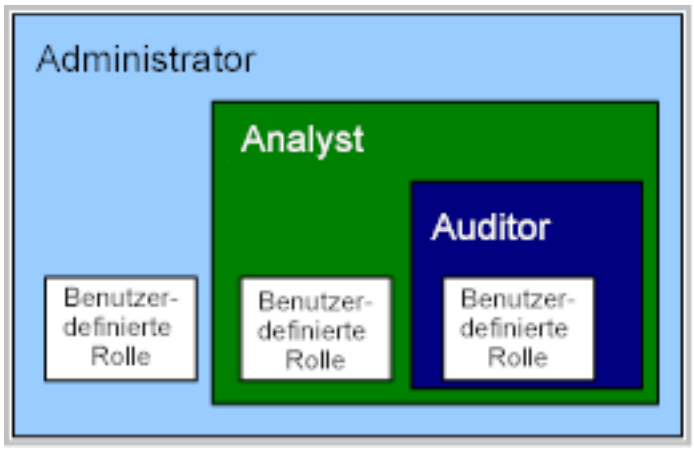
Hinweis: Weitere Informationen zum Konfigurieren des grundlegenden Benutzerzugriffs finden Sie im *Implementierungshandbuch von CA User Activity Reporting Module*. Weitere Informationen zu Richtlinien, die vordefinierte Rollen, das Erstellen von Benutzerkonten und das Zuweisen von Rollen unterstützen, finden Sie im *CA User Activity Reporting Module-Verwaltungshandbuch*.

Rollenbasierter Zugriff

CA User Activity Reporting Module bietet drei vordefinierte Anwendungsgruppen oder Rollen. Administratoren weisen Benutzern folgende Rollen zu, um Zugriffsrechte für CA User Activity Reporting Module-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.



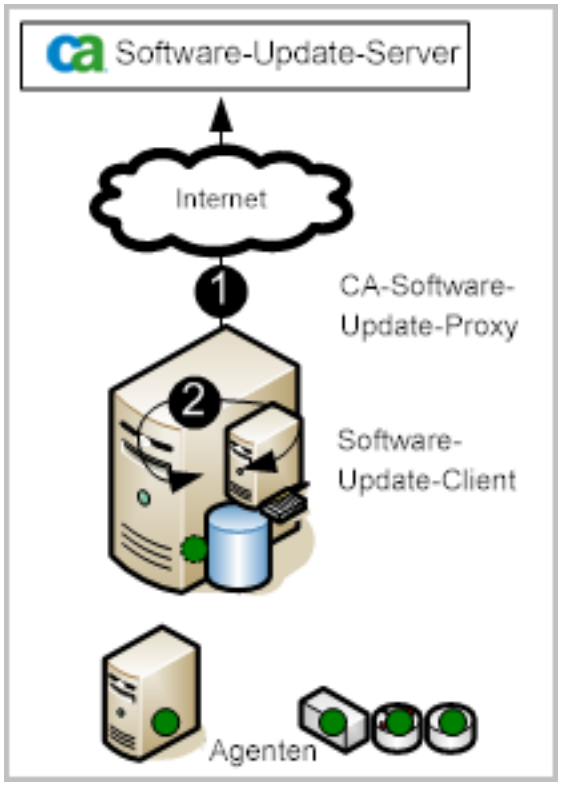
Administratoren können den Zugriff auf jede Ressource anpassen, indem sie eine benutzerdefinierte Anwendungsgruppe mit entsprechenden Richtlinien erstellen und diese Anwendungsgruppe oder Rolle bestimmten Benutzerkonten zuweisen.

Hinweis: Weitere Informationen zur Planung oder Erstellung von Rollen, benutzerdefinierten Richtlinien und Zugriffsfiltern finden Sie im *CA User Activity Reporting Module-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 User Activity Reporting Module-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 User Activity Reporting Module-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 User Activity Reporting Module-Server-kontaktiert als Standardserver für das-Software-Aktualisierungs-Höhlen-CA-Software-Update-Server-Und Lädt Alle Verfügbaren Neuen-aktualisieren-Herunter. Der CA User Activity Reporting Module-Server erstellt eine Sicherung und verschiebt dann als Inhaltsaktualisierungen zur eingebetteten Komponente des Verwaltungsservers sterben, der als Inhaltsaktualisierungen für alle anderen CA User Activity Reporting Modules speichert sterben.
2. Der-CA User Activity Reporting Module-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*.

