CA Enterprise Log Manager

Overview Guide

r12.1 SP1

ca technologies

CA Product References

This document references the following CA products:

- 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®

Contact CA

Contact CA Support

For your convenience, CA provides one site where you can access the information you need for your Home Office, Small Business, and Enterprise CA products. At http://ca.com/support, you can access the following:

- Online and telephone contact information for technical assistance and customer services

- Information about user communities and forums

- Product and documentation downloads

- CA Support policies and guidelines

- Other helpful resources appropriate for your product

Provide Feedback

If you have comments or questions about CA product documentation, you can send a message to techpubs@ca.com.

If you would like to provide feedback about CA product documentation, complete our short customer survey, which is available on the CA Support website at http://ca.com/docs.

Documentation Changes

The following documentation updates have been made since the last release of this documentation:

- Quick Start Overview—This existing topic has been updated to reference additional types of events, besides syslogs, that can be collected by the default agent on the CA Enterprise Log Manager server.

- Policy Violation Alerting—This existing topic has been updated to reference the ability to send alerts as SNMP traps to network security monitoring systems and to direct alerts to run an IT PAM event/alert output process, such as one to create help desk tickets.

- Explore the Bookshelf of Documentation—This existing topic has been updated to reference the new API Programming Guide, which now appears on the CA Enterprise Log Manager bookshelf.

More information:

Contents

Chapter 1: Introduction

This section contains the following topics:

About this Guide

This *Overview Guide* introduces CA Enterprise Log Manager. It begins with quick tutorials that give you hands on experience with the product right away. The first tutorial walks you through getting a single-server CA Enterprise Log Manager up and running and viewing syslogs collected from UNIX devices in close network proximity. The second tutorial walks you through installing an agent on a Windows operating system, configuring log collection, and viewing resulting events logs. It then describes the major features and where to go to learn more. This guide is intended for all audiences.

A summary of the contents follows:

Section	Describes how to
About CA Enterprise Log Manager	Integrate CA Enterprise Log Manager into your current network environment
Quick Start Deployment	Install a single-server system, configure syslog event sources, update the syslog connector for the default agent, and view refined events
Windows Agent Deployment	Prepare for agent installation, install an agent for the Windows operating system, configure one connector for agent-based collection, update the event source, and view generated events
Key Capabilities	Benefit from key features, including log collection, log storage, compliance reporting and alerting
Learning More about CA Enterprise Log Manager	Get the information you need through tooltips, online help, and the documentation bookshelf

Note: For details on operating system support or system requirements, see the *Release Notes*. For step-by-step procedures on installing CA Enterprise Log Manager and performing initial configuration, see the *Implementation Guide.* For details on installing an agent, see the *Agent Installation Guide*. For details on using and maintaining the product, see the *Administration Guide.* For help on using any CA Enterprise Log Manager page, see the online help.

About CA Enterprise Log Manager

CA Enterprise Log Manager focuses on IT compliance and assurance. It lets you collect, normalize, aggregate, and report on IT activity, and generate alerts requiring action when possible compliance violations occur. You can collect data from disparate security and non-security devices.

Your Network--Before Installation

Federal regulations and mandates require log record management. To comply, you must:

- Make logs available for auditing.

- Store logs for years.

- Restore logs upon request.

What makes log records difficult to manage is their large number, their location, and their temporary nature. Logs are generated continuously by user and process activity on software. The rate of generation is measured in events per second (eps). Raw events are recorded on every active system, database, and application in your network. Backing up log records for storage must be done at each event source before they are overwritten. Restoring event logs is difficult when backups from different event sources are stored separately.

What makes raw events tedious to interpret is their string format where the event severity does not stand out. Also, similar data from different systems varies.
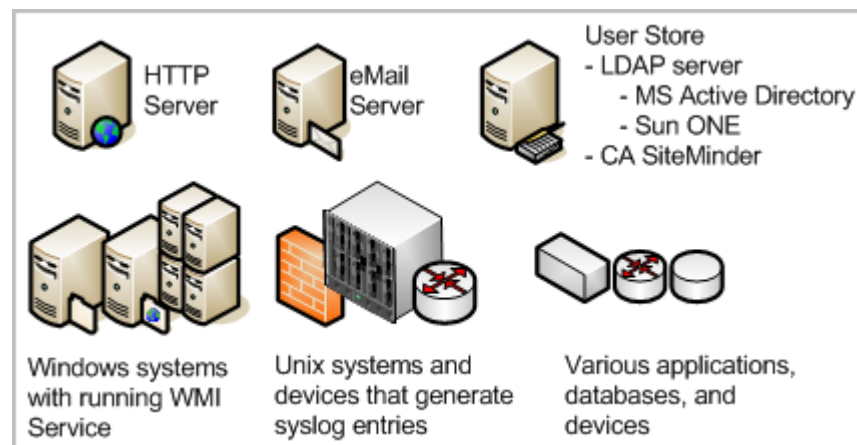
Operational efficiency demands a solution that consolidates all logs, makes logs easy to read, automates archiving to storage, and simplifies log restoration. CA Enterprise Log Manager offers these benefits, and lets you send alerts to individuals and systems when critical events occur.

What You Install

It does not take long to set up a single-server solution and begin collecting events.

The installation disks include these components:

- Operating system (Red Hat Enterprise Linux) for the soft appliance

- CA Enterprise Log Manager Server

- CA Enterprise Log Manager Agent (hereafter referred to as the agent)

In the following illustration, CA Enterprise Log Manager is depicted as a server containing a small server, a dark (green) circle, and a database. The small server represents the local repository that stores application-level content. The dark circle represents the default agent, and the database represents the event log store where incoming event logs are processed and made available to queries and reports.

The dark (green) circles on the collection point and the other event sources represent separately installed agents. Installing agents is optional. You can collect syslogs from UNIX-compatible event sources with the default agent after completing the required configuration.
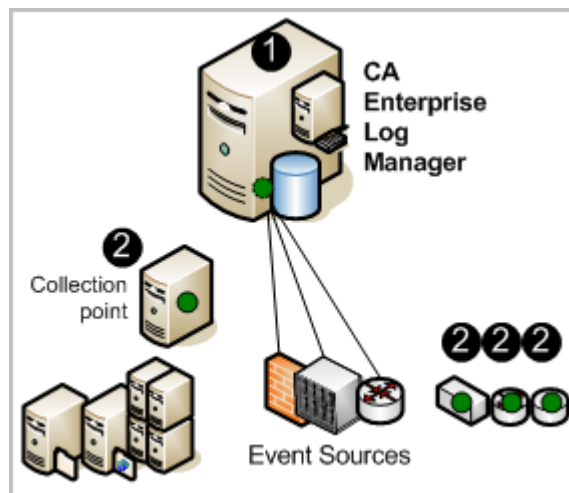
The numbers on the illustration refer to these steps:

1. You install the operating system for the soft appliance and then you install the CA Enterprise Log Manager application. As soon you configure your sources to push syslogs to CA Enterprise Log Manager and indicate the syslog targets in the configuration of the connector for the default agent, syslogs are collected and refined for easy interpretation.

2. (Optional) You can install an agent on a host you dedicate as a collection point or you can install agents directly on the hosts with sources that are generating events you want to collect.

Note: See the *Implementation Guide* for details on installing the soft appliance. See the *Agent Installation Guide* for details on installing agents.

More information:

Chapter 2: Quick Start Deployment

This section contains the following topics:

Quick Start Overview

You can achieve a simple, functioning CA Enterprise Log Manager deployment with one soft appliance. The predefined syslog connector makes it possible for the default agent to receive generated syslog events. All you need to do is configure your syslog sources to push syslog events to CA Enterprise Log Manager and edit the syslog connector configuration to identify the syslog targets. What is received depends on the bandwidth between the server and the syslog sources and latency.

Log sensors, including WinRM and ODBC, support direct log collection from over twenty non-syslog event sources. The WinRM log sensor lets you collect events directly from servers running Windows operating systems, such as Forefront Security for Exchange server, Forefront Security for SharePoint Server, Microsoft Office Communication Server, and Hyper-V virtual server and services such as Active Directory Certificate Services. The ODBC log sensor lets you capture events generated by Oracle9i or SQL Server 2005 databases. For details, see the CA Enterprise Log Manager Product Integration Matrix.

You need EiamAdmin credentials to install CA Enterprise Log Manager. As the EiamAdmin superuser, you configure an Administrator account which you use to do the configuration. If you log on with the Administrator credentials, you can verify that the setup is functioning by viewing self-monitoring events.

Install a Single-Server System

The simplest deployment that lets you view queried events is a single-server system. Be sure to select a machine that meets or exceeds the minimum hardware requirements for a CA Enterprise Log Manager soft appliance.

Note: See the *Release Notes* for the certified hardware list, operating system support, and system software and service requirements.

To install a CA Enterprise Log Manager for a single-server system

1. Have the following information at hand:

   - A password to be used as the root password

   - Host name for your appliance

   - If not using DHCP, the static IP address, subnet mask, and default gateway for your appliance

   - Domain for the appliance

     Note: The domain must be registered with the DNS Servers in your network for the installation to complete.

   - IP addresses of the DNS servers

   - (Optional) IP address of your NTP time server

   - A password for the default installation superuser name, EiamAdmin

   - CAELM.

     This is the default application name for the CA Enterprise Log Manager application.

2. Install the preconfigured operating system using the media you created from the CA Enterprise Log Manager download package. During the operating system installation, do the following:

    a. Choose a keyboard type. The default is U.S.

    b. Choose a time zone, for example, America/New York and select OK.

```
┤ Time Zone Selection ├

 What time zone are you located in?

 [ ] System clock uses UTC

  America/Montevideo          ▪
  America/Montreal            ▪
  America/Montserrat
  America/Nassau
  America/New_York            ▪


        ┌────────┐        ┌────────┐
        │   OK   │        │  Back  │
        └────────┘        └────────┘
```
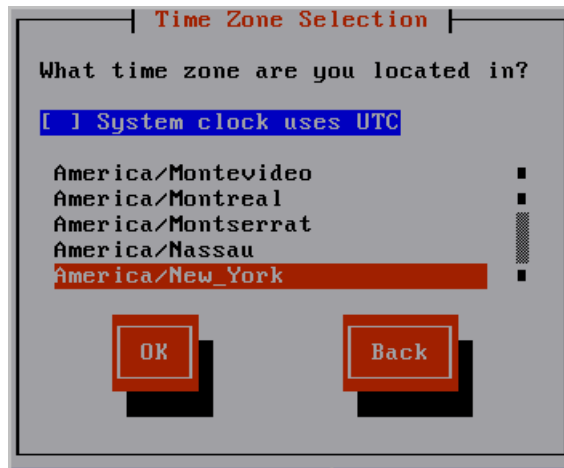
    c. Type the password to be used as the root password, then retype it to confirm. Select OK.

```
┤ Root Password ├

 Pick a root password. You must type it
 twice to ensure you know what it is and
 didn't make a mistake in typing. Remember
 that the root password is a critical part
 of system security!

 Password:           *******_____
 Password (confirm): *******_____

        ┌────────┐        ┌────────┐
        │   OK   │        │  Back  │
        └────────┘        └────────┘
```
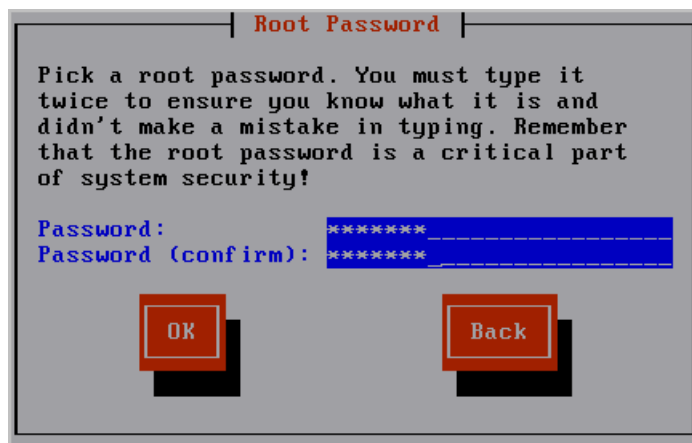
Installation progress information appears.

d. Remove the operating system installation disc and press Enter to reboot the system.

```
┤ Complete ├

Congratulations, your Red Hat Enterprise Linux Server
installation is complete.

Remove any media used during the installation process
and press <Enter> to reboot your system.


            ┌─────────┐
            │ Reboot  │
            └─────────┘
```

The system reboots and enters non-interactive startup. It displays messages describing installation progress. Detailed information about this installation is saved in the following file: /tmp/pre-install_ca-elm.log.

The following prompt appears:

`Please insert the CA Enterprise Log Manager r12 - Application Install disk and press enter.`

3. Insert the CA Enterprise Log Manager Application disc. Press Enter.

Your system is reviewed for whether it meets the minimum recommended specifications for optimal performance. If it does not, a prompt appears asking whether you want to stop the installation process.

The following prompt appears:

`Please enter a new hostname :`

4. Enter the host name for this CA Enterprise Log Manager soft appliance. For example, enter CALM1.

5. Accept the default device, eth0. Press Enter to go to the next screen.

```
┤ Select A Device ├

eth0 (eth0) - Advanced Micro Devices [AMD] 79c970 [PCnet32 LANCE]
<New Device>


        ┌───────┐                        ┌────────┐
        │ Quit  │                        │ Cancel │
        └───────┘                        └────────┘
```
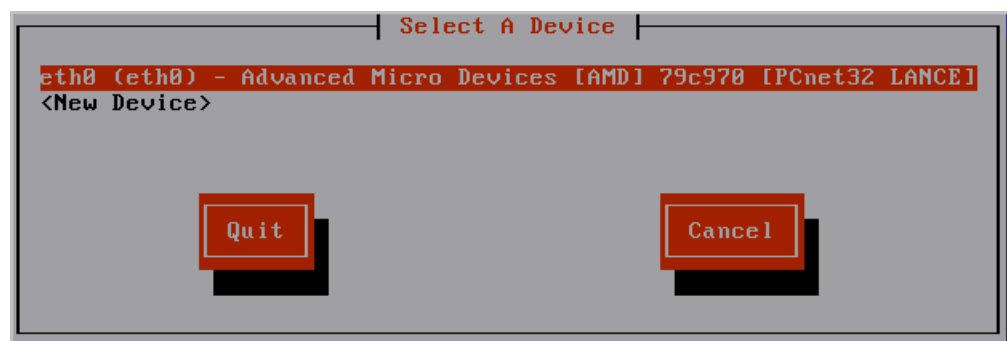
6. Do one of the following and then select OK.

   ■ Select Use DHCP, an acceptable option only for a standalone test system.

   ■ Enter the static IP address, subnet mask, and default gateway IP address to be associated with the hostname you entered.

```
┤ Devernet Configuration ├

Name              eth0_____
Device            eth0_____
Use DHCP          [ ]
Static IP         255.255.255.255_____
Netmask           255.255.255.0_____
Default gateway IP _____

        Ok                    Cancel
```
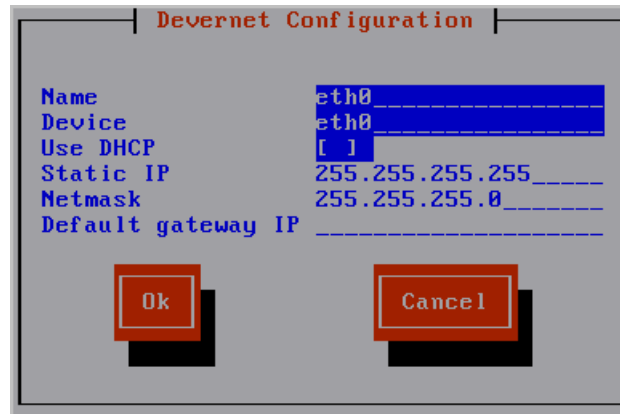
The network services are restarted with the new settings, which are displayed.