Vorgefertigter Inhalt

CA User Activity Reporting Module umfasst vordefinierten Inhalt, den Sie verwenden können, sobald Sie das Produkt installiert und konfiguriert haben. Durch das automatische Software-Update werden regelmäßig neue Inhalte hinzugefügt und vorhandene Inhalte aktualisiert.

Kategorien vordefinierter Inhalte sind z. B.:

- Berichte mit Kennungen
- Abfragen mit Kennungen
- Integrationen mit zugehörigen Sensoren, Analysedateien (XMP), Zuordnungsdateien (DM) und, in einigen Fällen, Unterdrückungsregeln
- Unterdrückungs- und Zusammenfassungsregeln

Kapitel 5: Weitere Informationen zu CA User Activity Reporting Module

Dieses Kapitel enthält folgende Themen:

Anzeigen von Kurzinfos

Sie können die Bedeutung von Schaltflächen, Kontrollkästchen und Berichten auf der CA User Activity Reporting Module-Seite in Ihrer aktuellen Ansicht abfragen.

So zeigen Sie Kurzinfos und andere Hilfselemente an:

1. Halten Sie den Cursor über die Schaltfläche, um eine Beschreibung der entsprechenden Funktion anzuzeigen. Auf diese Weise können Sie die Funktion aller Schaltflächen anzeigen.

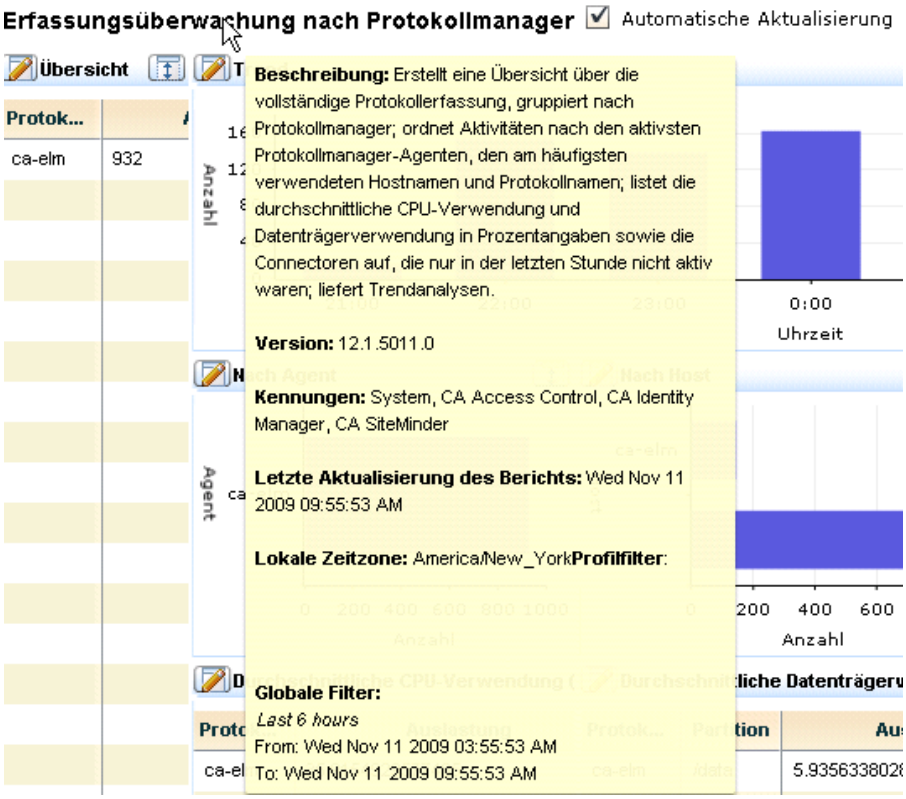
2. Beachten Sie den Unterschied zwischen aktiven und inaktiven Schaltflächen.

   Aktivierte Schaltflächen werden farbig angezeigt. So wird die Schaltfläche "Zugriffsfilterliste" für Administratoren der Benutzer- und Zugriffsverwaltung farbig angezeigt.

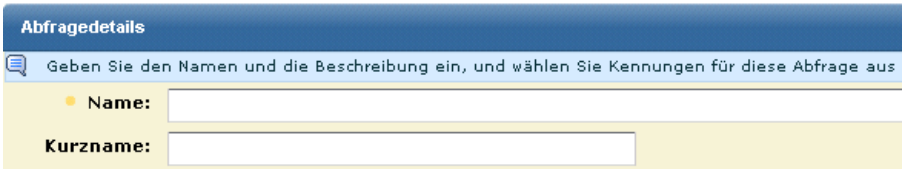
Deaktivierte Schaltflächen werden schwarz-weiß dargestellt. So wird die Schaltfläche "Zugriffsfilterliste" für Auditoren schwarz-weiß dargestellt.

3. Zeigen Sie die Beschreibungen für Eingabefelder und Kontrollkästchen an, indem Sie den Cursor über den Feldnamen halten.

4. Zeigen Sie Beschreibungen für Berichte an, indem Sie den Cursor über den Berichtnamen halten.



5. Links neben einigen Feldern wird ein orangefarbener Punkt angezeigt. Felder mit diesem Punkt müssen ausgefüllt werden. Eine zu speichernde Konfiguration kann erst gespeichert werden, wenn alle erforderlichen Felder ausgefüllt wurden.



Anzeigen der Online-Hilfe

Sie können für die angezeigte Seite oder für jede Aufgabe, die Sie durchführen möchten, Hilfe aufrufen.

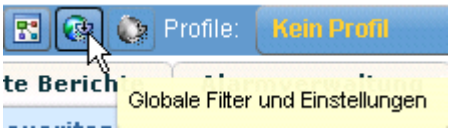
So öffnen Sie die Online-Hilfe:

1. Klicken Sie auf der Symbolleiste auf "Hilfe", um die Online-Hilfe für CA User Activity Reporting Module zu öffnen.

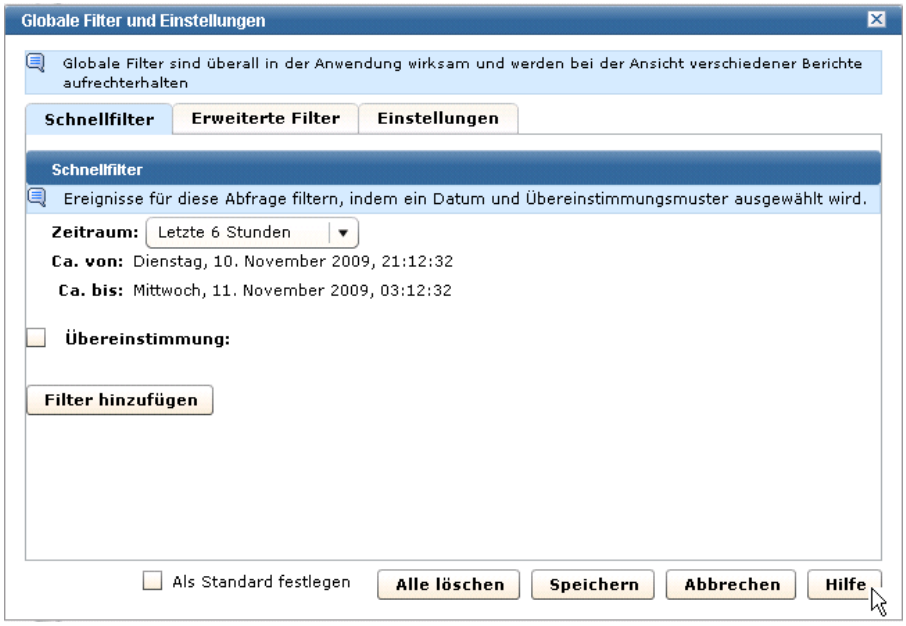
Das CA User Activity Reporting Module-Hilfesystem wird geöffnet. Im linken Fensterbereich wird der Inhalt aufgelistet.