The following message appears:

```
Do you want to change the network configuration? (n):
```

7. Review the network settings. If satisfactory, type n, or press Enter, when the message appears allowing you to change the network settings.

The following message appears:

```
Please enter the domain name for this system :
```

8. Enter your domain name, such as <yourcompany>.com.

The following message appears:

```
Please enter a comma separated list of DNS servers to use:
```

9. Enter the IP addresses of your internal DNS servers separated by commas with no spaces.

Your system date and time is displayed with the following message:

```
Do you want to change the system date and time? (n)
```

10. Review the displayed system date and time. If satisfactory, type n or press Enter.

The following message appears:

```
Do you want to configure the system to update the time through NTP?
```

11. If you want to use a Network Time Protocol (NTP) server, continue as follows. Otherwise, specify no and continue with the next step.

    a. Respond yes to the message.

       If you specify yes, the following message appears:

       ```
       Please enter the NTP Server name or IP Address
       ```

    b. Enter the host name or the IP address of the NTP server.

       A confirmation message similar to the following appears: "Your system has been configured to update the time at midnight using the NTP server located at <yourntpserver>."

12. Read the end user license agreements (EULAs) presented and respond as follows:

    a. Read the EULA for the Sun Java Development Kit (JDK).

       At the end of the EULA, the following message appears:

       ```
       Do you agree to the above license terms? [yes or no]
       ```

    b. Type yes if you agree to the terms.

       Product registration information is displayed followed by this message:

       ```
       Press Enter to continue.....
       ```

    c. Press Enter.

       Messages state that in preparation for CA Enterprise Log Manager installation, the system settings are being configured. The CA end user license agreement displays.

    d. Read the CA EULA.

       At the end of the license, the following message appears:

       ```
       Do you agree to the above license terms? [Yes or no]:
       ```

    e. Type Yes if you agree to the license terms.

       CA EEM server information appears.

13. Respond to the following prompts to configure CA EEM.

    ```
    Do you use a local or remote EEM server?
    Enter l (local) or r (remote) :
    ```

    a. To create a standalone test system, enter l for local.

       ```
       Enter the password for the EEM server EiamAdmin user :
       Confirm the password for the EEM server EiamAdmin user :
       ```

    b. Type the password you want to assign to the EiamAdmin default superuser; type it again.

       ```
       Enter an application name for this CAELM server (CAELM):
       ```

c.   Press Enter to accept CAELM, the default application name for CA Enterprise Log Manager.

The EEM Server information you entered so far appears with a message that asks if you want to make changes.

```
EEM server is not installed on the local host.

EEM Server Information:
EEM Server Type - l (local) or r (remote): l
EEM Server Name: CALM1
EEM application name for this CAELM server: CAELM
Do you want to change the EEM Server information? (n): _
```

d.   Press Enter or enter n for no to accept the CA EEM server information you entered.

The installation process begins. Messages appear showing the progress as each CA Enterprise Log Manager component is successfully installed, registrations completed, certificates acquired, files imported, and components configured. The message CA ELM Installation succeeded appears. When the installation completes, the system displays the console logon address.

14.   Respond to the following prompt:

```
Do you want to run CAELM Server in FIPS mode?
Enter Yes or No
```

If you enter y, the CA Enterprise Log Manager server will start up in FIPS mode. If you enter n, it will start up in non-FIPS mode.

15.   Make note of this address. This is the address you enter in a browser to access this CA Enterprise Log Manager server. That is, https://<hostname>:5250/spin/calm.

A <hostname> login prompt appears. You can ignore this.

Note: If, for any reason, you want to display the operating system prompt from this login prompt, you can do so by entering caelmadmin and the default password, which is the password you assigned to the EiamAdmin user account. You use the caelmadmin account to log in to the appliance on the console or through SSH.

16.   Continue as follows:

■   If you configured a static IP address, be sure to register this IP address with the DNS servers specified in step 9.

■   If you configured DHCP, update your hosts file on the machine from which you intend to browse to this server.

■   Browse to the URL you made note of in step 14 and configure the first Administrator.

Update Your Windows Hosts File

During CA Enterprise Log Manager installation, you can identify one or more DNS servers or select Use DHCP. If you selected DHCP, you must update your Windows hosts file on the computer from which you plan to access the CA Enterprise Log Manager with your browser.

To update your hosts file on the host with your browser

1. Open Windows Explorer and navigate to C:\WINDOWS\system32\drivers\etc.

2. Open the hosts file with an editor, for example, Notepad.

3. Add an entry with the IP address of the CA Enterprise Log Manager server and the corresponding hostname.

4. Select Save from the File menu, then close the file.

Configure the First Administrator

After installing a single-server CA Enterprise Log Manager, you prepare for configuration by browsing to the URL of the CA Enterprise Log Manager from a remote workstation, logging on, and creating an Administrator account you can use to perform the configuration.

Note: For the purpose of this Quick Start deployment, we accept the default user store, and the default password policies. Typically, these are configured before adding the first Administrator.

To configure the first Administrator

1. Connect to the following URL from your browser, where hostname is either the host name or IP address of the server where you installed the CA Enterprise Log Manager.

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

2. If a security alert appears, do the following:

   a. Click View Certificate.

   b. Click Install Certificate, accept the defaults, and finish the import wizard.

      A security warning appears stating you are about to install a certificate claiming to represent the host name of the CA Enterprise Log Manager server.

   c. Click Yes.

      The root certificate is installed and a successful import message appears.

   d. Click OK.

      The trusted certificate dialog appears.

   e. (Optional) Click the Certification Path and verify the certificate status says this certificate is OK.

   f. Click OK, and then click Yes.

      The logon page appears.

3. Log on with the EiamAdmin user name and the password you creating when you used to install the software. Click Log In.
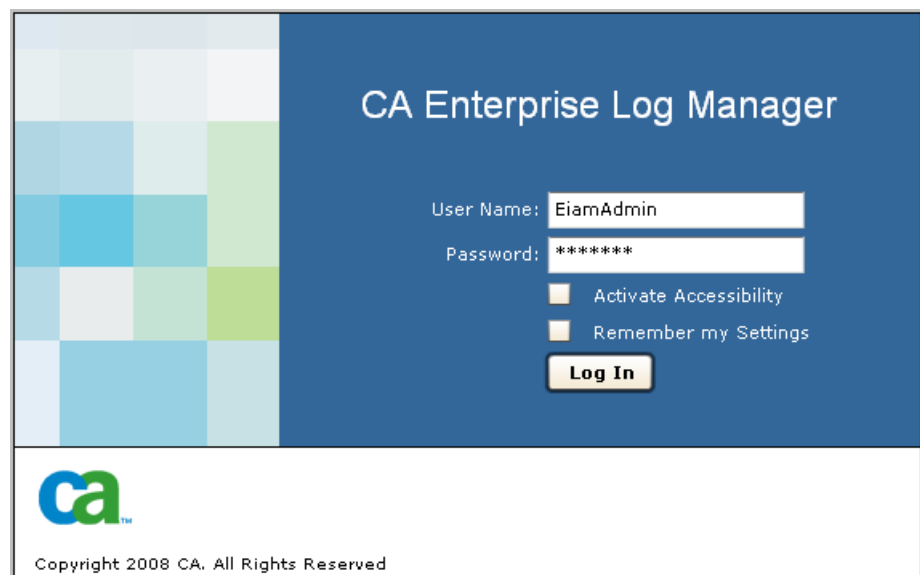
The application opens with only the Administrator tab and the User and Access Management subtab active.

4. Click Users.

5. Click Add New User.
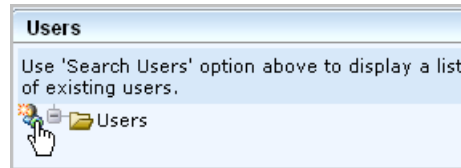
6. Enter your name in the Name field and click Add Application User Details.

7. Select Administrator and move it to the Selected User Groups list.

8. Under Authentication, enter a password for this new account in the two fields for entry and confirmation.

9. Click Save and then click Close. Click Close.

10. Click the Log out link on the toolbar.

   The logon page appears.

11. Log back into CA Enterprise Log Manager with the Administrator credentials you just defined.

   CA Enterprise Log Manager opens with all functionality enabled. The Queries and Reports tab and Queries subtab is displayed.

12. (Optional) View your login attempts as follows:

    a.   Select the System Access from the query tag list.

    b.   Select System Access Detail from the query list.

The query results show your two login attempts, first as EiamAdmin, then with your Administrator name where the login attempts are marked with S for successful.

CA Severity	Date	Ac...	Performer	Host	Log Na...	Category	Action	Result
● Information	Wed Oct 8 2008 09:30:37 AM		EiamAdmin		CALM	System Access	Login Attempt	S
● Information	Wed Oct 8 2008 09:31:38 AM			127.0.0.1	EiamSdk	System Access	Login Attempt	S
● Information	Wed Oct 8 2008 09:31:38 AM			127.0.0.1	EiamSdk	System Access	Authorization	S
● Information	Wed Oct 8 2008 09:31:48 AM		Administrator1		CALM	System Access	Login Attempt	S

Configure Syslog Event Sources

To enable direct collection of syslog events by the default agent that exists on each CA Enterprise Log Manager server, you begin by identifying the syslog event sources from which you want to collect events and determining the associated integration. Then you do the following two things in either order.

- Configure the syslog event sources. Log on to each host where a syslog event source is running and configure it as documented in the connector guide for that syslog integration.

- Configure the syslog connector on the default agent to add the target syslog integrations associated with the configured event sources.

As soon as you complete this two-step configuration, event collection and refinement begins. Then, you can use CA Enterprise Log Manager to view or report on events you care about in a standardized format. You can also generate alerts when specific events occur.

To configure a selected syslog event source

1. Log on to the host with a target syslog event source.

2. Launch CA Enterprise Log Manager from a browser on this host.

3. Click the Administration tab and Log Collection subtab.

The Log Collection Explorer appears.

4. Expand Event Refinement Library, Integrations, Subscription.

The list of predefined integrations displays. An abbreviated example follows:
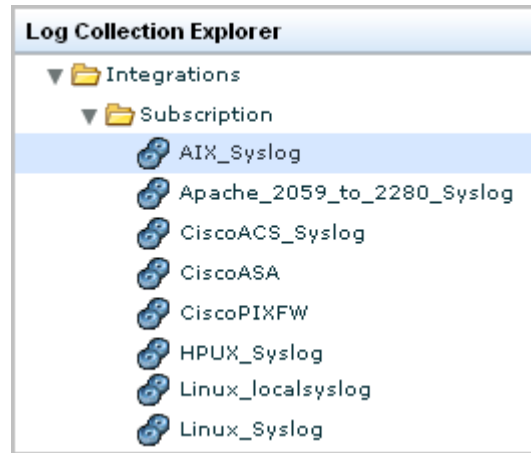
5. Select the integration for the event source you need to configure. For example, if you wanted to collect syslogs generated by an AIX operating system, you would select AIX_Syslog.

The integration details appears.
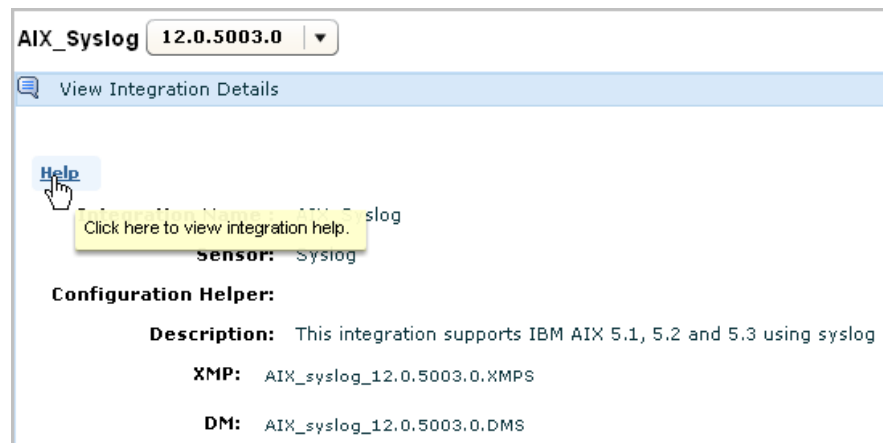
6. Click the Help button located just above the Integration name on the right hand pane.

The connector guide for the selected integration appears.

7. Click the section on the event source configuration requirements. In this example, the documentation describes how to configuring the AIX operating system event source to send its syslogs to CA Enterprise Log Manager.

1.0 Connector Guide for AIX

2.0 Prerequisites

3.0 AIX Configuration
3.1 Configure the Syslog File
3.2 Write a PERL Script
3.3 Enable Auditing
  3.3.1 Shut Down Auditing
  3.3.2 Configure the Audit Directory Files
    3.3.2.1 Configure the Objects File
    3.3.2.2 Configure the Config File
    3.3.2.3 Configure the Streamcmds File
  3.3.3 Modify the /etc/rc File
  3.3.4 Modify the /etc/shutdown File
  3.3.5 Start Auditing

Example--Alternative Source for Connector Guides: Support Online

You can open a selected connector guide from within the CA Enterprise Log Manager user interface or from CA Support Online. Following is an example that shows how to open a connector guide from this alternative source.

1. Log on to CA Support Online.

2. Select CA Enterprise Log Manager from the Select a Product page drop-down list.

3. Scroll to Product Status and select CA Enterprise Log Manager Certification Matrix.

4. Select Product Integration Matrix.

5. Find the category for the integration associated with the event source you are configuring. For example, if the event source is the AIX operating system, scroll to the Operating Systems category and click the AIX link.

Product	Version	Log Sensor
Operating Systems		
AIX	5.1 5.2 5.3	syslog

Edit the Syslog Connector

Each CA Enterprise Log Manager has a default agent. When a CA Enterprise Log Manager is installed, its default agent has a partially configured connector called Syslog_Connector, which is based on the listener, Syslog. This listener receives raw syslog events on the default ports as soon as you configure the event sources to send syslogs to CA Enterprise Log Manager. However, for CA Enterprise Log Manager to refine these raw events, you must edit this Syslog_Connector. Certain edits are mandatory; others are optional.

■ You must identify the syslog targets when you edit this connector. You select as syslog targets each integration that corresponds to one or more event sources you have configured or plan to configure. Your identification of syslog targets enables CA Enterprise Log Manager to properly refine the events.

■ Optionally, you can apply suppression rules, limit the acceptance of syslogs to trusted hosts, specify ports to listen on other than 514, the well-known syslog UDP port, and 1468, the default TCP port, and/or add a new time zone for a trusted host.

To edit the syslog connector for a default agent

1. Click the Administration tab.

   The Log Collection subtab is displayed.

2. Expand Agent Explorer and then expand the Default Agent Group or the user-defined group with the CA Enterprise Log Manager to be configured.

3. Select the name of a CA Enterprise Log Manager server.

   The connector named Syslog_Connector is displayed.

Connectors			
☐	**Connector Name**	**Integration**	**Edit**
☐	Syslog_Connector	Syslog	✏️ Edit

4. Click Edit.

   The Edit Connector wizard appears with the Connector Details step selected.

5. (Optional) Click Apply Suppression Rules. If there is any syslog event type that you want suppressed, that is, *not* collected, move that event type from the available list to the selected listed. Select the event to move and click the move button.

6. Click the Connector Configuration step.

   All available integrations are selected by default.