2. Öffnen Sie über eine Hilfe-Schaltfläche die kontextabhängige Hilfe (siehe folgendes Beispiel).

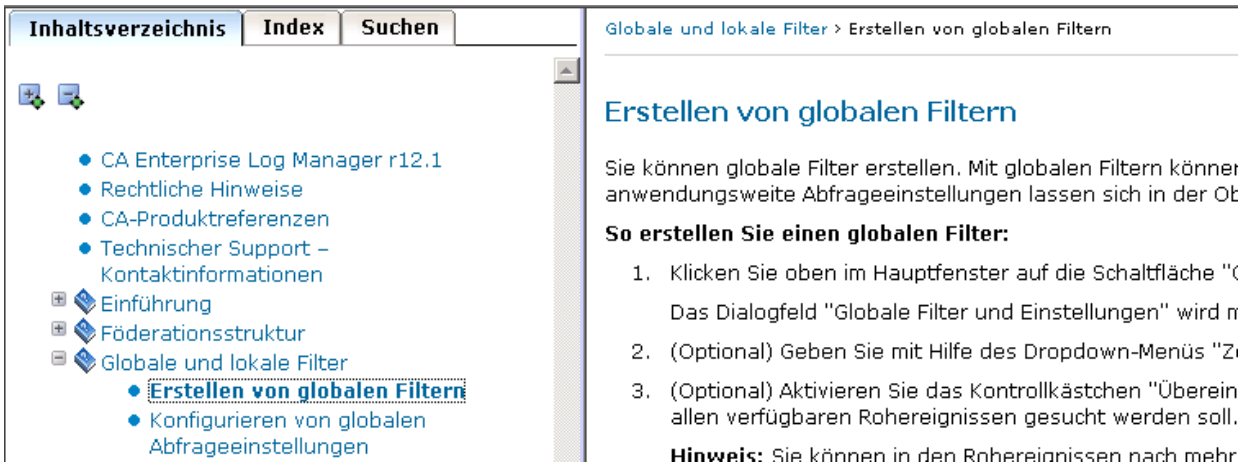
   a. Klicken Sie auf die Schaltfläche "Globale Filter anzeigen/bearbeiten".



   Das Fenster "Globale Filter und Einstellungen" mit einer Hilfe-Schaltfläche wird geöffnet.



b. Klicken Sie auf die Schaltfläche "Hilfe". In einem zweiten Fenster wird die Online-Hilfe für den Vorgang geöffnet, den Sie auf der aktuellen Seite, im aktuellen Bereich oder im Dialogfeld durchführen können.



c. Wenn Sie wissen, welche Aufgabe Sie ausführen möchten, aber nicht wissen, wie Sie in CA User Activity Reporting Module auf die entsprechende Seite gelangen, nutzen Sie zunächst das Inhaltsverzeichnis. Durch Klicken auf den Aufgabennamen wird die Seite geöffnet.

Hinweis: Wenn Sie die Aufgabe im Inhaltsverzeichnis nicht finden können, schlagen Sie im Bookshelf der Dokumentation nach.

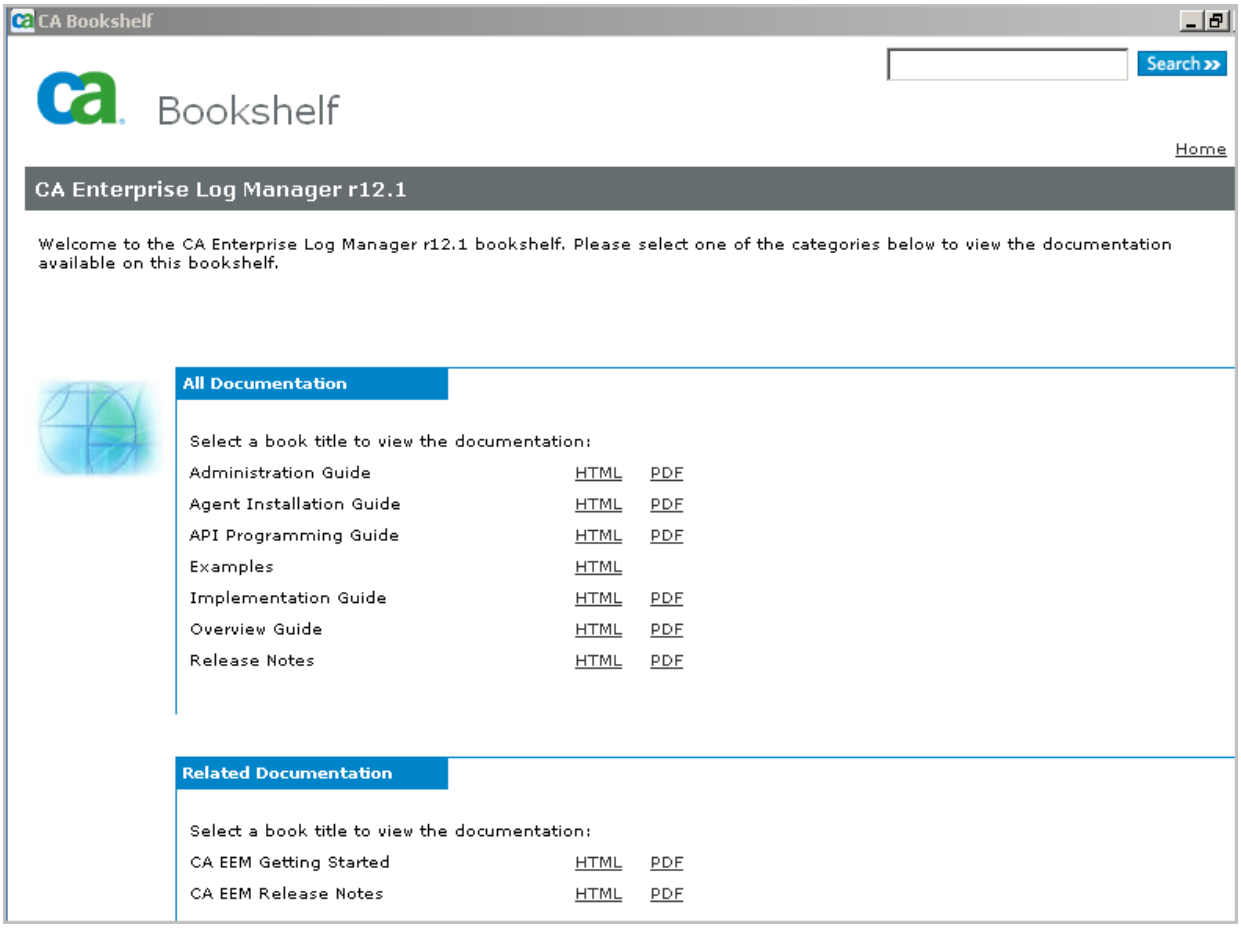
Überblick über das Bookshelf mit Dokumentation

Sie können das Bookshelf auf Ihr lokales Laufwerk kopieren. Die Bücher können als HTML oder PDF geöffnet werden. Bücher im HTML-Format enthalten buchübergreifende Querverweise.

So erhalten Sie einen Überblick über das Bookshelf:

1. Kopieren Sie das Bookshelf von der Installations-DVD der Anwendung auf Ihr lokales Laufwerk oder laden Sie es von der CA Kundensupport-Website herunter. Doppelklicken Sie auf die Datei "Bookshelf.hta" oder "Bookshelf.html", um das Bookshelf zu öffnen.