7. Select syslog targets by moving the syslog integrations to target from the available list to the selected list.

   For example, if you have configured the AIX operating system on a host in your network, you would move the syslog target, AIX_Syslog, from the available list to the selected list.
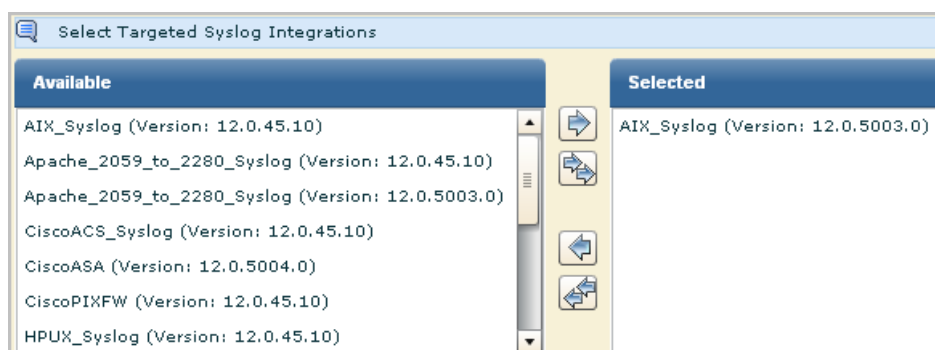
8. (Optional) Identify the trusted hosts from which the syslog connector is to accept incoming events. Enter the IP address in the entry field and click Add. Repeat for each trusted host. Then, when an event is received from a host not configured as trusted, that event is rejected.

   Note: It is a good practice to configure trusted hosts. Typically, you configure all the hosts on which you have configured event sources to send syslogs to CA Enterprise Log Manager. Specifying trusted hosts ensures the default agent does not accept events from rogue systems that an attacker has configured to send events to the syslog listener.

9. (Optional) Add ports.

   You can typically accept the default UPD and TCP ports for the default agent.

   Note: You can gain performance improvements by defining a syslog connector for different event types and specifying different ports for each. Be sure to select unused ports when making new port assignments.

10. (Optional) Add a time zone only if collecting syslogs from machines in a different time zone from the soft appliance.

    a. Click Create Folder and expand the folder.

    b. Highlight the blank entry under the folder. Enter the IP address of either a trusted host you configured for this connector or the NTP time server you specified at installation of the CA Enterprise Log Manager.
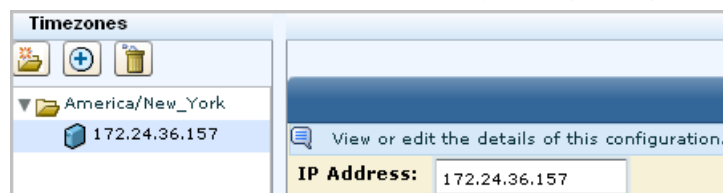
11. Click Save and Close.

12. View the status.

   a. Click Status and Command

   View Status of Agents is selected. The host name of the server you installed appears in the Agent column, since the default agent is on this server. The status is shown as running.

   b. Click the Running link to view details.

   c. Click the Connectors button to view the status of connectors.

   d. Click the Running link.

   The percentage CPU, memory usage, average events per second (EPS), and filtered event count appear.

View Syslog Events

One of the quickest ways to view query results on events collected by a syslog listener is to use the Prompt for Host.

To view syslog events

1. Select the Queries and Reports tab.

   The Queries subtab displays.

2. Expand Prompts under Query List and select Host.
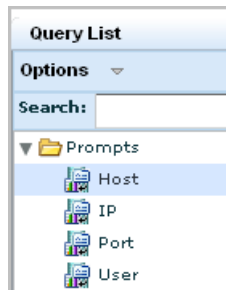
3. Submit a query for events collected by the default agent.

   a. Enter the default agent host name in the Host field, which is also the name of the CA Enterprise Log Manager on which it resides.

   b. Select agent_hostname.

   c. Click Go.

▲ Prompt Filters

💬 Enter the prompt values and check all the CEG Columns which apply

● **Host:** LogManager02   [Go]

☐ **source_hostname**   ☐ **dest_hostname**   ☐ **event_source_hostname**   ☐ **receiver_hostname**
☑ **agent_hostname**

4. Display the results to examine.

   a. Click the Results column to sort by results.

   b. Scroll to the first result of F for failure. Assume it is a configuration warning in the category Configuration Management.

   c. Double-click to select the row to view in detail.

   The Event Viewer appears.

5. Scroll to the area where the Result is displayed. In the example, the error is a warning that you need to configure the subscription module. This is a warning you should ignore until you have finished installing all of the CA Enterprise Log Manager servers you plan to install.

Event Viewer - Event Details - Host   ☒

☑ Hide empty rows   [Copy]

Show	Name	Value
☑	event_result	F
☐	result_string	No modules are selected for getting updates. Please select the modules for getting the updates from the Subscription server.
☐	event_source_address	127.0.0.1
☐	event_source_hostname	LogManager02
☑	agent_hostname	LogManager02
☐	agent_name	Subscription
☐	agent_version	12.0.44.2

■ Source	■ Destination	■ Event
■ Result	■ Event Source	■ Agent

[Close]

Chapter 3: Windows Agent Deployment

This section contains the following topics:

Create a User Account for the Agent

Before installing an agent on a Windows operating system, you create a new account for the agent in the Windows Users folder. The purpose of creating this low-privileged account for the agent is to allow it to run with the lowest possible privileges. You supply the user name and password you create here when you install the agent.

Note: You can bypass this step and specify the domain credentials of an Administrator for the agent when you do the installation, but this is not considered a good practice.
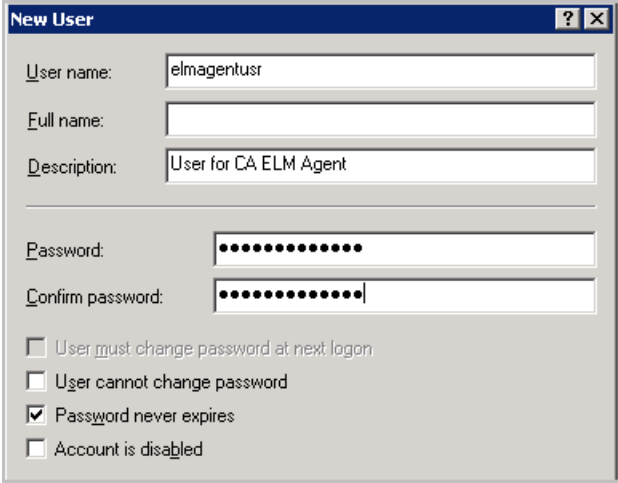
To create a Windows user account for the agent

1. Log on to the host where you plan to install the agent. Use Administrative credentials.

2. Click Start, Program Files, Administrative Tools, Computer Management.

3. Expand Local Users and Groups.

4. Right-click Users and select New User.

   The Windows dialog, New User appears.

5. Enter a user name and enter a password twice. A strong password has mix of alpha, numeric, and special characters. For example, calmr12_agent. Optionally, enter a description.

   Important! Remember this name and password or record it. You will need to enter it when you install the agent.

6. Click Create. Click Close.

More information:

Install an Agent (see page 35)

Set the Agent Authentication Key

Before you install the first agent, you must know the agent authentication key. You can use the default, if no key has been set, use the current key, if one is set, or set a new key. The agent authentication key configured here must be entered during the installation of each agent. Only an Administrator can perform this task.

To set the agent authentication key

1. Open the browser on the host where you plan to install the agent and enter the URL for the CA Enterprise Log Manager server for this agent. An example follows.

    ```
    https://<IP address>:5250/spin/calm/
    ```

2. Log on to the CA Enterprise Log Manager. Enter your name and password and click Logon.

3. Click the Administration tab.

    The Log Collection Explorer displays in the left pane.

4. Select the Agent Explorer folder.

    A toolbar appears in the main pane.

5. Click Agent Authentication Key
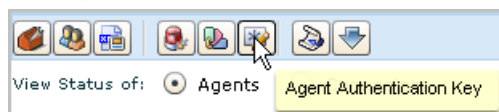
6. Enter the agent authentication key to be used for agent installation or take note of the current entry.

    Important! Remember or record this key. You will need it to install the agent.

7. Click Save.

8. Continue with the next step, Download the Agent Installation Program.

Download the Agent Installation Program

If you just set the agent authentication key, you are positioned to download the agent installation program onto the desktop.

To download the agent installation program

1. Click Download Agent binaries from the toolbar displayed for Agent Explorer.
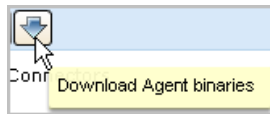
   Links for the available agent binaries appear in the main pane.

2. Click the Windows link to install the agent on a server with a Window Server 2003 operating system.

   The dialog, Select location for download by <IP address>, appears.

3. Select the desktop and click Save.

   A message showing the progress of the download of the selected agent binary appears, followed by a confirmation message.

4. Click OK.

5. Minimize the browser but leave the connection open so you can quickly verify the installation after it completes.

   The Setup Launcher for the agent installation program appears on the desktop.
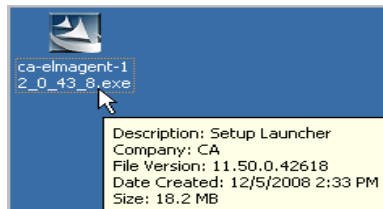
Install an Agent

Before you begin, have at hand the following:

■ IP address of the CA Enterprise Log Manager server from which you downloaded the agent program

■ User name and password from the user account you created for the agent

■ Agent authentication key you set

To install an agent for a Windows host

1. Double-click the agent installation launcher.

    The installation wizard starts.

2. Click Next, read the license, click I accept the terms in the license agreements to continue, and click Next.

3. Accept the installation path or change it and click Next.

4. Enter the requested information as follows:

    a. Enter the hostname for the CA Enterprise Log Manager to which this agent is to forward the logs it collects.

        Note: Since the CA Enterprise Log Manager in this example scenario uses DHCP for IP address assignment, you should not enter the IP address here; doing so introduces the risk of having to reinstall the agent if the IP address of the server ever changes.

    b. Enter the agent authentication key.

    An example follows:
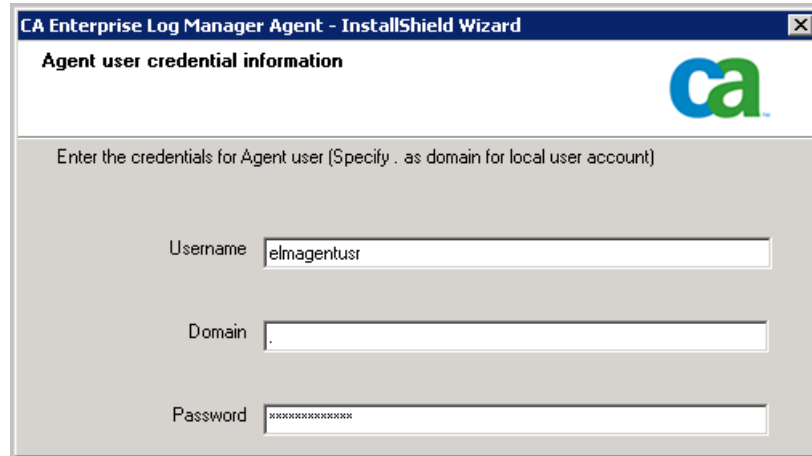
5. Enter the name and password defined in the user account you set up for the agent and then click Next.

6. Click Next. Specifying an exported connector file is optional.

   The Start Copying Files page appears.

7. Click Next.

   The agent installation process completes.

8. Click Finish.

9. Continue with configuring connectors for this agent.

   After connectors are configured, the collected events are sent to the CA Enterprise Log Manager Event Log Store through port 17001.

   Important! If you do not allow outgoing traffic from the host on which you installed the agent and you use the Windows Firewall, you need to open this port on your Windows Firewall.

More information:

Create a Connector Based on NTEventLog

After installing an agent, you create a connector to specify the event sources for the events you want to collect. Since you installed an agent on a server with a Windows operating system, you create a connector based on the NTEventLog integration and specify settings for the WMILogSensor as described in the connector guide you open from the New Connector Creation wizard. You specify the name of the host on which the agent is installed for agent-based log collection. Optionally, you can add another WMI log sensor for this connector and specify a host other than the one where the agent is installed. This enables agentless log connection. The additional host or hosts must be in the same domain and have the same Windows administrator as the first host you added.

To configure a connector based on NTEventLog

1. Maximize your browser displaying the CA Enterprise Log Manager Agent Explorer.

2. Expand Agent Explorer and then expand the Default Agent Group.

    The name of the computer where you installed the agent appears.

3. Select this agent.

    The Agent Connectors pane appears.

4. Click Create New Connector
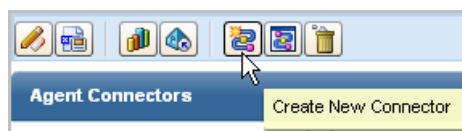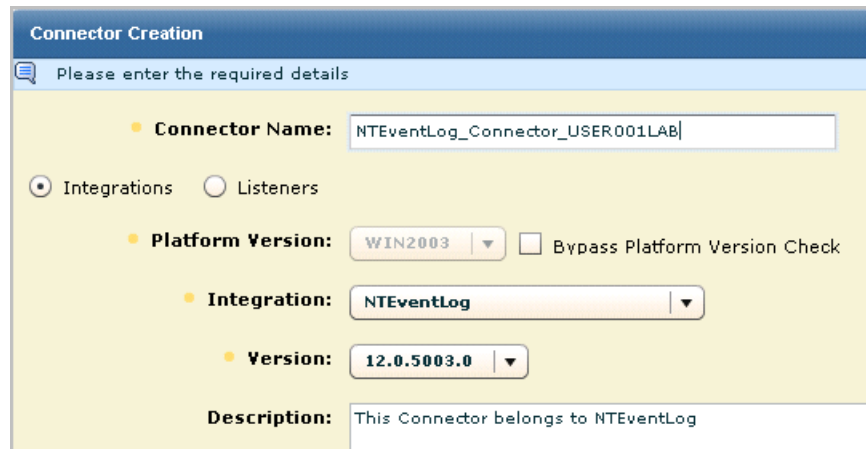
    The New Connector Creation wizard appears with the Connector Details step selected.

5. Leave Integrations selected, and select NTEventLog from the Integration drop-down list.

    The Connector Name and Description fields are populated based on the selection of Integration.

6. Edit the connector name to make it unique. Consider extending this name with the target server name, for example, NTEventLog_Connector_USER001LAB.

7. Select the Connector Configuration step.

The Sensor Configuration pane appears with a Help button to the Connector guide for NTEventLog, which provides help on the fields for sensor configuration.

8. Click the display details button for WMI sources.
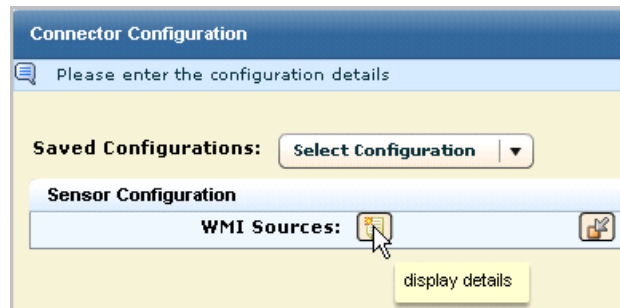
9. Configure the WMILogSensor settings for the local computer for agent-based log collection. Click the Help link for details.

    The following example shows a configuration where the user is a Windows administrator on the specified WMI server. The domain is for the WMI server.

WMI server name:	USER001LAB
User name:	user001
Password:	**********
Domain:	ca.com
Namespace:	root\cimv2
Event Log Name:	NT
UpdateAnchorRate:	100

10. (Optional) Configure a WMI sensor for a different computer for agentless log collection using this same connector.

    a. Click the repeat super node button.

        The following illustration shows a configuration with two WMI sources.

        Sensor Configuration

        WMI Sources:

        WMI Sources: repeat super node
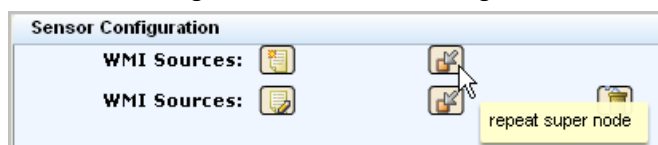
    b. Configure the WMILogSensor settings for another computer.

    The following example shows a configuration for a second WMI log sensor in the same domain and with the same administrator credentials.

WMI server name:	USER001XP
User name:	user001
Password:	**********
Domain:	ca.com
Namespace:	root\cimv2
Event Log Name:	NT
UpdateAnchorRate:	100

11. Click Save and Close.

12. To view the status of the connector you configured, do the following:

    a. Select the agent in the left pane.

    b. Click Status and Command.

    c. Select View Status of Connectors.

    The Status Details pane appears.

Status Details						
Select and:	Restart	Start	Stop			
Select	**Connector**	**Agent**	**Agent Group**	**Platform**	**Integration**	**Status**
☐	NTEventLog_Connector_USER001LAB	USER001LAB.ca.com	Default Agent Group	Windows_X86_32	NTEventLog	Running

13. Click the Running link.

    The displayed status of the target configured in the connector includes the CPU percentage, memory usage, and average events per second (EPS).

Configure a Windows Event Source

After configuring a connector using the NTEventLog integration on the agent, you should be able to see events through your Event Viewer. If events are not being forwarded to your event viewer, you should change the Windows settings for your Local Policies on the event source.

To configure local policies on the event source for a NTEventLog connector

1. If the Log Collection Explorer is not already displayed, click the Administration tab.

2. Expand Event Refinement Library, expand Integrations, expand Subscription, select NTEventLog, and click the Help link above the Integration Name on the View Integration Details pane.

   The Connector Guide for NT Event Log (Security, Application, System) appears.

3. Minimize the CA Enterprise Log Manager user interface and follow the directions in the Connector Guide for editing local policies on an event source running on a Windows operating system.

   Note: If your system is Windows Server 2003, select Control Panel, Administrative Tools, Local Security Policy, and then expand Local Policies.

4. (Optional) If you configured a WMI Sensor for a second WMI server, edit the local policies on that server also.

5. Maximize CA Enterprise Log Manager.

View Logs from Windows Event Sources

One of the quickest ways to view query results on incoming events is to use the Prompt for Host. You can also select queries or reports.

To view incoming event logs

1. Select the Queries and Reports tab.

    The Queries subtab displays.

2. Expand Prompts under Query List and select Host.

3. Enter the WMI server name configured for the sensor in the Host field. Clear the other check marks and click Go.

▲ Prompt Filters
📰 Enter the prompt values and check all the CEG Columns which apply

Host:	USER001LAB	Go

☐ source_hostname	☐ dest_hostname	☑ event_source_hostname	☐ receiver_hostname
☐ agent_hostname			

Events from the WMI server event sources appear.

4. Click the CA Severity and scroll through to find a warning. A compressed example without the Date and Event Source columns follows:

CA Severity ▼	Source User	Result	Category	Action	Log Name
⚠ Warning	calm_agent	S	System Access	Privilege Use	NT-Security

5. Click Show raw event to display the raw events for the warning.

6. Double-click the warning to display the Event Viewer with much more data. A few rows of example data follow:

Event Viewer - Event Details - Host		
☑ Hide empty rows		
Show	**Name**	**Value**
☑	event_result	S
☐	result_string	Privileged object operation
☑	event_source_hostname	USER001LAB
☐	event_source_processname	Privilege Use
☐	agent_connector_name	NTEventLog_Connector_USER001LAB

7. Click the Queries and Reports tab, click a query from the Query List, for example, Collection Monitor by Log Manager Trend. View the resulting bar graph.
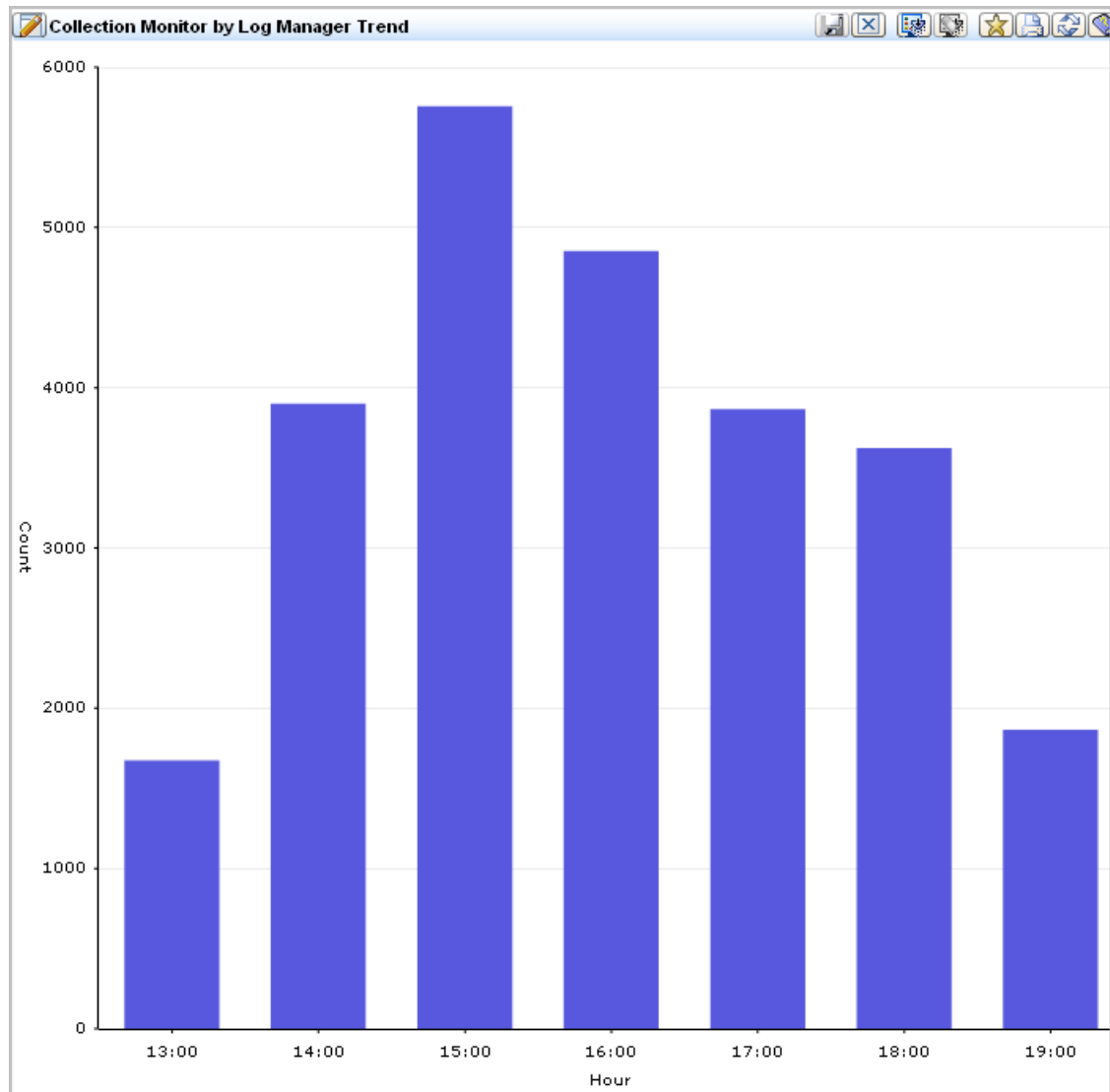
8. Click Reports. Under Report List, enter self in the Search field to display the report name System Self Monitoring Events. Select this report to display a listing of the events that are generated by the CA Enterprise Log Manager server.

Note: See online help or the *Administration Guide* for details on scheduling reports on information you are interested in analyzing.

Chapter 4: Key Capabilities

This section contains the following topics:

Log Collection

The CA Enterprise Log Manager server can be set up to collect logs using one or more supported techniques. The techniques differ in the type and location of the component that listens for and collects the logs. These components are configured on agents.

The following illustration depicts a single-server system, where agent locations are indicated with a dark (green) circle.
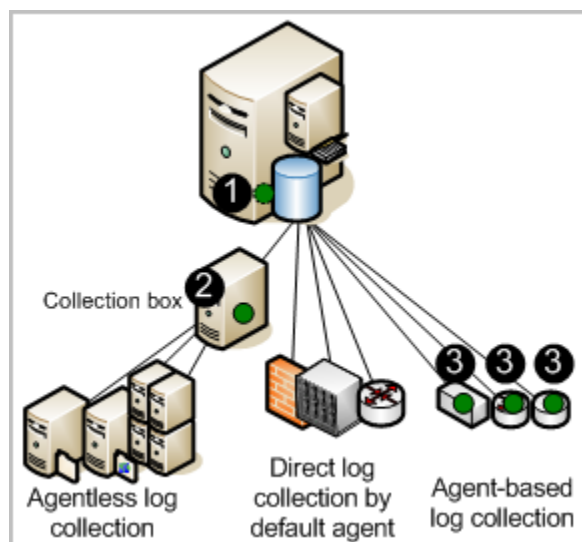
The numbers on the illustration refer to these steps:

1. Configure the default agent on the CA Enterprise Log Manager to fetch events directly from the syslog sources you specify.

2. Configure the agent installed on a Windows collection point to collect events from the Windows servers you specify and transmit them to the CA Enterprise Log Manager.

3. Configure agents installed on hosts where event sources are running to collect the configured type of events and perform suppression.

Note: Traffic from the agent to the destination CA Enterprise Log Manager server is always encrypted.

Consider the following advantages of each log collection technique:

- Direct log collection

  With direct log collection, you configure the syslog listener on the default agent to receive events from the trusted sources you specify. You can also configure other connectors to collect events from any event source that is compatible with the soft appliance operating environment.

  Advantage: You do not need to install an agent to collect logs from event sources that are in close network proximity to the CA Enterprise Log Manager server.

- Agentless collection

  With agentless collection, there is no local agent on the event sources. Rather, an agent is installed on a dedicated collection point. Connectors for each target event source are configured on that agent.

  Advantage: You can collect logs from event sources running on servers where you cannot install agents, such as severs where corporate policy prohibits agents. Delivery is guaranteed, for example, when ODBC log collection is configured properly.

- Agent-based collection

  With agent-based collection, an agent is installed where one or more event sources are running and a connector is configured for each event source.

  Advantage: You can gather logs from a source where the network bandwidth between that source and the CA Enterprise Log Manager is not good enough to support direct log collection. You can use the agent to filter the events and reduce the traffic sent across the network. Event delivery is guaranteed.

Note: See the *Administration Guide* for details on agent configuration.

Log Storage

CA Enterprise Log Manager provides managed embedded log storage for recently archived databases. Events collected by agents from event sources go through a storage lifecycle as illustrated by the following diagram.
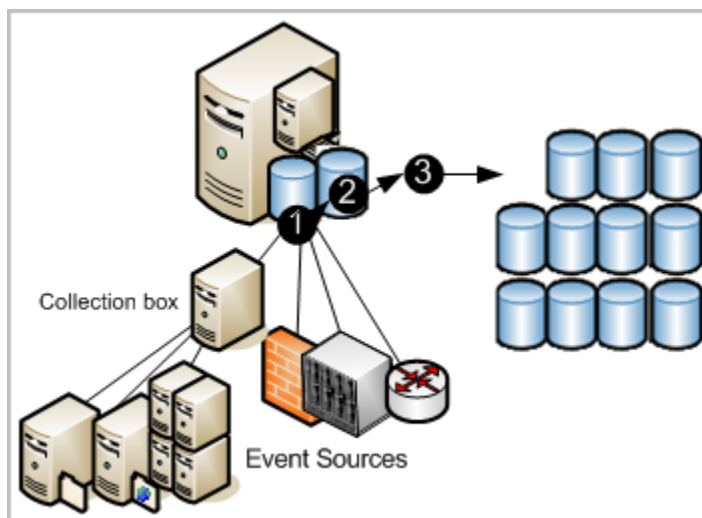
The numbers on the illustration refer to these steps:

1. New events collected by any technique are sent to the CA Enterprise Log Manager. The state of incoming events depends on the technique used to collect them. Incoming events must be refined before being inserted into the database.

2. When the database of refined records reaches the configured size, all records are compressed into a database and saved with a unique name. Compressing log data reduces the cost of moving it and reduces the cost of storage. The compressed database can either be moved automatically based on auto-archive configuration or you can back it up and move it manually before it reaches the age configured for deletion. (Auto-archived databases are deleted from the source as soon as they are moved.)

3. If you configure auto-archive to move the compressed databases to a remote server on a daily basis, you can move these backup to off-site long-term log storage at your convenience. Retaining backups of logs enables you to comply with the regulations that state that logs must be securely collected, centrally stored for a certain number of years, and available for review. (You can restore database from long-term storage at any time.)

Note: See the *Implementation Guide* for details on configuring the event log store, including how to set up auto-archiving. See the *Administration Guide* for details on restoring the backups for investigation and reporting.

Standardized Presentation of Logs

Logs generated by applications, operating systems, and devices all use their own formats. CA Enterprise Log Manager refines the collected logs to standardize the way the data is reported. The standard format makes it easier for auditors and upper management to compare data collected from different sources. Technically, the CA Common Event Grammar (CEG) helps implement event normalization and classification.

The CEG provides several fields which are used to normalize various aspects of the event, including the following:

- Ideal Model (Class of technologies such as antivirus, DBMS, and firewall)

- Category (Examples include Identity Management and Network Security)

- Class (Examples include Account Management and Group Management)

- Action (Examples include Account Creation and Group Creation)

- Results (Examples include Success and Failure)

Note: See the *CA Enterprise Log Manager Administration Guide* for details on the rules and files used in event refinement. See the section on Common Event Grammar in the online help for details on the normalizing and categorizing events.

Compliance Reporting

CA Enterprise Log Manager lets you gather and process security-relevant data and turn it into reports suitable for internal or external auditors. You can interact with queries and reports for investigations. You can automate the reporting process by scheduling report jobs.

The system provides:

- Easy to use query capability with tags

- Near-real time reporting

- Centrally searchable, distributed archives of critical logs

Its focus is on compliance reporting rather than real-time correlation of events and alerts. Regulations demand reporting that demonstrates compliance with industry-related controls. CA Enterprise Log Manager provides reports with the following tags for easy identification:

- Basel II

- COBIT

- COSO

- EU Directive - Data Protection

- FISMA

- GLBA

- HIPAA

- ISO\IEC 27001\2

- JPIPA

- JSOX

- NERC

- NISPOM

- PCI

- SAS 70

- SOX

You can review predefined log reports or perform searches based on criteria you specify. New reports are provided with subscription updates.

Log view capabilities are supported by the following:

- On demand query capability with predefined or user-defined queries, where results can include up to 5000 records

- Quick search, through Prompts, for a specified host name, IP address, port number, or user name

- Scheduled and on demand reporting with out-of-the-box reporting content

- Scheduled query and alerting

- Basic reports with trending information

- Interactive, graphical event viewers

- Automated reporting with email attachment

- Automated report retention policies

Note: For details on using predefined queries and reports or creating your own, see the *CA Enterprise Log Manager Administration Guide*.