   Ein Fenster wird angezeigt, das in etwa folgendermaßen aussieht:

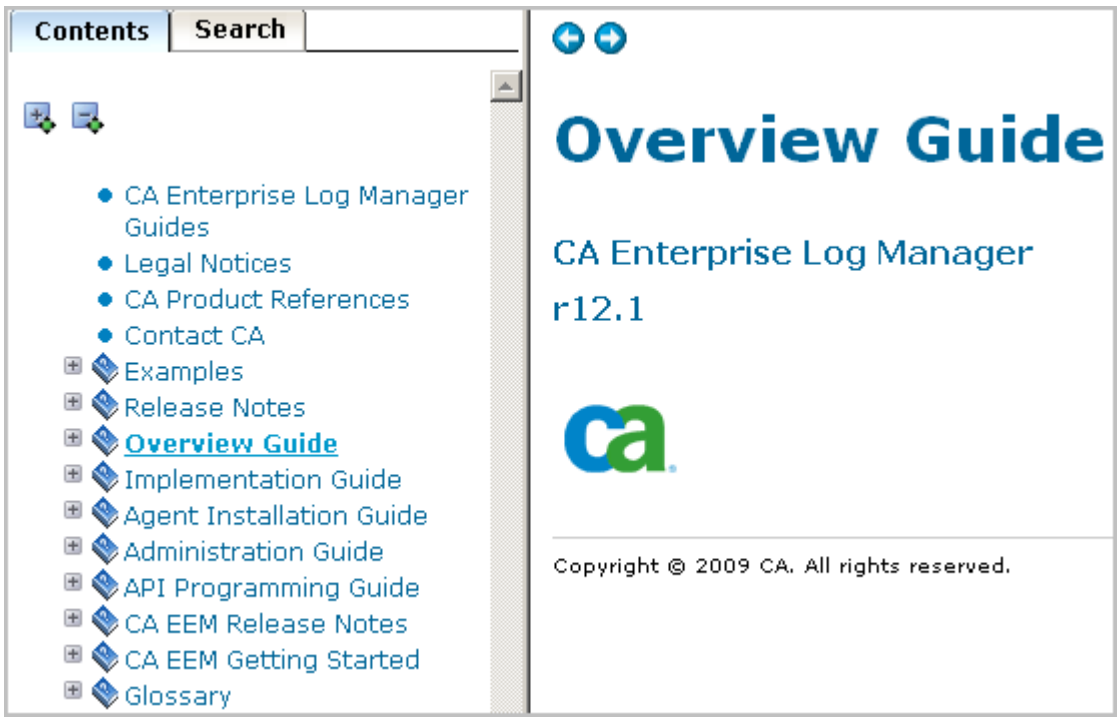


Eine Beschreibung des Inhalts der wichtigsten Handbücher und Beispiele folgen:

Komponente	Inhalt
Agent-Installationshandbuch	Installieren der Agents
Implementierungshandbuch	Installieren und Konfigurieren eines CA User Activity Reporting Module-Systems.
Administrationshandbuch	Anpassen der Konfiguration, Durchführen von routinemäßigen Verwaltungsaufgaben und Arbeiten mit Abfragen, Berichten und Alarmen.
API-Programmierhandbuch	Mit der API können Sie Ereignisdaten in einem Web-Browser anzeigen oder Berichte in ein anderes CA-Produkt oder ein Produkt eines Drittanbieters einbetten.
Beispiele	Lösen allgemeiner unternehmensbezogener Probleme mit Verknüpfungen zu Kapiteln in der Dokumentation.

2. Geben Sie im Eingabefeld "Suchen" einen Wert ein, und klicken Sie auf die Schaltfläche "Suchen", um alle dokumentierten Vorkommnisse anzuzeigen, die Ihren Eintrag enthalten.
3. Klicken Sie auf eine Druckverknüpfung, um die PDF-Version des ausgewählten Handbuchs zu öffnen.

4. Klicken Sie auf eine HTML-Verknüpfung, um den integrierten Dokumentationssatz zu öffnen. Der integrierte Satz enthält alle Handbücher im HTML-Format. Wenn Sie die HTML-Verknüpfung für das Übersichtshandbuch wählen, wird dieses Handbuch angezeigt.



Index