Policy Violation Alerting

CA Enterprise Log Manager lets you automate the sending of an alert when an event occurs that requires near-term attention. You can also monitor action alerts from CA Enterprise Log Manager at any time by specifying a time interval, such as from the last five minutes to the last 30 days. Alerts are automatically sent to an RSS feed that can be accessed from a web browser. Optionally, you can specify other destinations, including email addresses, a CA IT PAM process such as one that generates help desk tickets, and one or more SNMP trap destination IP addresses.

To help you get started, many predefined queries are available for scheduling as action alerts, as is. Examples include:

- Excessive user activity
- High CPU utilization average
- Low available disk space
- Security event log cleared in last 24 hours
- Windows audit policy changed in last 24 hours

Some queries use keyed lists, where you supply the values used in the query. Some keyed lists include predefined values that you can supplement. Examples include default accounts and privileged groups. Other keyed lists, such as that for business critical resources, have no default values. After you configure them, alerts can be scheduled for predefined queries such as:

- Group membership addition or removal by privileged groups
- Successful login by default account
- No events received by business critical sources

Keyed lists can be updated manually, by importing a file, or by running a CA IT PAM dynamic values process.

Note: See the *CA Enterprise Log Manager Administration Guide* for details on action alerts.

Entitlement Management

When you configure the user store, you choose whether to use the default user store on the CA Enterprise Log Manager for setting up user accounts or reference an external user store where user accounts are already defined. The underlying database is exclusive to CA Enterprise Log Manager and does not use a commercial DBMS.

Supported external user stores include CA SiteMinder and LDAP directories such as Microsoft Active Directory, Sun One, and Novell eDirectory. If you reference an external user store, user account information is automatically loaded in read-only format as shown by the arrow in the following diagram. You define only application-specific details to selected accounts. No data is moved from the internal user store to the referenced external user store.
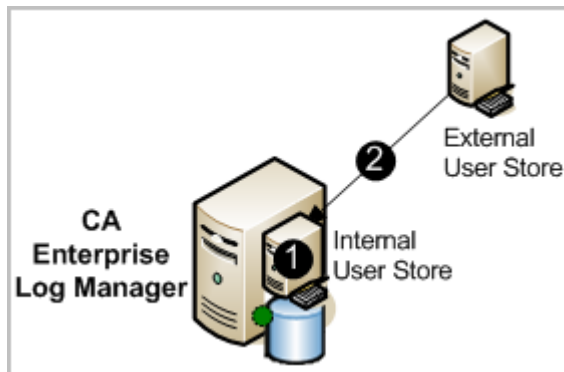
The numbers on the illustration refer to these steps:

1. The internal user store performs entitlement management by authenticating the credentials supplied by users at login and authorizing users to access different features of the user interface based on the policies associated with the roles assigned to their user accounts. If the user name and password of the user attempting to log in have been loaded by an external user store, the credentials entered must match the loaded credentials.

2. The external user store has no function other than to load its user accounts into the internal user store. These are loaded automatically when the reference to the user store is saved.

Note: See the *CA Enterprise Log Manager Implementation Guide* for details on configuring basic user access. See the *CA Enterprise Log Manager Administration Guide* for details on policies supporting predefined roles, creating user accounts, and assigning roles.

Role-Based Access

CA Enterprise Log Manager provides three predefined application groups or roles. Administrators assign the following roles to users to specify their access rights to CA Enterprise Log Manager features:

- Administrator

- Analyst

- Auditor

The Auditor has access to few features. The Analyst has access to all Auditor features plus more. The Administrator has access to all features. You can define a custom role with associated policies that limit user access to resources in the way that suits your business needs.
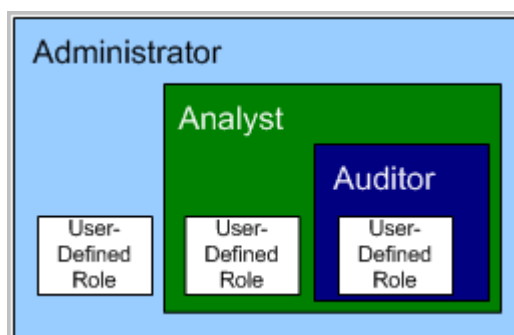
Administrators can customize access to any resource by creating a custom application group with associated policies and assigning that application group, or role, to user accounts.

Note: See the *CA Enterprise Log Manager Administration Guide* for details on planning and creating custom roles, custom policies, and access filters.

Subscription Management

The subscription module is the service that enables subscription updates from the CA Subscription Server to be automatically downloaded on a scheduled basis and distributed to CA Enterprise Log Manager servers. When a subscription update includes the module for agents, users initiate the deployment of these updates to agents. *Subscription update*s are updates to CA Enterprise Log Manager software components and operating system updates, patches, and content updates such as reports.

The following illustration depicts the simplest direct Internet connection scenario:
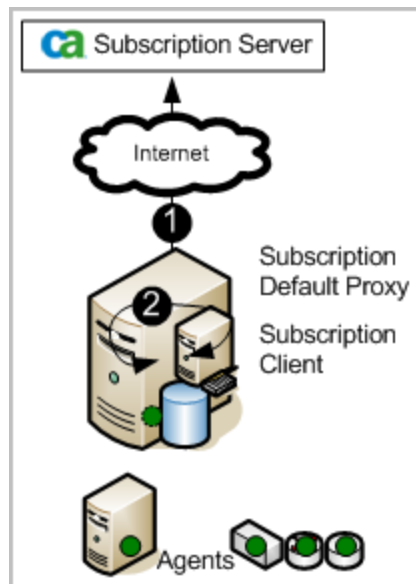
The numbers on the illustration refer to these steps:

1. The CA Enterprise Log Manager server, as the default subscription server, contacts the CA Subscription server for updates and downloads any new available updates. The CA Enterprise Log Manager server creates a backup, then pushes content updates to the embedded component of the management server that stores content updates for all other CA Enterprise Log Managers.

2. The CA Enterprise Log Manager server, as a subscription client, self-installs the product and operating system updates it needs.

Note: See the *Implementation Guide* for details on planning and configuring subscription. See the *Administration Guide* for details on refining and modifying the subscription configuration and for applying updates to agents.

Out-of-the-Box Content

CA Enterprise Log Manager includes predefined content that you can begin using as soon as you install and configure the product. The subscription process regularly adds new content and updates existing content.

Categories of predefined content include:

- Reports with tags

- Queries with tags

- Integrations with associated sensors, parsing files (XMP), mapping (DM) files, and in some cases, suppression rules

- Suppression and summarization rules

Chapter 5: Learning More about CA Enterprise Log Manager

This section contains the following topics:

Display Tooltips

You can identify the purpose of buttons, check boxes, and reports on the CA Enterprise Log Manager page in your current view.

To display tooltips and other help

1. Move your cursor over the buttons to display the description of the button function. You can view the function of any button in this way.
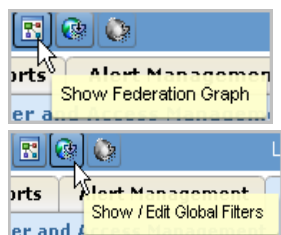
2. Notice the difference between active and inactive buttons.

   Enabled, active buttons are displayed in color. For example, Administrators of user and access management view the Access Filter List button in color.

   Disabled, inactive buttons are displayed in black and white. For example, Auditors view the Access Filter List buttons in black and white.

3. View descriptions for entry fields or check boxes by moving your cursor over the field name.
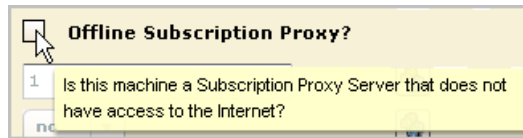
4. View descriptions of reports by moving your cursor over the report name.
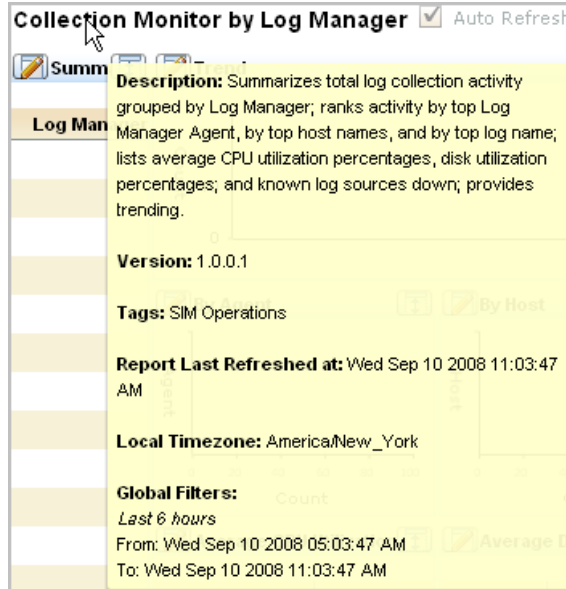
5. Notice an orange dot to the left of some fields. This dot indicates that the field is required. For configurations you can save, a save is not allowed until you have entries in all required fields.
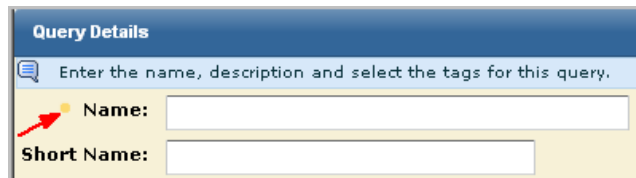
Display Online Help

You can display help for the page you are viewing or for any task you want to perform.

To display online help

1. Click the Help link in the toolbar to display the online help system for CA Enterprise Log Manager.

The CA Enterprise Log Manager help system appears, with the contents displayed in the left pane.
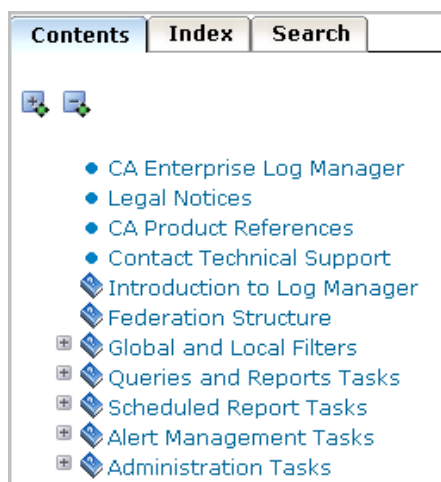
2. Access context-sensitive help from a Help button as shown in the following example.

    a.   Click the Show / Edit Global Filters button.
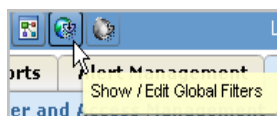
        The Global Filters and Settings window appears with a Help button.
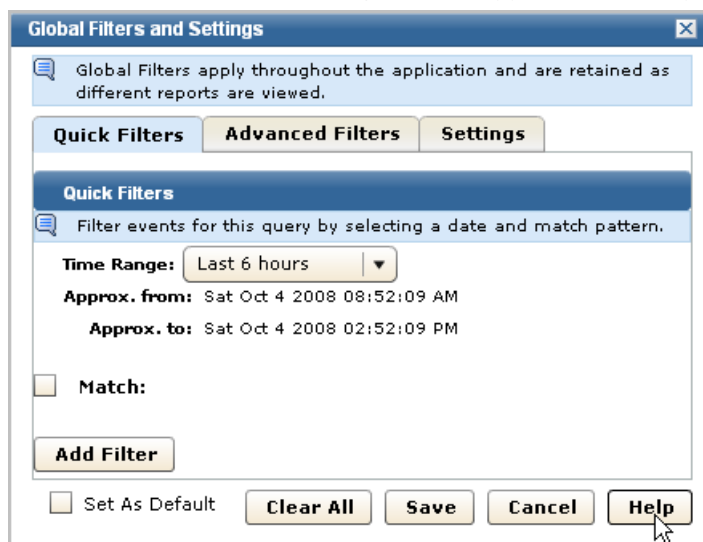
b. Click the Help button. Online help for the procedure you can perform on the current page, pane, or dialog appears in a secondary window.
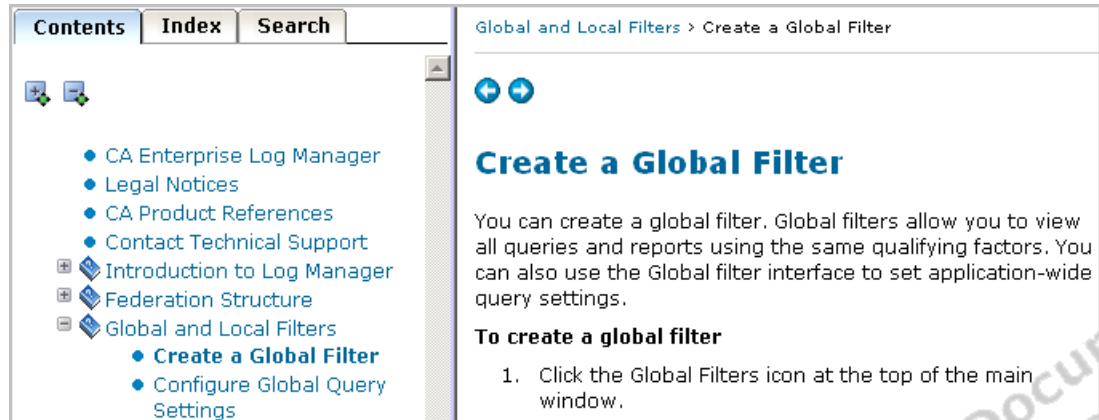
c. If you know the task you want to perform, but do not know how to access the corresponding page in CA Enterprise Log Manager, you may find it listed in the Table of Contents. Clicking the task title displays the page.

Note: If you are unable to find the task you need in the Table of Contents, refer to the bookshelf of documentation.

Explore the Bookshelf of Documentation

You can copy the bookshelf to your local drive and open any book in HTML or PDF format. Books in HTML format contain cross-book cross-references.

To explore the bookshelf

1. Copy the Bookshelf to your local drive from the installation DVD for the application or download it from the CA Customer Support website. Double-click Bookshelf.hta or Bookshelf.html to open the bookshelf.

    A page similar to the following appears.
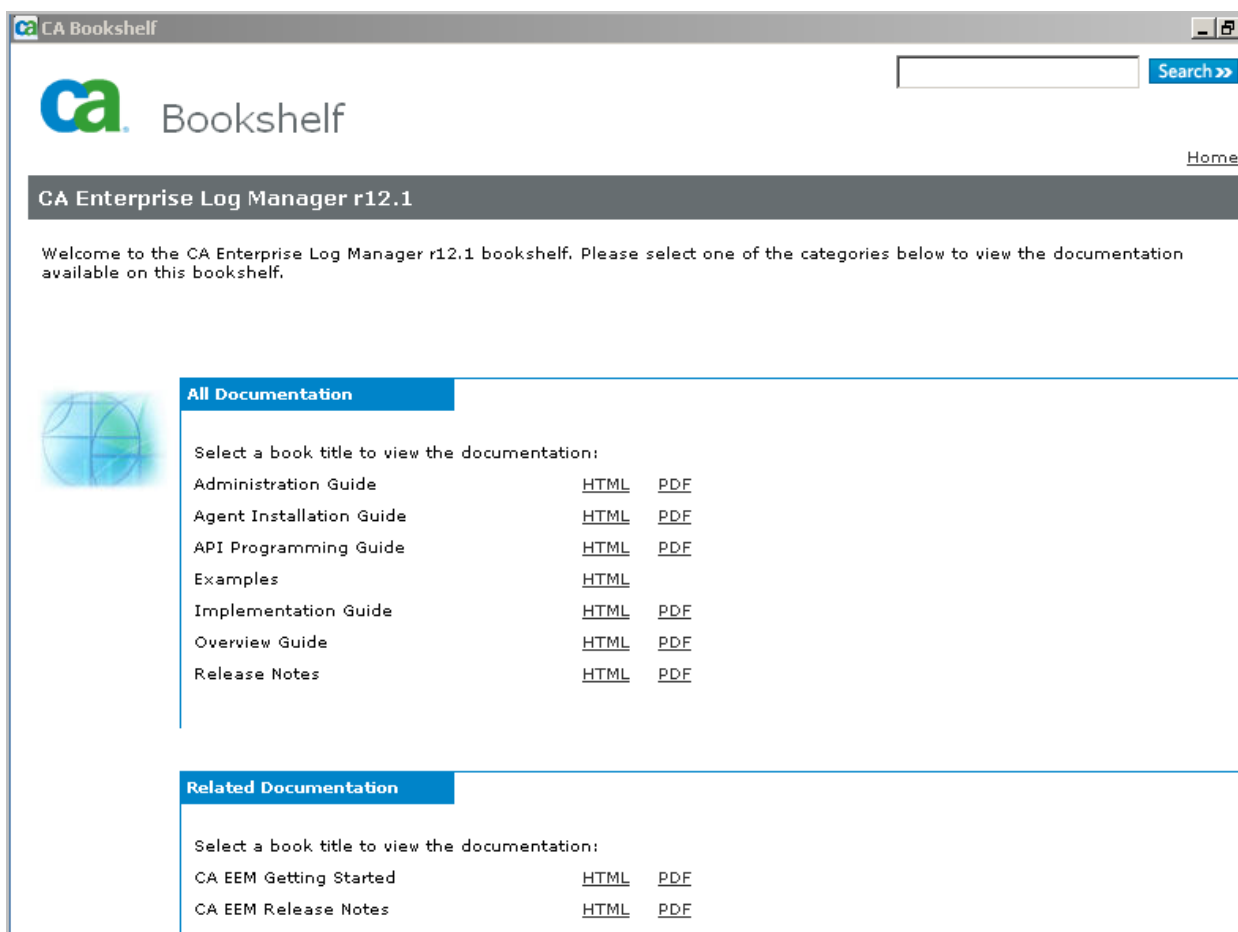
Descriptions of the contents of the major guides and the Examples follows:

Deliverable	Describes how to
Agent Installation Guide	Install agents

Deliverable	Describes how to
Implementation Guide	Install and configure a CA Enterprise Log Manager system.
Administration Guide	Customize the configuration, perform routine administration tasks, and work with queries, reports, and alerts.
API Programming Guide	Use the API to display event data in a web browser or to embed reports in another CA or third-party product.
Examples	Solve common business problems, with links to topics in the documentation.

2. Type a value in the Search entry field and click the Search button to display all documented occurrences that include your entry.

3. Click a Print link to open the PDF of the selected guide.

4. Click an HTML link to open the integrated documentation set. The integrated set includes all guides in HTML format. If you select the HTML link for the Overview Guide, that is the guide that is displayed.
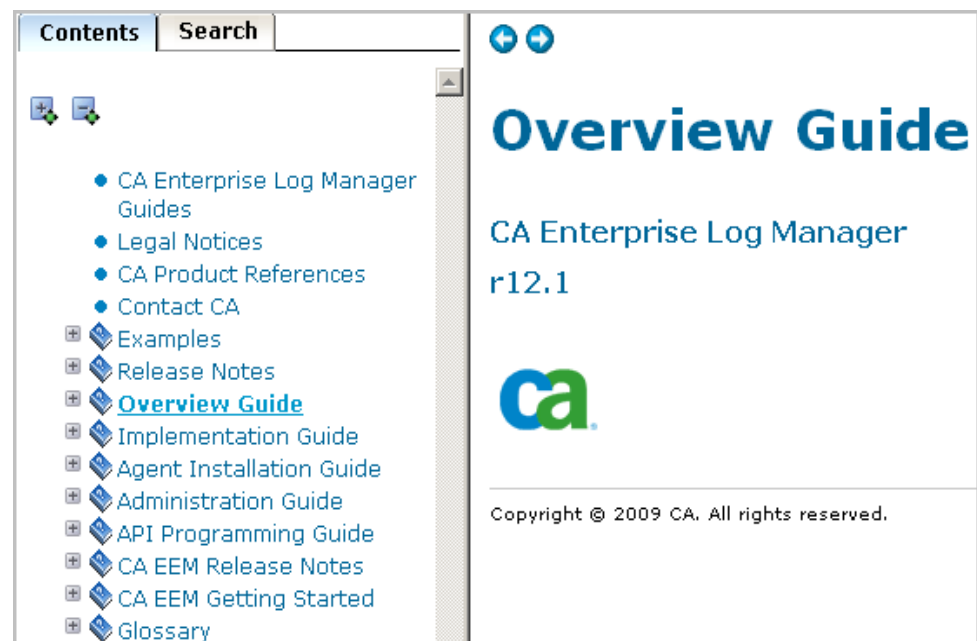
Glossary

access filter

An *access filter* is a filter that the Administrator can set to control what event data non-Administrator users or groups can view. For example, an access filter can restrict the data specified identities can view in a report. Access filters are automatically converted into obligation policies.

access policy

An *access policy* is a rule that grants or denies an identity (user or user group) access rights to an application resource. CA Enterprise Log Manager determines whether policies apply to the particular user by matching identities, resources, resource classes, and evaluating the filters.

account

An *account* is a global user who is also a CALM application user. A single person could have more than one account, each with a different user-defined role.

action alert

An *action alert* is a scheduled query job, which can be used to detect policy violations, usage trends, login patterns, and other event actions that require near-term attention. By default, when the alert queries return results, the results are displayed on the CA Enterprise Log Manager Alerts page and are also added to an RSS Feed. When you schedule an alert, you can specify additional destinations, including email, a CA IT PAM event/alert output process, and SNMP traps.

action query

An *action query* is a query that supports an Action Alert. It is run on a recurring schedule to test for the conditions outlined by the Action Alert to which it is attached.

Administrator role

The *Administrator role* grants users the ability to perform all valid actions on all CA Enterprise Log Manager resources. Only Administrators are permitted to configure log collection and services or manage users, access policies, and access filters.

agent

An *agent* is a generic service configured with connectors, each of which collects raw events from a single event source and then sends them to a CA Enterprise Log Manager for processing. Each CA Enterprise Log Manager has an onboard agent. Additionally, you can install an agent on a remote collection point and collect events on hosts where agents cannot be installed. You can also install an agent on the host where event sources are running and benefit from the ability to apply suppression rules and encrypt transmission to the CA Enterprise Log Manager.

agent explorer

The *agent explorer* is the store for agent configuration settings. (Agents can be installed on a collection point or on the endpoints where the event sources exist.)

agent group

An *agent group* is a tag that users can apply to selected agents that lets user apply an agent configuration to multiple agents at once and retrieve reports based on the groups. A given agent can belong to only one group at a time. Agent groups are based on user-defined criteria such as geographical region or importance.

agent management

Agent management is the software process that controls all agents associated with all federated CA Enterprise Log Managers. It authenticates agents that communicate with it.

alert server

The *alert server* is the store for action alerts and action alert jobs.

Analyst role

The *Analyst role* grants users the ability to create and edit custom reports and queries, edit and annotate reports, create tags, and schedule reports and action alerts. Analysts can also perform all Auditor tasks.

application group

An *application group* is a product-specific group that can be assigned to a global user. Predefined application groups for CA Enterprise Log Manager, or roles, are Administrator, Analyst and Auditor. These application groups are only available for CA Enterprise Log Manager users; they are not available for assignment to users of other products registered to the same CA EEM server. User-defined application groups must be added to the CALM Application Access default policy so that its users can access the CA Enterprise Log Manager.

application instance

An *application instance* is a common space in the CA EEM repository where all the authorization policies, users, groups, content, and configurations are stored. Typically, all CA Enterprise Log Manager servers in an enterprise use the same application instance (CAELM, by default). You can install CA Enterprise Log Manager servers with different application instances, but only severs that share the same application instance can be federated. Servers configured to use the same CA EEM server but with different application instances share only the user store, password policies, and global groups. Different CA products have different default application instances.

application resource

An *application resource* is any of the CA Enterprise Log Manager-specific resources to which CALM access policies grant or deny specified identities the ability to perform application-specific actions such as create, schedule and edit. Examples include report, alert, and integration. See also global resource.

application user

An *application user* is a global user that has been assigned application-level details. CA Enterprise Log Manager application user details include the user group and any restrictions on access. If the user store is the local repository, application user details also include the logon credentials and password policies.

AppObjects

The *AppObjects,* or Application Objects, are product-specific resources stored in CA EEM under the application instance for a given product. For the CAELM application instance, these resources include report and query content, scheduled jobs for reports and alerts, agent content and configurations, service, adapter, and integration configurations, data mapping and message parsing files, and suppression and summarization rules.

archive catalog

See catalog.

archive query

An *archive query* is a query of the catalog that is used to identify the cold databases that need to be restored and defrosted for querying. An archive query is different from a normal query in that it targets cold databases, whereas a normal query targets hot, warm, and defrosted databases. Administrators can issue an archive query from the Administration tab, Log Collection subtab, Archive Catalog Query option.

archived databases

The *archived databases* on a given CA Enterprise Log Manager server include all warm databases that are available for querying but need to be manually backed up before they expire, all cold databases that have been recorded as backed up, and all databases that have been recorded as restored from backup.

audit records

Audit records contain security events such as authentication attempts, file accesses, and changes to security policies, user accounts, or privileges. Administrators specify which types of events should be audited and what should be logged.

Auditor role

An *Auditor role* grants users access to reports and the data they contain. Auditors can view reports, the report template list, the scheduled report job list, the generated report list. Auditors can schedule and annotate reports. Auditors do not have access to the RSS (Rich Site Summary) feeds unless the configuration is set to require no authentication for viewing action alerts.

auto-archive

Auto-archive is a configurable process that automates the moving of archive databases from one server to another. In the first auto-archive phase, the collection server sends newly archived databases to the reporting server at the frequency you specify. In the second phase, the reporting server sends aging databases to the remote storage server for long-term storage, eliminating the need for a manual backup and move procedure. Auto-archiving requires you configure passwordless authentication from the source to the destination server.

CA adapters

The *CA Adapters* are a group of listeners that receive events from CA Audit components such as CA Audit clients, iRecorders, and SAPI recorders as well as sources that send events natively through iTechnology.

CA Enterprise Log Manager

CA Enterprise Log Manager is a solution that helps you collect logs from widely dispersed event sources of different types, check for compliance with queries and reports, and keep records of databases of compressed logs you have moved to external, long-term storage.

CA IT PAM

CA IT PAM is the short form for CA IT Process Automation Manager. This CA product automates processes you define. CA Enterprise Log Manager uses two processes--the process of creating an event/alert output process for a local product, such as CA Service Desk, and the process of dynamically generating lists that can be imported as keyed values. Integration requires CA IT PAM r2.1.

CA Spectrum

CA Spectrum is a network fault management product that can be integrated with CA Enterprise Log Manager for use as a destination for alerts sent in the form of SNMP traps.

CA Subscription Server

The *CA Subscription Server* is the source for subscription updates from CA.

CAELM

CAELM is the application instance name that CA EEM uses for CA Enterprise Log Manager. To access CA Enterprise Log Manager functionality in CA Embedded Entitlements Manager, enter the URL, https://<ip_address>:5250/spin/eiam/eiam.csp, select CAELM as the application name and enter the password of the EiamAdmin user.

caelmadmin

The *caelmadmin* user name and password are credentials required to access the operating system of the soft appliance. The caelmadmin user ID is created during the installation of this operating system. During installation of the software component, the installer must specify the password for the CA EEM superuser account, EiamAdmin. The caelmadmin account is assigned this same password. We recommend that the server administrator ssh in as the caelmadmin user and change this default password. Although the administrator cannot ssh in as root, the administrator can switch users to root (su root) if needed.

caelmservice

The *caelmservice* is a service account that allows iGateway and the local CA EEM services to run as a non-root user. The caelmservice account is used for installing operating system updates downloaded with subscription updates.

calendar

A *calendar* is a means of limiting the times that an access policy is effective. A policy allows specified identities to perform specified actions against a specified resource during a specified time.

CALM

CALM is a predefined resource class that includes the following CA Enterprise Log Manager resources: Alert, ArchiveQuery, calmTag, Data, EventGrouping, Integration, and Report. Actions permitted on this resource class are Annotate (Reports), Create (Alert, calmTag, EventGrouping, Integration, and Report), Dataaccess (Data), Run (ArchiveQuery), and Schedule (Alert, Report).

CALM Application Access policy

The *CALM Application Access policy* is an access control list type of scoping policy that defines who can log into the CA Enterprise Log Manager. By default, the [Group] Administrator, [Group] Analyst and [Group] Auditor are granted logon access.

calmTag

The *calmTag* is a named attribute on the AppObject used when creating a scoping policy to limit the users to reports and queries belonging to certain Tags. All reports and queries are AppObjects and have calmTag as an attribute. (This is not to be confused with the resource Tag.)

catalog

The *catalog* is the database on each CA Enterprise Log Manager that maintains the state of archived databases as well as acting like a high level index across all databases. State information (warm, cold, or defrosted) is maintained for all databases that have ever been on this CA Enterprise Log Manager and any database that has been restored to this CA Enterprise Log Manager as a defrosted database. Indexing ability extends to all hot and warm databases in the event log store on this CA Enterprise Log Manager.

CEG fields

CEG fields are labels used to standardize the presentation of raw event fields from disparate event sources. During event refinement, CA Enterprise Log Manager parses raw event messages into a series of name/value pairs, then maps the raw event names to standard CEG fields. This refinement creates name/value pairs consisting of CEG fields and values from the raw event. That is, different labels used in raw events for the same data object or network element are converted to the same CEG field name when raw events are refined. CEG fields are mapped to OIDs in the MIB used for SNMP traps.

certificates

The predefined *certificates* used by CA Enterprise Log Manager are CAELMCert.cer and CAELM_AgentCert.cer. All CA Enterprise Log Manager services use CAELMCert.cer to communicate with the management server. All agents use CAELM_AgentCert.cer to communicate with their collection server.

cold database state

A *cold database state* is applied to a warm database when an Administrator runs the LMArchive utility to notify CA Enterprise Log Manager that the database has been backed up. Administrators must back up warm databases and run this utility before they are deleted. A warm database is automatically deleted when its age exceeds the Max Archive Days or when the configured Archive Disk Space threshold is reached, whichever comes first. You can query the archive database to identify databases in the warm and cold states.

collection point

A *collection point* is a server on which an agent is installed, where the server has network proximity to all of the servers with event sources associated with its agent's connectors.

collection server

A *collection server* is a role performed by a CA Enterprise Log Manager server. A collection server refines incoming event logs, inserts them into the hot database, compresses the hot database, and auto-archives, or copies, it to the related reporting server. The collection server compresses the hot database when it reaches the configured size and auto-archives it on the configured schedule.

Common Event Grammar (CEG)

Common Event Grammar (CEG) is the schema that provides a standard format to which CA Enterprise Log Manager converts events using parsing and mapping files, before storing them in the Event Log Store. The CEG uses common, normalized fields to define security events from different platforms and products. Events that cannot be parsed or mapped are stored as raw events.

computer security log management

Computer Security Log Management is defined by NIST as "the process for generating, transmitting, storing, analyzing, and disposing of computer security log data."

connector

A *connector* is an integration for a particular event source that is configured on a given agent. An agent can load multiple connectors of similar or dissimilar types into memory. The connector enables raw event collection from an event source and rule-based transmission of converted events to an event log store, where they are inserted into the hot database. Out-of-the-box integrations provide optimized collection from a wide range of event sources, including operating systems, databases, web servers, firewalls, and many types of security applications. You can define a connector for a homegrown event source from scratch or using an integration as a template.

content updates

Content updates are the non-binary portion of subscription updates that are saved in the CA Enterprise Log Manager management server. Content updates include content such as XMP files, DM files, configuration updates for CA Enterprise Log Manager modules, and public key updates.

data access

Data access is a type of authorization granted to all CA Enterprise Log Managers through the Default Data Access policy on the CALM resource class. All users have access to all of the data except where restricted by data access filters.

data mapping (DM)

Data mapping is the process of mapping the key value pairs into the CEG. Data mapping is driven by a DM file.

data mapping (DM) files

Data mapping (DM) files are XML files that use the CA Common Event Grammar (CEG) to transform events from the source format into a CEG-compliant form that can be stored for reporting and analysis in the Event Log Store. One DM file is required for each log name before the event data can be stored. Users can modify a copy of a DM file and apply it to a specified connector.

database states

The database states include hot for the uncompressed database of new events, warm for a database of compressed events, cold for a backed up database, and defrosted for a database restored to the event log store where it was backed up. You can query hot, warm, and defrosted databases. An archive query displays information on cold databases.

default agent

The default agent is the onboard agent that is installed with the CA Enterprise Log Manager server. It can be configured for direct collection of syslog events as well as events from various non-syslog event sources such as CA Access Control r12 SP1, Microsoft Active Directory Certificate Service, and Oracle9i databases.

defrosted database state

A defrosted database state is the state applied to a database that has been restored to the archive directory after the Administrator runs the LMArchive utility to notify CA Enterprise Log Manager that it has been restored. Defrosted databases are retained for the number of hours configured for the Export Policy. You can query for event logs in databases that are in the hot, warm, and defrosted states.

defrosting

Defrosting is the process of changing the state of a database from cold to defrosted. This process is performed by CA Enterprise Log Manager when notified by the LMArchive utility that a known cold database has been restored. (If the cold database is not restored to its original CA Enterprise Log Manager, the LMArchive utility is not used and defrosting is not required; recataloging adds the restored database as a warm database.)

delegation policy

A delegation policy is an access policy that lets a user delegate their authority to another user, application group, global group, or dynamic group. You must explicitly delete the delegation policies created by the deleted or disabled user.

direct log collection

Direct log collection is the log collection technique where there is no intermediate agent between the event source and the CA Enterprise Log Manager software.

dynamic user group

A *dynamic user group* is composed of global users that share one or more common attributes. A dynamic user group is created through a special dynamic user group policy where the resource name is the dynamic user group name and membership is based on a set of filters configured on user and group attributes.

dynamic values process

A *dynamic values process* is a CA IT PAM process that you can invoke to populate or update the values list for a selected key that is used in reports or alerts. You provide the path to the Dynamic Values Process as part of IT PAM configuration on the Report Server Service List under the Administration tab. You click Import Dynamic Values list on the Values section associated with Key Values on this same UI page. Invoking the dynamic values process is one of three ways you can add values to your keys.

EEM User

The *EEM User*, configured in the Auto-Archiving section of the Event Log Store, specifies the user who can perform an archive query, recatalog the archive database, run the LMArchive utility, and run the restore-ca-elm shell script to restore archive databases for examination. This user must be assigned the predefined role of Administrator or a custom role associated with a custom policy that permits the edit action on the Database resource.

EiamAdmin user name

EiamAdmin is the default superuser name assigned to the installer of the CA Enterprise Log Manager servers. While installing the first CA Enterprise Log Manager software, the installer creates a password for this superuser account, unless a remote CA EEM server already exists. In that case, the installer must enter the existing password. After installing the soft appliance, the installer opens a browser from a workstation, enters the URL for CA Enterprise Log Manager and logs in as EiamAdmin with the associated password. This first user sets the user store, creates password policies, and creates the first user account with an Administrator role. Optionally, the EiamAdmin user can perform any operation controlled by the CA EEM.

entitlement management

Entitlement management is the means of controlling what users are allowed to do once they are authenticated and logged on to the CA Enterprise Log Manager interface. This is achieved with access policies associated with roles assigned to users. Roles, or application user groups, and access policies can be predefined or user-defined. Entitlement management is handled by the CA Enterprise Log Manager internal user store.

EPHI-related reports

The *EPHI-related reports*, are reports that focus on HIPAA security, where EPHI stands for Electronic Protected Health Information. These reports can help you demonstrate that all individually identifiable health information related to patients this is created, maintained, or transmitted electronically is protected.

event aggregation

Event aggregation is the process by which similar log entries are consolidated into a single entry containing a count of the number of occurrences of the event. Summarization rules define how events are aggregated.

event categories

Event categories are the tags used by the CA Enterprise Log Manager to classify events by their function before inserting them into the event store.

event collection

Event collection is the process of reading the raw event string from an event source and sending it to the configured CA Enterprise Log Manager. Event collection is followed by event refinement.

event filtering

Event filtering is the process of dropping events based on CEG filters.

event forwarding rules

Event forwarding rules specify that selected events are to be forwarded to third-party products, such as those that correlate events, after being saved in the event log store.

event log storage

Event log storage is the result of the archiving process, where the user backs up a warm database, notifies CA Enterprise Log Manager by running the LMArchive utility, and moves the backed up database from the event log store to long term storage.

event log store

The *event log store* is a component on the CA Enterprise Log Manager server where incoming events are stored in databases. The databases in the event log store must be manually backed up and moved to a remote log storage solution before the time configured for deletion. Archived databases can be restored to an event log store.

event refinement

Event refinement is the process where a collected raw event string is parsed into constituent event fields and mapped to CEG fields. Users can run queries to display the resulting refined event data. Event refinement follows event collection and precedes event storage.

event refinement library

The *event refinement library* is the store for predefined and user-defined integrations, mapping and parsing files, as well as suppression and summarization rules.

event source

An *event source* is the host from which a connector collects raw events. An event source can contain multiple log stores, each accessed by a separate connector. Deploying a new connector typically involves configuring the event source so that the agent can access it and read raw events from one of its log stores. Raw events for the operating system, different databases, and various security applications are stored separately on the event source.

event/alert output process

The *event/alert output process* is the CA IT PAM process that invokes a third-party product to respond to alert data configured in CA Enterprise Log Manager. You can select CA IT PAM Process as a destination when you schedule an alert job. When an alert runs the CA IT PAM process, CA Enterprise Log Manager sends CA IT PAM alert data and CA IT PAM forwards it along with its own processing parameters to the third party product as part of the event/alert output process.

event_action

The *event_action* is the fourth-level event-specific field in event normalization used by the CEG. It describes common actions. Examples of types of event actions include Process Start, Process Stop, and Application Error.

event_category

The *event_category* is the second-level event-specific field in event normalization used by the CEG. It provides a further classification of events with a specific ideal_model. Event category types include Operational Security, Identity Management, Configuration Management, Resource Access, and System Access.

event_class

The *event_class* is the third-level event-specific field in event normalization used by the CEG. It provides a further classification of events within a specific event_category.

events

Events in CA Enterprise Log Manager are the log records generated by each specified event source.

federation servers

Federation servers are CA Enterprise Log Manager servers connected to one another in a network for the purpose of distributing the collection of log data but aggregating the collected data for reporting. Federation servers can be connected in a hierarchical or meshed topology. Reports of federated data include that from the target server as well as that from children or peers of that server, if any.

filter

A *filter* is a means by which you can restrict an event log store query.

folder

A *folder* is a directory path location that CA Enterprise Log Manager management server uses to store the CA Enterprise Log Manager object types. You reference folders in scoping policies to grant or deny users the right to access a specified object type.

function mappings

Function mappings are an optional part of a Data Mapping file for a product integration. A function mapping is used to populate a CEG field when the needed value cannot be retrieved directly from the source event. All function mappings consist of a CEG field name, a pre-defined or class field value and the function used to obtain or calculate the value.

global configuration

The *global configuration* is a series of settings that apply to all CA Enterprise Log Manager servers that use the same management server.

global filter

A *global filter* is a set of criteria you can specify that limits what is presented in all reports. For example, a global filter of the last 7 days reports events generated in the last seven days.

global group

A *global group* is a group that is shared across application instances registered to the same CA Enterprise Log Manager management server. Any user can be assigned to one of more global groups. Access policies can be defined with global groups as Identities granted or denied the ability to perform selected actions on selected resources.

global resource

A *global resource* for the CA Enterprise Log Manager product is a resource shared with other CA applications. You can create scoping policies with global resources. Examples include user, policy, and calendar. See also application resource.

global user

A *global user* is the user account information that excludes application-specific details. The global user details and global group memberships are shared across all CA applications that integrate with the default user store. Global user details can be stored in the embedded repository or in an external directory.

hierarchical federation

A *hierarchical federation* of CA Enterprise Log Manager servers is a topology that establishes a hierarchical relationship between servers. In its simplest form, server 2 is a child of server 1 but server 1 is not a child of server 2. That is, the relationship is one-way only. A hierarchical federation can have multiple levels of parent-child relationships and a single parent server can have many child servers. A federated query return results from the selected server and its children.

hot database state

A *hot database state* is the state of the database in the event log store where new events are inserted. When the hot database reaches a configurable size on the collection server, the database is compressed, cataloged, and moved to warm storage on the reporting server. Additionally, all servers store new self-monitoring events in a hot database.

HTTP proxy server

An *HTTP proxy server* is a proxy server that acts like a firewall and prevents Internet traffic from entering or leaving the enterprise except through the proxy. Outgoing traffic can specify an ID and password to bypass the proxy server. The use of a local HTTP proxy server in subscription management is configurable.

ideal_model

ideal_model represents the technology expressing the event. This is the first CEG field in a hierarchy of fields used for event classification and normalization. Examples of an ideal model include antivirus, DBMS, firewall, operating system, and web server. Check Point, Cisco PIX and Netscreen/Juniper firewall products could be normalized with a value of "Firewall" in the field ideal_model.

identity

An *identity* in CA Enterprise Log Manager is a user or group that is allowed access to the CAELM application instance and its resources. An identity for any CA product can be a global user, an application user, a global group, an application group, or a dynamic group.

identity access control list

An *identity access control list* lets you specify different actions each selected identity can take on the selected resources. For example, with an identity access control list, you can specify that one identity can create reports and another can schedule and annotate reports. An identity access control list differs from an access control list in that it is identity-centric rather than resource-centric.

installer

The *installer* is the individual who installs the soft appliance and the agents. During the installation process, the caelmadmin and EiamAdmin user names are created and the password specified for EiamAdmin is assigned to caelmadmin. These caelmadmin credentials are required for the first access to the operating system; the EiamAdmin credentials are required for the first access to the CA Enterprise Log Manager software and for installing agents.

integration

Integration is the means by which unclassified events are processed into refined events so that they can be displayed in queries and reports. Integration is implemented with a set of elements that enables a given agent and connector to collect events from one of more types of event sources and send them to CA Enterprise Log Manager. The set of elements includes the log sensor and the XMP and DM files that are designed to read from a specific product. Examples of predefined integrations include those for processing syslog events and WMI events. You can create custom integrations to enable the processing of unclassified events.

integration elements

Integration elements include a sensor, a configuration helper, a data access file, one or more XMP message parsing (XMP) files, and one or more data mapping files.

iTech event plugin

The *iTech event plugin* is a CA adapter that an Administrator can configure with selected mapping files. It receives events from remote iRecorders, CA EEM, iTechnology itself, or any product that sends events through iTechnology.

key values

Key values are user-defined values assigned to a user-defined list (key group). When a query uses a key group, the search results include matches to any of the key values in the key group. There are several predefined key groups, some of which contain predefined key values, which are used in predefined queries and reports.

LMArchive utility

The *LMArchive utility* is the command line utility that tracks the backup and restoration of archive databases to the event log store on a CA Enterprise Log Manager server. Use LMArchive to query for the list of warm database files that are ready for archiving. After backing up the listed database and moving it to long-term (cold) storage, use LMArchive to create a record on CA Enterprise Log Manager that this database was backed up. After restoring a cold database to its original CA Enterprise Log Manager, use LMArchive to notify CA Enterprise Log Manager, which in turn changes the database files to a defrosted state that can be queried.

LMSEOSImport utility

The *LMSEOSImport* utility is a command line utility used to import SEOSDATA, or existing events, into CA Enterprise Log Manager as part of the migration from Audit Reporter, Viewer, or Audit Collector. The utility is supported only on Microsoft Windows and Sun Solaris Sparc.

local event

A *local event* is an event that involves a single entity, where the source and the destination of the event is the same host machine. A local event is type 1 of the four event types used in the Common Event Grammar (CEG).

local filter

A *local filter* is a set of criteria you can establish while viewing a report to limit the displayed data for the current report.

log

A *log* is an audit record, or recorded message, of an event or a collection of events. A log may be an audit log, a transaction log, an intrusion log, a connection log, a system performance record, a user activity log, or an alert.

log analysis

Log analysis is the study of log entries to identify events of interest. If logs are not analyzed in a timely manner, their value is significantly reduced.

log archiving

> *Log archiving* is the process of that occurs when the hot database reaches its maximum size, where row-level compression is done and the state is changed from hot to warm. Administrators must manually back up the warm databases before the threshold for deletion is reached and run the LMArchive utility to record the name of the backups. This information then becomes available for viewing through the Archive Query.

log entry

> A *log entry* is an entry in a log that contains information on a specific event that occurred on a system or within a network.

log parsing

> *Log parsing* is the process of extracting data from a log so that the parsed values can be used in a subsequent stage of log management.

log record

> A *log record* is an individual audit record.

log sensor

> A *log sensor* is an integration component designed to read from a specific log type such as a database, syslog, file, or SNMP. Log sensors are reused. Typically, users do not create custom log sensors.

management server

> The *management server* is a role assigned to the first CA Enterprise Log Manager server installed. This CA Enterprise Log Manager server contains the repository that stores shared content, such as policies, for all its CA Enterprise Log Managers. This server is typically the default subscription proxy. While not recommended for most production environments, the management server can perform all roles.

mapping analysis

> A *mapping analysis* is a step in the Mapping File wizard that lets you test and make changes to a data mapping (DM) file. Sample events are tested against the DM file and results are validated with the CEG.

meshed federation

> A *meshed federation* of CA Enterprise Log Manager servers is a topology that establishes a peer relationship between servers. In its simplest form, server 2 is a child of server 1 and server 1 is a child of server 2. A meshed pair of servers has a two-way relationship. A meshed federation can be defined such that many servers are all peers of one another. A federated query returns results from the selected server and all its peers.

message parsing

> *Message parsing* is the process of applying rules to the analysis of a raw event log to get relevant information such as timestamp, IP address, and user name. Parsing rules use character matching to locate specific event text and link it with selected values.

message parsing file (XMP)

A *message parsing file (XMP)* is an XML file associated with a specific event source type that applies parsing rules. Parsing rules break out relevant data in a collected raw event into name/value pairs, which are passed to the data mapping file for further processing. This file type is used in all integrations, and in connectors, which are based on integrations. In the case of CA Adapters, XMP files can also be applied at the CA Enterprise Log Manager server.

message parsing library

The *message parsing library* is a library that accepts events from the listener queues and uses regular expressions to tokenize strings into name/value pairs.

message parsing token (ELM)

A *message parsing token* is a re-usable template for building the regular expression syntax used in CA Enterprise Log Manager message parsing. A token has a name, a type, and a corresponding regular expression string.

MIB (management information base)

The *MIB (management information base)* for CA Enterprise Log Manager, CA-ELM.MIB, must be imported and compiled by each product that is to receive alerts in the form of SNMP traps from CA Enterprise Log Manager. The MIB shows the origin of each numeric object identifier (OID) used in an SNMP trap message with a description of that data object or network element. In the MIB for SNMP traps sent by CA Enterprise Log Manager, the textual description of each data object is for the associated CEG field. The MIB helps ensure that all name/value pairs sent in an SNMP trap are correctly interpreted at the destination.

module (to download)

A *module* is a logical grouping of component updates that is made available for download through subscription. A module can contain binary updates, content updates, or both. For example, all reports make up one module, all sponsor binary updates make up another module. CA defines what makes up each module.

native event

A *native event* is the state or action that triggers a raw event. Native events are received and parsed/mapped as appropriate, then transmitted as raw or refined events. A failed authentication is a native event.

NIST

The *National Institute of Standards and Technology (NIST)* is the federal technology agency that provides recommendations in its Special Publication 800-92 *Guide to Computer Security Log Management* that were used as the basis for the CA Enterprise Log Manager.

obligation policy

An *obligation policy* is a policy that is created automatically when you create an access filter. You should not attempt to create, edit, or delete an obligation policy directly. Instead, create, edit or delete the access filter.

observed event

An *observed event* is an event that involves a source, a destination, and an agent, where the event is observed and recorded by an event-collection agent.

ODBC and JDBC access

ODBC and JDBC access to CA Enterprise Log Manager event log stores supports your use of event data with a variety of third-party products, including custom event reporting with third-party reporting tools, event correlation with correlation engines, and event evaluation by intrusion and malware detections products. Systems with Windows operating systems use ODBC access; those with UNIX and Linux operating systems use JDBC access.

ODBC server

The *ODBC server* is the configured service that sets the port used for communications between the ODBC or JDBC client and the CA Enterprise Log Manager server and specifies whether to use SSL encryption.

OID (object identifier)

An *OID (object identifier)* is a unique numeric identifier for a data object that is paired with a value in an SNMP trap message. Each OID used in an SNMP trap sent by CA Enterprise Log Manager is mapped to a textual CEG field in the MIB. Each OID that is mapped to a CEG field has this syntax: 1.3.6.1.4.1.791.9845.x.x.x, where 791 is the enterprise number for CA and 9845 is the product identifier for CA Enterprise Log Manager.

parsing

Parsing, also called message parsing (MP), is the process of taking raw device data and turning it into key-value pairs. Parsing is driven by an XMP file. Parsing, which precedes data mapping, is one step of the integration process that turns the raw event collected from an event source into a refined event you can view.

parsing file wizard

The *parsing file wizard* is a CA Enterprise Log Manager feature that Administrators use to create, edit, and analyze eXtensible Message Parsing (XMP) files stored in the CA Enterprise Log Manager management server. Customizing the parsing of incoming event data involves editing the pre-matched strings and filters. New and edited files are displayed in the Log Collection Explorer, Event Refinement Library, Parsing Files, User folder.

pozFolder

The *pozFolder* is an attribute of the AppObject, where the value is the parent path of the AppObject. The pozFolder attribute and value is used in the filters for access policies that restrict access to resources such as reports, queries, and configurations.

profile

A *profile* is an optional, configurable, set of tag and data filters that can be product-specific, technology-specific or confined to a selected category. A tag filter for a product, for example, limits the listed tags to the selected product tag. Data filters for a product display only data for the specified product in the reports you generate, the alerts you schedule, and the query results you view. After you create the profile you need, you can set that profile to be in effect whenever you log in. If you create several profiles, you can apply different profiles, one at a time, to your activities during a session. Predefined filters are delivered with subscription updates.

prompt

A *prompt* is a special type of query that displays results based on the value you enter and the CEG fields you select. Rows are returned only for events where the value you enter appears in one or more of the selected CEG fields.

query

A *query* is a set of criteria used to search the Event Log Stores of the active CA Enterprise Log Manager server and, if specified, its federated servers. A query targets hot, warm, or defrosted databases specified in the where clause of the query. For example, if the where clause limits the query to events with source_username="myname" in a certain time frame and only ten of the 1000 databases contain records meeting this criteria based on information contained in the catalog database, the query will run against only those ten databases. A query can return a maximum of 5000 rows of data. Any user with a predefined role can run a query. Only Analysts and Administrators can schedule a query to distribute an action alert, create a report by selecting the queries to include, or create a custom query using the Query Design wizard. See also archive query.

query library

The *query library* is the library that stores all predefined and user-defined queries, query tags, and prompt filters.

raw event

A *raw event* is the information triggered by a native event that is sent by a monitoring agent to the Log Manager collector. The raw event is often formatted as a syslog string or name-value pair. It is possible to review an event in its raw form in CA Enterprise Log Manager.

recataloging

A *recataloging* is a forced rebuild of the catalog. A recatalog is required only when restoring data to an event log store on a different server than the one on which it was generated. For example, if you designated one CA Enterprise Log Manager to act as a restore point for investigations on cold data, you would then need to force a recatalog of the database after restoring it to the designated restore point. A recatalog is automatically performed when iGateway is restarted, if needed. Recataloging a single database file can take several hours.

recorded event

A *recorded event* is the raw or refined event information after it is inserted into the database. Raw events are always recorded unless suppressed or summarized, as are refined events. This information is stored and searchable.

refined event

A *refined event* is mapped or parsed event information derived from raw or summarized events. CA Enterprise Log Manager performs the mapping and parsing so that the stored information is searchable.

remote event

A *remote event* is an event that involves two different host machines, the source and the destination. A remote event is type 2 of the four event types used in the Common Event Grammar (CEG).

remote storage server

A *remote storage server* is a role assigned to a server that receives auto-archived databases from one or more reporting servers. A remote storage server stores cold databases for the required number of years. The remote host used for storage typically does not have CA Enterprise Log Manager or any other product installed. For auto-archiving, configure non-interactive authentication.

report

A *report* is a graphical or tabular display of event log data that is generated by executing predefined or custom queries with filters. The data can be from hot, warm, and defrosted databases in the event log store of the selected server and, if requested, its federated servers.

report library

The *report library* is the library that stores all predefined and user-defined reports, report tags, generated reports and scheduled report jobs.

report server

The *report server* is the service that stores configuration information such as the email server to use when emailing alerts, the appearance of reports that are saved to PDF format, and the retention of policies for reports saved to the Report Server and alerts sent to the RSS feed.

reporting server

A *reporting server* is a role performed by a CA Enterprise Log Manager server. A reporting server receives auto-archived warm databases from one or more collection servers. A reporting server handles queries, reports, scheduled alerts, and scheduled reports.

restore point server

A *restore point server* is a role performed by a CA Enterprise Log Manager server. To investigate "cold" events, you can move databases from the remote storage server to the restore point server with a utility, add the databases to the catalog, and then conduct queries. Moving cold databases to a dedicated restore point is an alternative to moving them back to their original reporting server for investigation.

RSS event

An *RSS event* is an event generated by CA Enterprise Log Manager to convey an Action Alert to third-party products and users. The event is a summary of each Action Alert result and a link to the result file. The duration for a given RSS feed item is configurable.

RSS feed URL for action alerts

The *RSS feed URL for action alerts* is: https://{elmhostname}:5250/spin/calm/getActionQueryRssFeeds.csp. From this URL, you can view action alerts subject to the configuration for maximum age and quantity.

RSS feed URL for subscription

The *RSS feed URL for subscription* is a preconfigured link used by online subscription proxy servers in the process of retrieving subscription updates. This URL is for the CA Subscription Server.

SafeObject

SafeObject is a predefined resource class in CA EEM. It is the resource class to which AppObjects, stored under the scope of Application, belong. Users who define policies and filters for granting access to AppObjects refer to this resource class.

SAPI collector

The *SAPI collector* is a CA adapter that receives events from CA Audit Clients. CA Audit Clients send with the Collector action that provides build-in failover. Administrators configure the CA Audit SAPI Collector with, for example, selected ciphers and DM files.

SAPI recorder

A *SAPI recorder* was the technology used to send information to CA Audit before iTechnology. SAPI stands for Submit API (Application Programming Interface). CA Audit recorders for CA ACF2, CA Top Secret, RACF, Oracle, Sybase, and DB2 are examples of SAPI recorders.

SAPI router

The *SAPI router* is a CA adapter that receives events from integrations, such as Mainframe, and sends them to a CA Audit router.

saved configuration

A *saved configuration* is a stored configuration with the values for the data access attributes of an integration that can be used as a template when creating a new integration.

scoping policy

A *scoping policy* is a type of access policy that grants or denies access to resources stored in the management server, such as AppObjects, users, groups, folders, and policies. A scoping policy defines the identities that can access the specified resources.

scp utility

The *scp* secure copy (remote file copy program) is a UNIX utility that transfers files between UNIX computers on a network. This utility is made available at CA Enterprise Log Manager installation for you to use to transfer subscription update files from the online subscription proxy to the offline subscription proxy.

self-monitoring event

A *self-monitoring event* is an event that is logged by CA Enterprise Log Manager. Such events are automatically generated by acts performed by logged in users and by functions performed by various modules such as services and listeners. The SIM Operations Self Monitoring Events Details report can be viewed by selecting a report server and opening the Self Monitoring events tab.

services

The CA Enterprise Log Manager *services* are event log store, report server, and subscription. Administrators configure these services at a global level, where all settings apply to all CA Enterprise Log Managers by default. Most global settings for services can be overridden at the local level, that is, for any specified CA Enterprise Log Manager.

SNMP

SNMP is the acronym for Simple Network Management Protocol, an open standard for sending alert messages in the form of SNMP traps from an agent system to one or more management systems.

SNMP trap contents

An *SNMP trap* consists of name/value pairs, where each name is an OID (object identifier) and each value is one returned from the scheduled alert. Query results returned by an action alert consist of CEG fields and their values. The SNMP trap is populated by substituting an OID for each CEG field used for the name of the name/value pair. The mapping of each CEG field to an OID is stored in the MIB. The SNMP trap only includes name/value pairs for the fields you select when you configure the alert.

SNMP trap destinations

One or more *SNMP trap destinations* can be added when you schedule an action alert. Each SNMP trap destination is configured with an IP address and port. The destination is typically a NOC or a management server such as CA Spectrum or CA NSM. An SNMP trap is sent to configured destinations when queries for a scheduled alert job returns results.

soft appliance

The *soft appliance* includes an operating system component and the CA Enterprise Log Manager software component.

subscription client

A *subscription client* is a CA Enterprise Log Manager server that gets content updates from another CA Enterprise Log Manager server called a subscription proxy server. Subscription clients poll the configured subscription proxy server on a regular schedule and retrieve new updates when available. After retrieving updates, the client installs the downloaded components.

subscription module

The *subscription module* is the service that enables subscription updates from the CA Subscription Server to be automatically downloaded and distributed to all CA Enterprise Log Manager servers, and all agents. Global settings apply to local CA Enterprise Log Manager servers; local settings include whether the server is an offline proxy, an online proxy, or a subscription client.

subscription proxies (for client)

The *subscription proxies for client* make up the subscription proxy list that the client contacts in a round robin fashion to get CA Enterprise Log Manager software and operating system updates. If one proxy is busy, the next one in the list is contacted. If all are unavailable and the client is online, the default subscription proxy is used.

subscription proxies (for content updates)

S*ubscription proxies for content updates* are the subscription proxies selected to update the CA Enterprise Log Manager management server with content updates that are downloaded from the CA Subscription Server. Configuring multiple proxies for redundancy is a good practice.

subscription proxy (default)

The *default subscription proxy* is typically the CA Enterprise Log Manager server that is installed first and may also be the Primary CA Enterprise Log Manager. The default subscription proxy is also an online subscription proxy and, therefore, must have Internet access. If no other online subscription proxies are defined, this server gets subscription updates from the CA Subscription server, downloads binary updates to all clients, and pushes content updates to CA EEM. If other proxies are defined, this server still gets subscription updates, but is contacted by clients for updates only when no subscription proxy list is configured or when the configured list is exhausted.

subscription proxy (offline)

An *offline subscription proxy* is a CA Enterprise Log Manager server that gets subscription updates through a manual directory copy (using scp) from an online subscription proxy. Offline subscription proxies can be configured to download binary updates to clients that request them and to push the latest version of content updates to the management server if it has not yet received them. Offline subscription proxies do not need Internet access.

subscription proxy (online)

An *online subscription proxy* is a CA Enterprise Log Manager with Internet access that gets subscription updates from the CA Subscription server on a recurring schedule. A given online subscription proxy can be included in the proxy list for one or more clients, who contact listed proxies in round-robin fashion to request the binary updates. A given online proxy, if so configured, pushes new content and configuration updates to management server unless already pushed by another proxy. The subscription update directory of a selected online proxy is used as the source for copying updates to offline subscription proxies.

subscription updates

*Subscription update*s refer to the binary and non-binary files that are made available by CA Subscription server. Binary files are product module updates that are typically installed on the CA Enterprise Log Managers. Non-binary files, or content updates, are saved to the management server.

summarization rules

Summarization rules are rules that combine certain native events of a common type into one refined event. For example, a summarization rule can be configured to replace up to 1000 duplicate events with the same source and destination IP addresses and ports with a single summarization event. Such rules simplify event analysis and reduce log traffic.

suppression

Suppression is the process of dropping events based on CEG filters. Suppression is driven by SUP files.

suppression rules

Suppression rules are rules you configure to prevent certain refined events from appearing in your reports. You can create permanent suppression rules to suppress routine events of no security concern and you can create temporary rules to suppress the logging of planned events such as the creation of many new users.

tag

A *tag* is a term or key phrase that is used to identify queries or reports that belong to the same business-relevant grouping. Tags enable searches based on business-relevant groupings. Tag is also the resource name used in any policy that grants users the ability to create a tag.

URL for CA Embedded Entitlements Manager

The *URL for CA Embedded Entitlements Manager* (CA EEM) is: https://<ip_address>:5250/spin/eiam. To log in, select CAELM as the application and enter the password associated with the EiamAdmin user name.

URL for CA Enterprise Log Manager

The *URL for CA Enterprise Log Manager* is: https://<ip_address>:5250/spin/calm. To log in, enter the user name defined for your account by the Administrator and the associated password. Or, enter the EiamAdmin, the default superuser name, with the associated password.

user group

A *user group* can be an application group, a global group, or a dynamic group. Predefined CA Enterprise Log Manager application groups are Administrator, Analyst, and Auditor. CA Enterprise Log Manager users may belong to global groups through memberships apart from CA Enterprise Log Manager. Dynamic groups are user-defined and created through a dynamic group policy.

user role

A *user role* can be a predefined application user group or a user-defined application group. Custom user roles are needed when the predefined application groups (Administrator, Analyst, and Auditor) are not sufficiently fine-grained to reflect work assignments. Custom user roles require custom access policies and modification of predefined policies to include the new role.

user store

A *user store* is the repository for global user information and password policies. The CA Enterprise Log Manager user store is the local repository, by default, but can be configured to reference CA SiteMinder or a supported LDAP directory such as Microsoft Active Directory, Sun One, or Novell eDirectory. No matter how the user store is configured, the local repository on the management server contains application-specific information about users, such as their user role and associated access policies.

visualization components

Visualization components are available options for displaying report data including a table, a chart (line graph, bar graph, column graph, pie chart), or an event viewer.

warm database state

The *warm database state* is the state that a hot database of event logs is moved into when the size (Maximum Rows) of the hot database is exceeded or when a recatalog is performed after restoring a cold database to a new event log store. Warm databases are compressed and retained in the event log store until their age in days exceeds the configured value for Max Archive Days. You can query for event logs in databases that are in the hot, warm, and defrosted states.

XMP file analysis

XMP file analysis is the process performed by the Message Parsing utility to find all events containing each pre-match string and, for each matched event, parse the event into tokens using the first filter found that uses the same pre-match string.

Index